kaspersky

Kaspersky Endpoint Security 14.2 für Windows

© 2026 AO Kaspersky Lab

Inhalt

Hilfe zu Kaspersky Endpoint Security für Windows
- Neuerungen
- Behobene Probleme
- Häufige Fragen

Kaspersky Endpoint Security für Windows
- Modi des Programms: Standard, EDR Agent, Light Agent
- Lieferumfang
- Hard- und Softwarevoraussetzungen
- Vergleich der Programmfunktionen im Hinblick auf den Typ des Betriebssystems
- Vergleich der Programmfunktionen in Abhängigkeit der Verwaltungs-Tools
- Kompatibilität mit anderen Programmen

Programm installieren und deinstallieren
- Software-Verteilung über Kaspersky Security Center
  - Standardmäßige Installation des Programms
  - Erstellung eines Installationspakets
  - Datenbanken-Update im Installationspaket
  - Erstellung einer Aufgabe zur Remote-Installation
- Lokale Programminstallation mithilfe des Assistenten
- Remote-Installation des Programms mithilfe von System Center Configuration Manager
- Beschreibung der Installationseinstellungen in der Datei setup.ini
- Prozesse von Kaspersky Endpoint Security für Windows
- Auswahl der Programmkomponenten ändern
- Upgrade einer älteren Programmversion
  - Programm-Upgrade ohne Neustart
  - SMU-Update der Anwendung
- Die App entfernen

Lizenzverwaltung des Programms
- Über den Endbenutzer-Lizenzvertrag
- Über die Lizenz
- Über das Lizenzzertifikat
- Über das Abo
- Über den Lizenzschlüssel
- Über den Aktivierungscode
- Über die Schlüsseldatei
- Vergleich der Programmfunktionalität abhängig vom Lizenztyp für Arbeitsstationen
- Vergleich der Programmfunktionalität abhängig vom Lizenztyp für Server
- Programm aktivieren
- Einen Lizenzschlüssels entfernen
- Lizenz-Info anzeigen
- Lizenz kaufen
- Abo verlängern

Erste Schritte
- Über das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows
- Besonderheiten für die Verwendung unterschiedlicher Versionen des Verwaltungs-Plug-ins
- Besondere Überlegungen bei der Verwendung verschlüsselter Protokolle für die Interaktion mit externen Diensten
- Programmoberfläche
  - Programmsymbol im Infobereich
  - Einfache Programmoberfläche
  - Darstellung der Programmoberfläche anpassen
- Vorbereitung des Programms
- Richtlinienverwaltung
  - Richtlinie erstellen
  - Eine Richtlinie exportieren und importieren
  - Indikator des Schutzniveaus
- Aufgabenverwaltung
- Lokale Programmeinstellungen anpassen
- Kaspersky Endpoint Security starten und beenden
- Anhalten und Fortsetzen von Computerschutz und -kontrolle
- Konfigurationsdatei erstellen und verwenden
- Standardeinstellungen für das Programm wiederherstellen
- Leistung von Kaspersky Endpoint Security und Kompatibilität mit anderen Programmen
  - Energiesparmodus aktivieren und deaktivieren
  - Freigabe von Ressourcen für andere Programme aktivieren und deaktivieren
  - Bewährte Methoden zur Leistungsoptimierung von Kaspersky Endpoint Security

Schadsoftware-Untersuchung
- Untersuchung des Computers
- Wechseldatenträger beim Anschließen an den Computer untersuchen
- Untersuchung im Hintergrund
- Untersuchung aus dem Kontextmenü
- Integritätsprüfung für Anwendungen
- Untersuchungsbereich bearbeiten
- Untersuchung nach Zeitplan ausführen
- Untersuchung als anderer Benutzer ausführen
- Untersuchung optimieren

Update der Datenbanken und Programm-Module
- Schemata für das Update der Datenbanken und Programm-Module
  - Update aus dem Serverspeicher
  - Update aus dem gemeinsamen Ordner
  - Update mithilfe von Kaspersky Update Utility
  - Update im mobilen Modus
- Update-Aufgabe starten und abbrechen
- Update-Aufgabe mit den Rechten eines anderen Benutzers starten
- Startmodus für die Update-Aufgabe wählen
- Update-Quelle hinzufügen
- Aktualisierung von Programm-Modulen
- Verwendung eines Proxyservers beim Update
- Rollback des letzten Updates

Technologie zur Aktiven Desinfektion
Desinfektion aktiver Bedrohungen auf Workstations
Desinfektion aktiver Bedrohungen auf Servern
Unverarbeitete Bedrohungen eliminieren
Computerschutz
Echtzeit-Schutzstatus
Schutz vor bedrohlichen Dateien
Schutz vor bedrohlichen Dateien aktivieren und deaktivieren
Schutz vor bedrohlichen Dateien automatisch anhalten
Ändern der Aktion, welche die Komponente „Schutz vor bedrohlichen Dateien“ mit infizierten Dateien ausführen soll
Schutzbereich für die Komponente „Schutz vor bedrohlichen Dateien”
Untersuchungsmethoden verwenden
Verwendung von Untersuchungstechnologien durch die Komponente „Schutz vor bedrohlichen Dateien”
Dateiuntersuchung optimieren
Untersuchung von zusammengesetzten Dateien
Untersuchungsmodus für Dateien ändern
Container untersuchen
Programm-Überwachung
Programm-Überwachung aktivieren und deaktivieren
Sicherheitsgruppe für Programme verwenden
Die Sicherheitsgruppe eines Programms ändern
Rechte von Sicherheitsgruppen konfigurieren
Sicherheitsgruppe für Programme wählen, die vor Kaspersky Endpoint Security gestartet werden
Eine Sicherheitsgruppe für unbekannte Programme auswählen
Eine Sicherheitsgruppe für digital signierte Programme wählen
Verwendung von Rechten für Programme
Schutz für Betriebssystemressourcen und persönliche Daten
Löschen von Informationen über nicht verwendete Programme
Übersicht über die Programm-Überwachung
Schutz des Zugriffs auf Audio und Video
Schutz vor modifizierten USB-Geräten
Schutz vor modifizierten USB-Geräten aktivieren und deaktivieren
Verwenden der Bildschirmtastatur für die Autorisierung von USB-Geräten
Autorisierung eines Barcode-Scanners
AMSI-Schutz
AMSI-Schutz aktivieren und deaktivieren
Dateiuntersuchung durch den AMSI-Schutz optimieren
Schutz vor Web-Bedrohungen
Schutz vor Web-Bedrohungen aktivieren und deaktivieren
Konfigurieren von Methoden zur Erkennung bösartiger Webadressen
Anti-Phishing
Liste mit vertrauenswürdigen Webadressen erstellen
Exportieren und importieren der Liste vertrauenswürdiger Webadressen
Schutz vor E-Mail-Bedrohungen
Schutz vor E-Mail-Bedrohungen aktivieren und deaktivieren
Aktion für infizierte E-Mail-Nachrichten ändern
Schutzbereich für die Komponente „Schutz vor E-Mail-Bedrohungen“

- Untersuchung zusammengesetzter Dateien, die an E-Mail-Nachrichten angehängt sind
- Filterung von E-Mail-Anlagen
- Exportieren und Importieren von Erweiterungen für die Anlagenfilterung
- E-Mail-Untersuchung in Microsoft Office Outlook
- Untersuchung von E-Mails in Thunderbird, MyOffice, R7-Office

Schutz vor Netzwerkbedrohungen

- Schutz vor Netzwerkbedrohungen aktivieren und deaktivieren
- Angreifenden Computer blockieren
- Adressen anpassen, die bei der Sperrung als Ausnahmen gelten sollen
- Liste der Sperr-Ausnahmen exportieren und importieren
- Schutz vor Netzwerkbedrohungen nach Typ konfigurieren

Firewall

- Firewall aktivieren und deaktivieren
- Typ einer Netzwerkverbindung ändern
- Arbeit mit Netzwerkregeln für Pakete
  - Eine Netzwerkpaketregel erstellen
  - Netzwerkregel für Pakete aktivieren und deaktivieren
  - Verhalten der Firewall in Bezug auf Netzwerkregeln für Pakete ändern
  - Priorität einer Netzwerkregel für Pakete ändern
  - Exportieren und Importieren von Netzwerkpaketregeln
  - Regeln für Netzwerkpakete in XML definieren
- Verwendung von Netzwerkregeln für Programme
  - Eine Netzwerkregel für das Programm erstellen
  - Netzwerkregel für Programme aktivieren und deaktivieren
  - Firewall-Aktion für die Netzwerkregel für Programme ändern
  - Priorität der Netzwerkregel für Programme ändern
- Netzwerkmonitor

Exploit-Prävention

- Exploit-Prävention aktivieren und deaktivieren
- Schutz für den Arbeitsspeicher von Systemprozessen

Verhaltensanalyse

Schutz vor Verschlüsselung

- Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren und deaktivieren
- Sperrdauer für einen nicht vertrauenswürdigen Computer konfigurieren
- Schutzbereich bearbeiten
- Vertrauenswürdige Computer für die externe Datenverschlüsselung hinzufügen
- Exportieren und Importieren einer Liste der Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern

Rollback von schädlichen Aktionen

Kaspersky Security Network

- Verwendung von Kaspersky Security Network aktivieren und deaktivieren
- Einschränkungen von Kaspersky Private Security Network
- Cloud-Modus für die Schutzkomponenten aktivieren und deaktivieren
- KSN Proxy-Einstellungen
- Reputation einer Datei in Kaspersky Security Network überprüfen

Untersuchung verschlüsselter Verbindungen
Untersuchung verschlüsselter Verbindungen aktivieren
Installation von vertrauenswürdigen Stammzertifikaten
Untersuchung von verschlüsselten Verbindungen mit einem nicht vertrauenswürdigen Zertifikat
Kaspersky-Zertifikat zum eigenen Zertifikatspeicher hinzufügen
Geschütze Verbindungen von der Untersuchung ausschließen
Blockieren des Zugriffs auf Domänen mit nicht vertrauenswürdigen Zertifikaten
Daten löschen
Kontrolle des Computers
Web-Kontrolle
Hinzufügen einer Web-Ressourcen-Zugriffsregel
Nach Adressen von Webressourcen filtern.
Nach dem Inhalt von Webressourcen filtern.
Zugriffsregeln für Webressourcen testen
Exportieren und Importieren von Regeln der „Web-Kontrolle“
Adressen von Webressourcen für eine Regel der Web-Kontrolle exportieren und importieren
Überwachung der Internetaktivitäten von Benutzern
Meldungsvorlagen für die Web-Kontrolle ändern
Regeln für das Erstellen von Adressmasken für Webressourcen
Web-Kontrolle für virtuelle Maschinen
Variablen in Nachrichtenvorlagen der Web-Kontrolle
Gerätekontrolle
Über Zugriffsregeln
Abrufen von Informationen über installierte Geräte
Zugriff auf Geräte nach Typ verwalten
Zugriff auf Geräte nach Verbindungsschnittstelle verwalten
Differenzierung von Benutzerrechten für den Zugriff auf Geräte
Zugriff auf Mobilgeräte verwalten
Zugriff auf Bluetooth-Geräte verwalten
Druckerüberwachung
Kontrolle von WLAN-Verbindungen
Überwachung der Nutzung von Wechseldatenträgern
Ändern der Cache-Dauer
Aktionen für vertrauenswürdige Geräte
Hinzufügen eines Geräts zur Liste der vertrauenswürdigen Geräte
Liste mit vertrauenswürdigen Geräten exportieren und importieren
Freigabe eines blockierten Geräts
Online-Modus für die Freigabe
Offline-Modus für die Freigabe
Meldungsvorlagen für die Gerätekontrolle ändern
Anti-Bridging
Anti-Bridging aktivieren
Status einer Verbindungsregel ändern
Priorität einer Verbindungsregel ändern
Adaptive Kontrolle von Anomalien
Training der „Adaptiven Kontrolle von Anomalien“
Regel der Adaptiven Kontrolle von Anomalien aktivieren und deaktivieren

- Aktion für den Fall, dass eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst wird, ändern
- Um eine Ausnahme für eine „Adaptive Kontrolle von Anomalien"-Regel zu löschen, gehen Sie wie folgt vor:
- Exportieren und Importieren von Ausnahmen für die Regeln der „Adaptiven Kontrolle von Anomalien"
- Updates für die Regeln der Adaptiven Kontrolle von Anomalien übernehmen
- Meldungsvorlagen für die Adaptiven Kontrolle von Anomalien ändern
- Überwachungstools der „Adaptiven Kontrolle von Anomalien"

Programmkontrolle

- Funktionelle Beschränkungen der Programmkontrolle
- Abrufen von Informationen über installierte Programme
- So aktivieren Sie den Modus „Blockierte Programme"
- Programmkontrolle auf Basis eines Baseline-Computers
- Regeln der Programmkontrolle verwalten
  - Auslösebedingung für die Regel der „Programmkontrolle" hinzufügen
  - Ausführbare Dateien aus dem Ordner „Ausführbare Dateien" zu einer Programmkategorie hinzufügen
  - Ausführbare Dateien, die mit Ereignissen zusammenhängen, zu einer Programmkategorie hinzufügen
  - Regel der Programmkontrolle hinzufügen
  - Ändern des Status einer Regel der Programmkontrolle mithilfe von Kaspersky Security Center
  - Exportieren und Importieren von Regeln der Programmkontrolle
  - Ereignisse aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle" anzeigen
  - Bericht über verbotene Programme anzeigen
- Regeln der Programmkontrolle testen
  - Prüfung von Regeln der „Programmkontrolle" aktivieren und deaktivieren
  - Bericht über im Testmodus verbotene Programme anzeigen
  - Ereignisse aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle" anzeigen
- Aktivitätsmonitor für Programme
- Regeln für das Erstellen von Masken für Datei- oder Ordnernamen
- Meldungsvorlagen für die Programmkontrolle ändern
- Variablen in Nachrichtenvorlagen der Programmkontrolle
- Bewährte Methoden für die Inventarisierung ausführbarer Dateien
- Bewährte Praktiken für die Implementierung einer Liste zulässiger Programme
  - Konfigurieren des Allowlist-Modus für Programme
  - Testen des Allowlist-Modus
  - Unterstützung für den Allowlist-Modus

Kontrolle von Netzwerkports

- Kontrolle aller Netzwerkports aktivieren
- Liste der zu kontrollierenden Netzwerkports erstellen
- Liste der Programme erstellen, für die alle Netzwerkports überwacht werden
- Exportieren und Importieren von Listen überwachter Ports

Protokollanalyse

- Vordefinierte Regeln konfigurieren
- Benutzerdefinierte Regeln hinzufügen

Überwachung der Systemintegrität

- Über Regeln für die Überwachung der Systemintegrität
- Echtzeitüberwachung der Systemintegrität
- Prüfung der Systemintegrität auf Befehl
- Regeln für die Überwachung der Systemintegrität exportieren und importieren

Berichte zur Überwachung der Systemintegrität anzeigen
Status der Systemintegrität zurücksetzen
Cloud Discovery
Vertrauenswürdige Zone
Erstellung von Untersuchungsausnahmen
Eine Ausnahme nach dem Typ der gefundenen Objekte erstellen
Liste mit vertrauenswürdigen Programmen erstellen
Lokale vertrauenswürdige Zone erstellen
Vertrauenswürdige Zone exportieren und importieren
Umgang mit Programmen, die eine vertrauenswürdige digitale Signatur besitzen
Anhang. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme
Microsoft SQL Server
Microsoft Exchange Server
Microsoft System Center Configuration Manager
Citrix
VMware
Datendeduplizierung in Microsoft Windows Server
Arbeit mit dem Backup
Maximale Speicherdauer für Dateien im Backup anpassen
Maximale Größe für das Backup anpassen
Dateien aus dem Backup wiederherstellen
Backup-Kopien von Dateien aus dem Backup löschen
Benachrichtigungsdienst
Einstellungen der Ereignisberichte anpassen
Anzeige und Versand von Benachrichtigungen anpassen
Anzeige von Warnungen über den Programmstatus im Infobereich anpassen
Nachrichtenaustausch zwischen Benutzer und Administrator
Arbeit mit Berichten
Berichte anzeigen
Maximale Speicherdauer für Berichte anpassen
Maximale Größe der Berichtsdatei anpassen
Bericht in Datei speichern
Berichte löschen
Selbstschutz für Kaspersky Endpoint Security
Selbstschutz-Mechanismus aktivieren und deaktivieren
Aktivierung und Deaktivierung der AM-PPL-Unterstützung
Schutz der App-Dienste vor externer Steuerung
Gewährleistung der Funktion von Programmen für Remote-Administration
Kennwortschutz
Kennwortschutz aktivieren
Berechtigungen für bestimmte Benutzer oder Gruppen gewähren
Verwenden eines temporären Kennworts, um Berechtigungen zu gewähren
Temporäres Kennwort widerrufen
Besonderheiten der Berechtigungen für den Kennwortschutz
KLAdmin-Kennwort zurücksetzen
Schutz der Verbindung zum Administrationsserver

Virtuelle Datentresore
Beschränkungen der Verschlüsselungsfunktionalität
Änderung der Länge des Chiffrierschlüssels (AES56 / AES256)
Kaspersky-Festplattenverschlüsselung
Besondere Merkmale der SSD-Laufwerksverschlüsselung
Kaspersky-Festplattenverschlüsselung starten
Liste mit Festplatten erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen
Exportieren und Importieren einer Liste von Festplatten, die von der Verschlüsselung ausgenommen wurden
Verwendung der Technologie zur Einmalanmeldung (SSO) aktivieren
Authentifizierungsagenten-Konten verwalten
Verwendung eines Tokens oder einer Smartcard bei der Arbeit mit dem Authentifizierungsagenten
Entschlüsselung von Festplatten
Wiederherstellen des Zugriffs auf einen Datenträger, der mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist
Anmeldung mit dem Authentifizierungsagenten-Dienstkonto
Update des Betriebssystems
Behebung von Fehlern beim Upgrade der Verschlüsselungsfunktionalität
Ablaufverfolgung des Authentifizierungsagenten
Hilfetexte für den Authentifizierungsagenten ändern
Objekte und Daten löschen, die nach dem Testlauf des Authentifizierungsagenten verblieben sind
Verwaltung von BitLocker
Start der „BitLocker-Laufwerkverschlüsselung"
Entschlüsselung einer Festplatte, die mit BitLocker geschützt ist
Wiederherstellen des Zugriffs auf einen Datenträger, der mit BitLocker geschützt ist
Anhalten des BitLocker-Schutzes für ein Software-Update
Dateiverschlüsselung auf lokalen Festplatten des Computers
Dateiverschlüsselung auf lokalen Festplatten des Computers starten
Programmzugriffsrechte für verschlüsselte Dateien formulieren
Verschlüsselung von Dateien, die von bestimmten Programmen erstellt und geändert werden
Entschlüsselungsregel erstellen
Dateientschlüsselung auf lokalen Festplatten des Computers
Verschlüsselte Archive erstellen
Wiederherstellen des Zugriffs auf verschlüsselte Dateien
Zugriff auf verschlüsselte Daten beim Ausfall des Betriebssystems wiederherstellen
Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anpassen
Wechseldatenträger verschlüsseln
Verschlüsselung von Wechseldatenträgern starten
Verschlüsselungsregel für Wechseldatenträger hinzufügen
Exportieren und Importieren einer Liste von Verschlüsselungsregeln für Wechseldatenträger
Portabler Modus für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern
Wechseldatenträger entschlüsseln
Informationen zur Datenverschlüsselung anzeigen
Verschlüsselungsstatus anzeigen
Verschlüsselungsstatistik in den Informationsbereichen von Kaspersky Security Center anzeigen
Fehler anzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten
Bericht über die Datenverschlüsselung anzeigen

Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht
Datenwiederherstellung mithilfe des Reparatur-Tools FDERT
Notfall-CD erstellen
„Detection and Response"-Lösungen
Lizenzverwaltung für MDR und EDR Optimum
Kompatibilität mit Drittanbieter-EDR-Lösungen
Kaspersky Endpoint Agent
Migration der Konfiguration [KES+KEA] zur Konfiguration [KES+built-in agent]
Migration von Richtlinien und Aufgaben für Kaspersky Endpoint Agent
Endpoint Detection and Response Agent (EDR Agent)
EDR Agent installieren
Integration von EDR Agent in MDR
Integration von EDR Agent in EDR (KATA)
Integration von EDR Agent in NDR (KATA)
Integration von EDR Agent in EDR Expert (on-premises)
Kompatibilität mit Drittanbieter-EPP-Anwendungen
Managed Detection and Response
Integration des integrierten Agenten in MDR
Leitfaden zur Migration von KEA zu KES für MDR
Endpoint Detection and Response
Integration des integrierten Agenten in EDR Optimum / EDR Expert
Untersuchung auf Kompromittierungsindikatoren (Standardaufgabe)
Erweiterte Telemetrie für die IOC-Untersuchung
Datei in die Quarantäne verschieben
Datei anfordern
Datei löschen
Prozess-Start
Prozess beenden
Ausführungsprävention
Isolation des Computernetzwerks
Cloud Sandbox
Leitfaden zur Migration von KEA zu KES für EDR Optimum
Kaspersky Sandbox
Integration des integrierten Agenten in Kaspersky Sandbox
Untersuchung auf Kompromittierungsindikatoren (eigenständige Aufgabe)
Leitfaden zur Migration von KEA zu KES für Kaspersky Sandbox
Kaspersky Anti Targeted Attack Platform
Integration des integrierten Agenten in EDR / NDR (KATA)
EDR-Telemetrie (KATA) konfigurieren
Ausnahmen für die EDR (KATA)-Telemetrie
Beispiel 1. Ausgeschlossene Prozesse
Beispiel 2. Ausgeschlossene Netzwerkkommunikationen
Beispiel 3. Ausgeschlossene Dateivorgänge
Beispiel 4. Ausgeschlossene Registrierungsänderungen

KATA Sandbox
Integration des integrierten Agenten in KATA Sandbox
Konfigurieren von Aktionen zur Reaktion auf Bedrohungen
Leitfaden für die Migration von KEA zu KES, für EDR (KATA)
Endpoint Detection and Response Expert (on-premises)
Integration des integrierten Agenten in EDR Expert (on-premises)
Telemetrie-Einstellungen für EDR Expert (on-premises) konfigurieren
Telemetrie-Ausnahmen für EDR Expert (on-premises)
Ereignisfilter für EDR Expert (on-premises) exportieren und importieren
Besonderheiten bei der Verwendung von Richtlinienprofilen zur Konfiguration der Integration mit EDR Expert (on-premises) und EDR (KATA)
Endpoint Detection and Response Expert (cloud)
Integration des integrierten Agenten in EDR Expert (cloud)
Telemetrie-Einstellungen für EDR Expert (cloud) konfigurieren
Telemetrie-Ausnahmen für EDR Expert (cloud)
So exportieren oder importieren Sie Ereignisfilter für EDR Expert (cloud)
Verwalten der Quarantäne
Konfigurieren der maximalen Quarantäne-Größe
Senden von Daten über Quarantäne-Dateien an Kaspersky Security Center
Wiederherstellen von Dateien aus der Quarantäne
Überwachung von EDR-Aktionen
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Integration von Kaspersky Endpoint Security in KUMA
Vorbereitung auf die Integration von KES mit KUMA
Verbinden von KES mit KUMA
Filterung von Ereignissen, die an KUMA gesendet werden sollen
Filter für KUMA-Ereignisse exportieren und importieren
Leitfaden zur Migration von KSWS zu KES
Entsprechung von KSWS- und KES-Komponenten
Entsprechung von KSWS- und KES-Einstellungen
Migration von KSWS-Komponenten
Migration von KSWS-Aufgaben und -Richtlinien
Migration der vertrauenswürdigen Zone für KSWS
Regeln für die KSWS-Kontrolle des Programmstarts migrieren
Installation von KES anstelle von KSWS
Migration der Konfiguration [KSWS+KEA] zur Konfiguration [KES+built-in agent]
Überprüfen, ob Kaspersky Security für Windows Server erfolgreich entfernt wurde
Aktivieren von KES mit einem KSWS-Schlüssel
Spezielle Aspekte für die Migration von Servern mit hoher Auslastung
Verwaltung der App auf einem Server im Server Core-Modus
Migration von [KSWS+KEA] zu [KES+built-in agent]
Light Agent-Modus zum Schutz virtueller Maschinen
Besonderheiten für den Light Agent-Modus
Vorherige Konfiguration der virtuellen Maschine
Kompatibilität mit der Citrix App Layering-Technologie
Kompatibilität mit der Citrix Provisioning-Technologie (Citrix Provisioning Services)
Kompatibilität mit der Omnissa App Volumes-Technologie

Light Agent installieren
Über die Verbindung des Light Agents zur SVM
SVM-Ermittlung
Algorithmus der SVM-Auswahl für Light Agent konfigurieren
Verbindungen der Light Agents auf SVMs verteilen (Tags)
Schutz der Verbindung zwischen Light Agent und SVM
Light Agent aktivieren
Leitfaden zur Migration von KSVLA Light Agent zu KES Light Agent
Installation von KES Light Agent anstelle von KSVLA Light Agent
Entsprechung der Komponenten von KSVLA Light Agent und KES Light Agent
Migration der Aufgaben und Richtlinien von KSVLA Light Agent
Migration der Konfiguration [KSVLA Light Agent+KEA] zur Konfiguration [KES Light Agent+built-in agent]
Programm über die Befehlszeile verwalten
Setup. Programm installieren
Setup /x. Die App entfernen
msiexec /i. Programm wiederherstellen
AVP-Befehle
SCAN. Schadsoftware-Untersuchung
UPDATE. Update der Datenbanken und Programm-Module
ROLLBACK. Rollback des letzten Updates
TRACES. Protokollierung
START. Ein Profil starten
STOP. Profil beenden
STATUS. Status des Profils
STATISTICS. Ausführungsstatistik für das Profil
RESTORE. Dateien aus dem Backup wiederherstellen
EXPORT. Programmeinstellungen exportieren
IMPORT. Programmeinstellungen importieren
ADDKEY. Schlüsseldatei übernehmen
LICENSE. Lizenzverwaltung
RENEW. Lizenz kaufen
PBATESTRESET. Untersuchungsergebnisse vor der Datenträgerverschlüsselung zurücksetzen
EXIT. Programm beenden
EXITPOLICY. Richtlinie deaktivieren.
STARTPOLICY. Richtlinie aktivieren
DISABLE. Schutz deaktivieren
SPYWARE. Spyware erkennen
KSN. Zwischen KSN / KPSN umschalten
SERVERBINDINGDISABLE. Den Schutz der Serververbindung deaktivieren
KESCLI-Befehle
Scan. Schadsoftware-Untersuchung
GetScanState. Abschluss-Status der Untersuchung
GetLastScanTime. Abschlusszeit der Untersuchung festlegen
GetThreats. Daten über erkannte Bedrohungen abrufen
UpdateDefinitions. Update der Datenbanken und Programm-Module
GetDefinitionState. Zeitpunkt (Datum und Uhrzeit) des letzten Datenbanken-Updates ermitteln
EnableRTP. Schutz aktivieren

GetRealTimeProtectionState. Status des „Schutzes vor bedrohlichen Dateien“
GetEncryptionState. Status der Festplattenverschlüsselung
Version. Anwendungsversion ermitteln
Befehle zur Verwaltung von „Detection and Response“
SANDBOX. Verwaltung von „Sandbox“
PREVENTION. Verwaltung der Ausführungsprävention
ISOLATION. Verwalten der Netzwerkisolation
RESTORE. Wiederherstellen von Dateien aus der Quarantäne
IOCSCAN. Untersuchung auf Kompromittierungsindikatoren (IOC)
MDRLICENSE. MDR-Aktivierung
EDRKATA. EDR (KATA)-Integration
EDRExpertOnPrem. Integration von EDR Expert (on-premises)
KUMA. KUMA-Integration
YARA. YARA-Untersuchung ausführen
TELEMETRIE-FILTER. Filterung von Ereignissen, die an KUMA gesendet werden sollen
Befehle zur Verwaltung von Light Agent
KSVLAINFO. Light Agent-Modus bestimmen
VIISINFO. Status der Verbindung des Light Agent zum Integrationsserver
SVMINFO. Status der Verbindung von Light Agent zum Schutzserver
Fehlercodes
Anhang. Programmprofile
Programmverwaltung über eine REST API
Programminstallation mit einer REST API
Verwendung einer API
Informationsquellen zum Programm
Kontaktaufnahme mit dem Technischen Support
Über die Zusammensetzung und Speicherung von Protokolldateien
Anwendungsnachverfolgung
Überwachung der Programmleistung
Aufzeichnung von Dump-Dateien
Schutz von Dump- und Protokolldateien
Betriebssystemdaten abrufen (Kaspersky Get System Info)
Einschränkungen und Warnungen
Glossar
Administrationsagent
Administrationsgruppe
Aktiver Schlüssel
Antiviren-Datenbanken
Archiv
Aufgabe
Authentifizierungsagent
Cloud Discovery
Datenbank für bösartige Webadressen
Datenbank für Phishing-Webadressen
Desinfektion von Objekten
Fehlalarm
Infizierte Datei

Integrationsserver
IOC
IOC-Datei
Kerberos-Authentifizierung
Light Agent
Lizenzzertifikat
Maske
Normalisierte Form der Adresse einer Webressource
OLE-Objekt
OpenIOC
Portabler Dateimanager
Potenziell infizierbare Datei
Schutzbereich
SVM
Trusted Platform Module
Untersuchungsbereich
Zertifikataussteller
Anhänge
Anhang 1. Programmeinstellungen
Schutz vor bedrohlichen Dateien
Schutz vor Web-Bedrohungen
Schutz vor E-Mail-Bedrohungen
Schutz vor Netzwerkbedrohungen
Firewall
Schutz vor modifizierten USB-Geräten
AMSI-Schutz
Exploit-Prävention
Verhaltensanalyse
Programm-Überwachung
Rollback von schädlichen Aktionen
Kaspersky Security Network
Protokollanalyse
Schutz vor Verschlüsselung
Web-Kontrolle
Gerätekontrolle
Programmkontrolle
Adaptive Kontrolle von Anomalien
Überwachung der Systemintegrität
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
KUMA-Integration
Vollständige Festplattenverschlüsselung
Verschlüsselung von Dateien

Wechseldatenträger verschlüsseln
Vorlagen (Datenverschlüsselung)
Ausnahmen
Programmeinstellungen
Berichte und Speicher
Netzwerkeinstellungen
Benutzeroberfläche
Einstellungen verwalten
Update der Datenbanken und Programm-Module
Anhang 2. Sicherheitsgruppen für Programme
Anhang 3. Dateierweiterungen für die schnelle Untersuchung von Wechseldatenträgern
Anhang 4. Dateitypen für die Anlagenfilterung im „Schutz vor E-Mail-Bedrohungen"
Anhang 5. Netzwerkeinstellungen für die Interaktion mit externen Diensten
Anhang 6. Programmereignisse
Kritisch
Funktionsstörung
Warnung
Informative Meldung
Anhang 7. Unterstützte Dateierweiterungen für die Ausführungsverhinderung
Anhang 8. Unterstützte Skript-Interpreter für die Ausführungsprävention
Anhang 9. IOC-Untersuchungsbereich in der Registrierung (RegistryItem)
Anhang 10. Anforderungen für IOC-Dateien
Anhang 11. API für EDR Threat Response
Anhang 12. Benutzerkonten in Regeln für App-Komponenten
Rechtliche Informationen
Bereitstellung von Daten
Bereitstellung von Daten im Rahmen des Endbenutzer-Lizenzvertrags
Datenbereitstellung bei der Verwendung von Kaspersky Security Network
Bereitstellung von Daten beim Einsatz der Lösungen von Detection and Response
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
Integration in Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Einhaltung der Gesetzgebung der Europäischen Union (DSGVO)
Markenrechtliche Hinweise
Informationen über den Code von Drittherstellern

Hilfe zu Kaspersky Endpoint Security für Windows

Neuerungen in Version 14.2

Unterstützung für die tokenbasierte Authentifizierung beim Kennwortschutz wurde hinzugefügt.

Neuerungen in den einzelnen Versionen von Kaspersky Endpoint Security für Windows

Erste Schritte

Bereitstellung von Kaspersky Endpoint Security für Windows

Erstkonfiguration von Kaspersky Endpoint Security für Windows

Lizenzierung von Kaspersky Endpoint Security für Windows

Bereitstellung von Daten

Im Rahmen des Endbenutzer-Lizenzvertrags

Bei Nutzung von KSN

DSGVO

Beseitigung von Bedrohungen

Auf Arbeitsstationen

Auf Servern

Reaktion auf die Erkennung eines Kompromittierungsindikators (Netzwerkisolation → Quarantäne → Ausführungsprävention)

Bewährte Methoden

Optimierung der Programmleistung

Implementieren des Default Deny-Modus in der Programmkontrolle

Migration von KEA zu KES mit integriertem Agenten

Verwendung von KES als Teil anderer Lösungen

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

Neuerungen

Update 14.2

Kaspersky Endpoint Security 14.2 für Windows bietet die folgenden neuen Funktionen und Verbesserungen:

1. Der Satz der standardmäßig installierten Komponenten wurde geändert. Die Standardkonfiguration des Programms umfasst jetzt den Schutz vor BadUSB-Angriffen, die BitLocker-Verwaltung und den integrierten EDR Optimum-Agenten.

2. Unterstützung für die tokenbasierte Authentifizierung (Kennwortschutz) wurde hinzugefügt. Für den Zugriff auf das Programm können Sie jetzt entweder Ihren Benutzernamen und Ihr Kennwort, ein vom Administrator ausgegebenes temporäres Kennwort oder ein Token verwenden. Die tokenbasierte Authentifizierung kann beispielsweise für Dienstbenutzerkonten verwendet werden, für die kein Kennwort erforderlich ist.

3. Ein neues Kriterium für die Kennwortstärke in BitLocker wurde hinzugefügt: die Prüfung des Kennwortverlaufs. Das Programm verhindert, dass Benutzer ein Kennwort festlegen, das sie bereits zuvor verwendet haben.

4. Unterstützung für das Ändern der Sprache der Benutzeroberfläche von Kaspersky Endpoint Security beim Aktualisieren des Programms mithilfe der Aufgabe *Programm remote installieren* wurde hinzugefügt. Wenn Sie die falsche Sprache für die Benutzeroberfläche ausgewählt haben, müssen Sie das Programm jetzt nicht mehr neu installieren.

5. Neue Telemetrieereignisse für Benutzer von Kaspersky Endpoint Detection and Response-Lösungen hinzugefügt: GPO-Änderung, Nicht übereinstimmende lokale SCCM-Konfiguration, SCCM-Konfigurationsänderung, SCCM-Bereitstellungsaufgabe, SMB-Verbindung geöffnet. Diese neuen Ereignisse verbessern die Funktionen zur Bedrohungserkennung der EDR-Lösungen.

6. Für Benutzer von Kaspersky Endpoint Detection and Response Expert (on-premises) wurde die neue Bedrohungsreaktion *Datei platzieren* hinzugefügt. Mit dieser Aufgabe können Sie Konfigurationsdateien, Skripte zur Bedrohungsreaktion, Dienstprogramme zur Minderung der Auswirkungen von Angriffen usw. auf Computer übertragen. Die Aufgabe *Datei platzieren* ist in der OSMP-Konsole verfügbar, wenn Kaspersky EDR Expert (On-Premise) Version 9.0 bereitgestellt ist.

7. Das Verhalten von Bedrohungsreaktionen für Benutzer von Kaspersky Endpoint Detection and Response Optimum wurde verbessert. Vor der Ausführung einer Aktion (*Datei löschen*, *Datei in die Quarantäne verschieben* oder *Ausführungsprävention*) prüft das Programm jetzt, ob das Objekt als systemkritisch eingestuft ist (systemkritisches Objekt, SCO), und warnt vor möglichen Auswirkungen auf die Systemstabilität. Es wird nicht empfohlen, diese Aktionen auf Dateien des Typs „System Critical Object“ (SCO) anzuwenden.

8. Unterstützung für den Betrieb des Programms als Teil eines Hochverfügbarkeitsclusters von Integrationsservern wurde für Benutzer von Kaspersky Security for Virtualization Light Agent hinzugefügt. Ein Hochverfügbarkeitscluster aus Integrationsservern gewährleistet den unterbrechungsfreien Schutz der virtuellen Umgebung, da SVMs und Light Agents beim Ausfall des primären Integrationsservers auf einen Backup-Integrationsserver umgeschaltet werden.

9. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security haben wir die Änderungen berücksichtigt, die in den folgenden privaten Patches enthalten sind: PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF22065, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF23095, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF24037, PF24043, PF24048, PF25013, PF25016, PF25019, PF25030.

Update 14.1

Kaspersky Endpoint Security 14.1 für Windows bietet die folgenden neuen Funktionen und Verbesserungen:

1. Die Unterstützung für das Betriebssystem Windows Server 2025 wurde hinzugefügt.

2. Die maximal zulässige Anzahl der Filterregeln für Telemetrie-Ereignisse für Endpoint Detection and Response Expert (on-premises) und Kaspersky Endpoint Detection and Response Expert (cloud) wurde erhöht. Kaspersky Endpoint Security unterstützt jetzt insgesamt bis zu 10.000 inklusive und exklusive Filterregeln.

3. Sie können jetzt Aufgaben so konfigurieren, dass sie nur an bestimmten Wochentagen und in einem festgelegten Abstand von Wochen ausgeführt werden. Der Zeitplan ist in Kaspersky Security Center 16.1 oder höher verfügbar.

4. Für die Aufgabe *Schadsoftware-Untersuchung* können Sie jetzt einen Zeitraum angeben, in dem die Aufgabe angehalten werden soll. Dadurch können beispielsweise die Auswirkungen auf die Computerleistung bei erhöhter Auslastung minimiert werden.

5. Die Leistung des Festplatten-Subsystems auf dem geschützten Computer wurde optimiert. Dazu wurde die Anzahl der E/A-Vorgänge reduziert.

6. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security haben wir die Änderungen berücksichtigt, die in den folgenden privaten Patches enthalten sind: PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF14071, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF18057, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF20081, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF21062, PF21063, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF22059, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF23063, PF24005, PF24011, PF24013, PF24014, PF24017, PF24019, PF25013, PF25016, PF25019.

Update 14.0

Kaspersky Endpoint Security 14.0 für Windows bietet die folgenden neuen Funktionen und Verbesserungen:

1. Arm-basierte Computer werden jetzt unterstützt. Sie können das Programm entweder im Standardmodus oder im EDR Agent-Modus installieren. Das Programm weist jedoch einige Einschränkungen auf (z. B. wird nur die BitLocker-Datenverschlüsselungstechnologie unterstützt).

2. In Kaspersky Security Center Web Console Version 15.0 oder höher wird die erweiterte Richtlinienüberwachung unterstützt. Jetzt können Sie Richtlinienrevisionen ansehen und in einer Datei speichern. Eine *Revision* ist eine Auswahl geänderter Parameter, die vom Benutzer gespeichert wurden. Anhand von Revisionen können Sie Änderungen an Richtlinienparametern vergleichen und rückgängig machen.

3. Benutzern von Kaspersky Endpoint Detection and Response stehen jetzt neue Telemetrie-Ereignisse zur Verfügung. Diese neuen Ereignisse verbessern die Funktionen zur Bedrohungserkennung mithilfe von Kaspersky-EDR-Lösungen.

4. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen berücksichtigt, die in den folgenden privaten Patches enthalten sind: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Update 12.12

Kaspersky Endpoint Security 12.12 für Windows bietet die folgenden neuen Funktionen und Verbesserungen:

1. Der Schutz vor der externen Verschlüsselung freigegebener Ordner, der bisher Teil der Komponente „Verhaltensanalyse“ war, wird jetzt von der separaten Komponente Schutz vor Verschlüsselung übernommen.

2. Die Unterstützung für das Kerberos-Protokoll wurde hinzugefügt. Dies dient der Authentifizierung des Programms, damit es über einen Proxyserver auf das Internet zugreifen kann.

3. Jetzt können Sie einen Datei-Hash für ein vertrauenswürdiges Programm angeben (zuvor war nur ein vollständiger Pfad möglich).

4. Benutzern von Endpoint Detection and Response (EDR)-Lösungen stehen jetzt mehr Funktionen für die Aufgabe *IOC-Untersuchung* zur Verfügung. Jetzt ist die Funktionalität Retrospektive IOC-Untersuchung verfügbar. Die *retrospektive IOC-Untersuchung* ist ein Modus der Aufgabe *IOC-Untersuchung*. Dabei sucht Kaspersky Endpoint Security innerhalb eines bestimmten Zeitraums nach Kompromittierungsindikatoren. In diesem Modus können in den Daten über die Netzwerkaktivität des Computers Kompromittierungsindikatoren erkannt werden. Kaspersky Endpoint Security analysiert Daten aus den Protokollen des Betriebssystems und des Browsers auf dem Computer.

5. Benutzer von Kaspersky Endpoint Detection and Response (EDR) können die Größenbeschränkung der Quarantäne deaktivieren. Dies kann für die YARA-Untersuchung erforderlich sein, bei der das Programm möglicherweise eine große Speicherabbilddatei speichert. Jetzt können Sie Ihren gesamten freien Speicherplatz für die Quarantäne verwenden.

6. Jetzt wird die HTTPS-Komprimierung unterstützt, um den Export von Ereignissen nach Kaspersky Unified Monitoring and Analysis Platform (KUMA) zu optimieren. Dadurch wird der ausgehende Datenverkehr reduziert.

7. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen berücksichtigt, die in den folgenden privaten Patches enthalten sind: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF17060, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF19065, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF20078, PF20080, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF21040, PF21058, PF22004, PF22008, PF22014, PF22027, PF22036, PF22049, PF22053, PF22056, PF23022, PF23026, PF23029, PF23031, PF23039, PF23049, PF24005, PF24011.

Update 12.11

Kaspersky Endpoint Security 12.11 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Das Programm überprüft die Konfiguration der Kontrollkomponenten, bevor die Einstellungen gespeichert werden. Die Überprüfung wurde für die Komponenten Programmkontrolle, Gerätekontrolle und Überwachung der Systemintegrität hinzugefügt. Das Programm zeigt jetzt eine Warnung an, wenn die aktuellen Einstellungen der Kontrollkomponente die Auslastung des Computers erhöhen oder zu Systemausfällen führen können. Ein Beispiel für die Programmkontrolle: Wenn Sie den Modus ausgewählt haben, in dem alle Programme außer den erlaubten blockiert werden, und keine Erlaubnisregel hinzugefügt wurde, zeigt das Programm eine Warnung an, da eine solche Konfiguration zu Systemfehlern führen kann.

2. Die Unterstützung für die automatische Übermittlung von Dateien zur Untersuchung an KATA Sandbox wurde hinzugefügt. *KATA Sandbox* ist eine Komponente von Kaspersky Anti Targeted Attack Platform, die Dateien auf virtuellen Betriebssystem-Images ausführt. „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). Damit KATA Sandbox im automatischen Modus funktioniert, muss Kaspersky Anti Targeted Attack Platform 8.0 oder höher bereitgestellt werden.

3. Das Senden von EDR-Telemetrie wurde optimiert. Jetzt können Sie die maximale Paketlänge angeben.

4. Die Diagnose der Verbindung zu Kaspersky Security Network wurde verbessert. Die Details zu Verbindungsfehlern für Kaspersky Security Network wurden erweitert, um potenzielle Probleme zu beheben.

5. Die Unterstützung für die Konfiguration von Ereignislisten, die an Kaspersky Unified Monitoring and Analysis Platform (KUMA) gesendet werden, wurde hinzugefügt. Zusätzlich zu den vordefinierten Ereignislisten können Sie in KUMA jetzt Ereignisse manuell zur Telemetrie hinzufügen oder Ereignisse nach ihrer ID im Windows-Ereignisprotokoll ausschließen.

6. Die Richtlinienoberfläche in der Web Console wurde aktualisiert. Das Layout der Richtlinienabschnitte wurde geändert, um einen schnelleren Zugriff auf wichtige Funktionen zu ermöglichen.

7. Unterstützung für Windows 11 25H2.

8. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen berücksichtigt, die in den folgenden privaten Patches enthalten sind: PF13115, PF13118, PF13119, PF13120, PF13123, PF13124, PF14061, PF14062, PF14064, PF14065, PF14069, PF14070, PF15054, PF15056, PF15058, PF15062, PF15063, PF15064, PF16052, PF16053, PF16055, PF16056, PF16057, PF16060, PF16061, PF16062, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF17051, PF17053, PF17054, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF18050, PF18051, PF18053, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF19051, PF19055, PF19056, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF20052, PF20055, PF20060, PF20065, PF21007, PF21010, PF21019, PF21021, PF21024, PF21026, PF22004, PF22008, PF22014.

Update 12.10

Kaspersky Endpoint Security 12.10 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Neue Option für die Komponente „Schutz vor modifizierten USB-Geräten“: Barcode-Scanner können autorisiert werden, indem ein Strichcode vom Bildschirm abgescannt wird. Jetzt müssen Sie keinen Code mehr über die Bildschirmtastatur eingeben, um Barcode-Scanner zu autorisieren.

2. Die folgenden Funktionen und Verbesserungen stehen Benutzern der Endpoint Detection and Response-Lösungen (EDR) von Kaspersky zur Verfügung:

   - Jetzt können Sie die Netzwerkisolation des Computers in den Warnungsdetails verwalten. Außerdem können Sie in den Warnungsdetails den Zeitraum für die Netzwerkisolation des Computers angeben und Ausnahmen hinzufügen.

   - Neue Daten in den Warnungsdetails. Die Warnungsdetails enthalten jetzt mehr Informationen über die Bedrohung. Dazu gehören auch Angaben zum Verhaltens des Programms bei der Reaktion auf EDR-Bedrohungen.

   - Die Verarbeitung von IOC-Dateien wurde verbessert. Jetzt können Sie den Inhalt von IOC-Dateien auf der Benutzeroberfläche von Kaspersky Security Center Web Console anzeigen und bearbeiten. Nachdem eine IOC-Datei geladen wurde zeigt das Programm einen Bericht über die Anwendung von IOC-Ausdrücken an.

   - Die Reaktion auf erkannte IOCs wurde optimiert. Dateien, die mit der Aufgabe *IOC-Untersuchung* gefunden wurden, können jetzt direkt in die Quarantäne verschoben werden (über die IOC-Erkennungsergebnisse in den Aufgabeneigenschaften). Außerdem können Sie Computer über die Aufgabeneigenschaften vom Netzwerk isolieren.

   - Jetzt können Sie IOC-Dateien direkt in den Eigenschaften der Aufgabe *IOC-Untersuchung* erstellen und dabei Listen mit Datei-Hashs, IP-Adressen oder DNS-Namen verwenden, die in einer txt-Datei generiert wurden.

   - Erweiterter Untersuchungsbereich für die Aufgabe *IOC-Untersuchung*. Jetzt können Sie einen Bereich für die IOC-Untersuchung der Registrierung festlegen (**Windows-Registrierung – Registryltem**). In früheren Versionen des Programms konnte nur ein vordefinierter IOC-Untersuchungsbereich für die Registrierung verwendet werden.

3. Eine neue Berechtigung für den Kennwortschutz wurde hinzugefügt: *Einstellungen exportieren*. Standardmäßig kann in der Programmoberfläche nur der Benutzer KLAdmin eine Konfigurationsdatei mit Einstellungen von Kaspersky Endpoint Security erstellen. Um anderen Benutzern Zugriff zu gewähren, müssen Sie ihnen eine entsprechende Berechtigung erteilen.

4. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen berücksichtigt, die in den folgenden privaten Patches enthalten sind: PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF13120, PF13123, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF15062, PF16052, PF16053, PF16055, PF16056, PF16057, PF17027, PF17029, PF17039, PF17041, PF17043, PF17048, PF17050, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF18031, PF18032, PF18043, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF19043, PF19049, PF20011, PF20016, PF20017, PF20020, PF20021, PF20033, PF20036, PF20038, PF20039, PF20049, PF21007.

Update 12.9

Kaspersky Endpoint Security 12.9 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Eine neue Funktionalität zur *Verwaltung temporärer Kennwörter* wurde hinzugefügt. Mit einem temporären Kennwort können Sie den Zugriff auf Kaspersky Endpoint Security für einen separaten Computer gewähren, wenn der Kennwortschutz aktiviert ist. Die Verwaltung temporärer Kennwörter bietet folgende Möglichkeiten: Kennwortverlauf speichern (bis zu 30 Tage), Status des temporären Kennworts überwachen (*Aktiv*, *Abgelaufen*, *Gesperrt*) und temporäre Kennwörter widerrufen.

2. Neue Option: Die Verbindung zu Webressourcen, die durch Regeln der Web-Kontrolle verboten sind, kann sofort nach dem Anwenden der Richtlinie getrennt werden. In früheren Programmversionen beschränkte die Web-Kontrolle nur neue Verbindungen zu verbotenen Webressourcen.

3. Neue Option für Benutzer von Kaspersky Anti Targeted Attack Platform: Auf dem Computer kann lokal eine YARA-Untersuchung ausgeführt werden. Dazu müssen Sie eine Datei mit YARA-Regeln herunterladen und den Befehl in der Befehlszeile ausführen.

4. Das Programm reagiert nun anders, wenn BitLocker auf Computern aktiviert wird, auf denen Laufwerke bereits mithilfe von Drittanbieter-Tools durch BitLocker geschützt sind. Kaspersky Endpoint Security initiiert den Wiederherstellungsvorgang, um den Wiederherstellungsschlüssel an Kaspersky Security Center zu senden. Dadurch wird die BitLocker-Verwaltung an die Kaspersky Security Center-Konsole übertragen.

5. Den Benutzern der Detection and Response-Lösungen von Kaspersky steht der neue Abschnitt **Reaktionsverlauf** zur Verfügung. Dieser Abschnitt enthält Informationen zu Aktionen, die zur Reaktion auf Bedrohungen auf dem Computer ausgeführt werden. Zu diesen Aktionen gehören beispielsweise das Ausführen der Aufgabe *Prozess beenden* oder die Isolierung des Computers vom Netzwerk. Der Reaktionsverlauf ist nur für Benutzer der folgenden Kaspersky-Lösungen verfügbar: MDR, EDR, KATA.

6. Für Benutzer von Kaspersky Unified Monitoring and Analysis Platform werden jetzt EDR-Aktionen zur Reaktion auf Bedrohungen unterstützt. Bei der Reaktion auf Bedrohungen führt KUMA Skripte aus, die entsprechende EDR-Aufgaben erstellen. Um EDR-Aufgaben auszuführen, müssen Sie in der KUMA-Konsole eine Reaktionsregel für das benutzerdefinierte Skript erstellen und Ereignisse auswählen.

7. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen der folgenden privaten Patches berücksichtigt: PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018, PF19017, PF19032, PF19034, PF19036, PF19037, PF19041, PF20011, PF20016, PF20017, PF20020, PF20021.

Update 12.8

Kaspersky Endpoint Security 12.8 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Das Programm unterstützt jetzt den Light Agent-Modus zum Schutz virtueller Umgebungen. Jetzt können Sie das Programm als Light Agent im Rahmen der Lösung Kaspersky Security for Virtualization Light Agent 6.2 bereitstellen.

2. Das Abfangen von Dateivorgängen in Docker-Containern auf Servern wird jetzt unterstützt. Ein *Container* ist eine isolierte Umgebung, in der ein Programm ohne direkte Interaktion mit dem Betriebssystem ausgeführt werden kann. Kaspersky Endpoint Security untersucht die Dateien in den Containern, auf die der Benutzer Zugriff erhält. Wird eine Bedrohung erkannt, blockiert die App diese bösartige Aktivität und versucht, die Datei im Container zu desinfizieren. Wenn die Datei nicht desinfiziert werden kann, sperrt die App den Container.

3. Jetzt können Sie einen Schutzbereich für den Schutz vor der externen Verschlüsselung freigegebener Ordner festlegen (Komponente Verhaltensanalyse). Jetzt können Sie freigegebene Ordner angeben, deren Dateiaktivität vom Programm überwacht werden soll. Sie können auch Dateien aus dem Schutzbereich ausschließen. In älteren Versionen des Programms hat die Komponente Verhaltensanalyse die Dateiaktivität aller freigegebenen Ordner überwacht.

4. Jetzt können Sie im Installationspaket verschiedene Komponentensätze für verschiedene Betriebssysteme konfigurieren. Sie können das Programm also mithilfe desselben Installationspakets auf Workstations und Servern bereitstellen. Komponenten, die für einen bestimmten Betriebssystemtyp nicht verfügbar sind, werden in den Eigenschaften des Installationspakets automatisch ausgeschlossen.

5. Es wurde die Möglichkeit zur Auswahl von vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Anwendungen hinzugefügt. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen kann die vertrauenswürdige Zone für das Programm in einer virtuellen Umgebung (Citrix, Vmware) schnell konfiguriert werden. Diese Ausnahmen umfassen beispielsweise VHD- und VHDX-Dateien für virtuelle Maschinen. Sie können Ausnahmen hinzufügen, wenn Sie ein Installationspaket für das Programm erstellen, eine Richtlinie erstellen oder Kaspersky Endpoint Security installieren.

6. Die EDR-Telemetrie enthält jetzt Ereignisse für Vorgänge mit über USB verbundenen Geräten. Sie können diese Ereignisse auch zu den Ausnahmen der EDR-Telemetrie hinzufügen.

7. Neue Option: Netzwerkverbindungen, die das veraltete Protokoll TLS 1.0 verwenden, können blockiert werden. TLS 1.0 hat eine niedrige Sicherheitsstufe. Daher wird empfohlen, dieses Protokoll zu deaktivieren und die neuere Version TLS 1.2 oder TLS 1.3 zu verwenden. Standardmäßig werden TLS 1.0-Verbindungen durch Kaspersky Endpoint Security blockiert. Nachdem die Programmversion aktualisiert wurde, funktionieren Drittanbieterdienste, die das TLS 1.0-Protokoll verwenden, möglicherweise nicht mehr wie vorgesehen. Um Probleme beim Betrieb von Drittanbieterdiensten zu vermeiden, können Sie die Verwendung des TLS 1.0-Protokolls in Gruppenrichtlinien erlauben, bevor Sie die Programmversion aktualisieren.

8. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen der folgenden privaten Patches berücksichtigt: PF10053, PF10054, PF10360, PF10362, PF10363, PF12120, PF12121, PF12122, PF13115, PF13118, PF13119, PF14061, PF14062, PF14064, PF14065, PF15054, PF15056, PF15058, PF16052, PF16053, PF16055, PF16056, PF17027, PF17029, PF17039, PF17041, PF17043, PF18010, PF18011, PF18014, PF18015, PF18020, PF18021, PF18022, PF18023, PF18024, PF18028, PF19003, PF19016, PF19018.

Update 12.7

Kaspersky Endpoint Security 12.7 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Jetzt können Sie die Nutzung von CPU-Ressourcen für Aufgaben zur *Malware-Untersuchung* beschränken. Geben Sie dazu in den App-Einstellungen an, wie viel Prozent der CPU-Leistung für alle Kerne während der Untersuchung des Computers genutzt werden dürfen.

2. Jetzt können Sie manuell Dateien zur Untersuchung in KATA Sandbox senden. *KATA Sandbox* ist eine Komponente von Kaspersky Anti Targeted Attack Platform, die Dateien auf virtuellen Betriebssystem-Images ausführt. „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). Um eine Datei zur Untersuchung an KATA Sandbox zu senden, wählen Sie den entsprechenden Befehl im Kontextmenü der Datei aus.

3. Jetzt können Sie die Integration in die Lösung *Kaspersky Network Detection and Response* einrichten. Diese Lösung schützt das Unternehmens-LAN. Kaspersky Network Detection and Response (NDR) ist Teil der Kaspersky Anti Targeted Attack Platform. Die Interaktion mit NDR können Sie sowohl im Standardmodus als auch im EDR Agent-Modus konfigurieren.

4. Die Erweiterung für den Schutz vor E-Mail-Bedrohungen unterstützt jetzt den E-Mail-Client Microsoft Office Outlook Version 2021. Die Erweiterung ermöglicht die Untersuchung von Nachrichten auf der Ebene eines E-Mail-Clients statt auf Protokollebene. Zusätzlich zu Nachrichten können Sie mit der Erweiterung auch Objekte untersuchen, die über die MAPI-Schnittstelle von Microsoft Exchange-Repositorys empfangen werden (z. B. Objekte im Kalender). Diese Untersuchung erfolgt im Mail-Client.

5. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen der folgenden privaten Patches berücksichtigt: PF10049, PF10355, PF12114, PF13109, PF14056, PF15038, PF15045, PF16037, PF16042, PF16047, PF17014, PF17018, PF17021, PF17024, PF18006, PF18007.

Update 12.6

Kaspersky Endpoint Security 12.6 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Die Funktionalität zur Integration mit der SIEM-Lösung von Kaspersky – *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* – wurde hinzugefügt. Jetzt können Ereignisse aus Windows-Ereignisprotokollen an den KUMA-Kollektor gesendet werden. Dadurch kann KUMA von allen Computern, auf denen Kaspersky Endpoint Security installiert ist, Windows-Ereignisse empfangen (die Anzahl der unterstützten EventIDs ist begrenzt). Dazu muss der KUMA-Agent nicht auf diesen Computern installiert sein.

2. Die neue Komponente *Überwachung der Systemintegrität* wurde als Ersatz der Komponente „Überwachung der Dateiintegrität" hinzugefügt. Die Überwachung der Systemintegrität enthält alle Funktionen der Überwachung der Dateiintegrität und ermöglicht zusätzlich die Überwachung von Registrierungsänderungen und angeschlossenen Geräten. 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 Dateiintegrität ist nicht mehr im Lieferumfang der App enthalten. Die Einstellungen aus der Überwachung der Dateiintegrität werden bei einem Update der App automatisch in die Überwachung der Systemintegrität migriert. Um für die Überwachung der Systemintegrität einen ordnungsgemäße Ausführung der zu gewährleisten, sollten sowohl die App von Kaspersky Endpoint Security als auch das Verwaltungs-Plug-in auf Version 12.6 aktualisiert werden.

3. Der Status des installierten und integrierten EDR Agent (KATA) wurde in der Konsole von Kaspersky Security Center zu den Computereigenschaften hinzugefügt. Wenn Sie einen integrierten EDR Agent (KATA) installiert haben, zeigt die Spalte **Status von Endpoint Sensor** den aktuellen Status der Komponente an (z. B. *Wird ausgeführt*, *Abgebrochen* oder *Wird nicht von der Lizenz unterstützt*).

4. Es wurde die Möglichkeit zur Auswahl von vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Anwendungen hinzugefügt. Die vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Anwendungen erlauben eine zeitsparende Konfiguration der vertrauenswürdigen Zone, wenn die App auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Managern verwendet wird. Diese Ausnahmen umfassen beispielsweise MDF- und LDF-Datenbankdateien. Sie können weitere Ausnahmen hinzufügen, indem Sie eine neue Richtlinie erstellen, eine bestehende Richtlinie ändern oder Kaspersky Endpoint Security installieren.

5. Die Anzeige von Alarmdetails für Kaspersky Endpoint Detection and Response Optimum wurde aus dem Verwaltungs-Plug-in für Kaspersky Endpoint Security in ein separates Verwaltungs-Plug-in für Kaspersky Endpoint Detection and Response verlegt. Das EDR-Verwaltungs-Plug-in ist ein spezielles Plug-in für die Arbeit mit den Agenten auf Windows-, Mac- und Linux-Betriebssystemen. Wenn Sie jetzt mit EDR Optimum arbeiten, benötigen Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security, um Aufgaben zur Reaktion auf Bedrohungen zu erstellen, und das EDR-Verwaltungs-Plug-in, um Details zu Warnungen anzuzeigen.

6. Unterstützung für Windows 11 24H2.

7. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen der folgenden privaten Patches berücksichtigt: pf10048, pf10353, pf12106, pf12107, pf12108, pf13090, pf13100, pf15031, pf15034, pf15036, pf16021, pf16023, pf16029, pf17002.

Update 12.5

Kaspersky Endpoint Security 12.5 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Eine Option zum Konfigurieren von Telemetrie-Ausnahmen wurde hinzugefügt. *Telemetrie* ist eine Liste von Ereignissen, die auf dem geschützten Computer aufgetreten sind. Telemetriedaten werden von Kaspersky Anti Targeted Attack Platform (EDR) verwendet, um die IT-Infrastruktur des Unternehmens zu überwachen und zu schützen. Wenn Telemetrie-Ausnahmen konfiguriert werden, lässt sich die Computerleistung verbessern und die Datenübertragung an den Telemetrie-Erfassungsserver optimieren.

2. Die Benutzeroberfläche der vertrauenswürdigen Zone der App wurde verbessert. Kaspersky Endpoint Security blendet Objekte der vertrauenswürdigen Zone jetzt für den Benutzer aus, wenn der Administrator dem Benutzer das Hinzufügen eigener (lokaler) Untersuchungsausnahmen und vertrauenswürdiger Programme untersagt hat. Dadurch wird der unbefugte Zugriff eines Angreifers auf die vertrauenswürdige Zone verhindert und die Sicherheit des Computers erhöht.

3. Eine Option zur Untersuchung des Datenverkehrs für die E-Mail-Clients MyOffice Mail und R7-Office Organizer wurde hinzugefügt. Die Komponente Schutz vor E-Mail-Bedrohungen untersucht jetzt beim Herunterladen nicht nur Nachrichtenanhänge, sondern auch gesendete und empfangene Nachrichten.

4. Die neue Webressourcen-Kategorie *Generative KI-Tools* wurde hinzugefügt. Mithilfe der „Web-Kontrolle“ können Sie den Zugriff auf Websites der neuen Kategorie anpassen.

5. Jetzt können Sie in der Firewall-Liste den Speicherort einer Netzwerkpaketregel auswählen. Die Priorität einer Netzwerkpaketregel wird durch ihre Position in der Liste bestimmt. In früheren Versionen der App konnte eine neue Regel nur am Ende der Liste hinzugefügt werden. Anschließend musste die Regel manuell in der Liste verschoben werden, um ihr die gewünschte Priorität zuzuweisen. Wenn Sie nun eine Regel hinzufügen, können Sie die Position der Regel auswählen: am Anfang bzw. am Ende der Liste oder neben der ausgewählten Regel.

6. In den Regeln der Komponenten von Kaspersky Endpoint Security können Sie jetzt Benutzer nicht nur aus Active Directory auswählen, sondern auch aus der Benutzerliste in Kaspersky Security Center. Sie können die Daten eines lokalen Benutzerkontos auch manuell eingeben. Diese Möglichkeit wurde für die Regeln der folgenden Komponenten hinzugefügt: Programmkontrolle, Gerätekontrolle, Web-Kontrolle, Adaptive Kontrolle von Anomalien und Protokollanalyse.

7. Der Bericht zur Erkennung von Netzwerkangriffen enthält jetzt eine Spalte mit der MAC-Adresse des angreifenden Computers (Komponente „Schutz vor Netzwerkbedrohungen"). Der Bericht enthält jetzt zusätzlich zur IP-Adresse auch die MAC-Adresse des angreifenden Computers. Dies ist für die Untersuchung von Vorfällen hilfreich. Berichte, die die MAC-Adresse des angreifenden Computers enthalten, sind auch in der Konsole von Kaspersky Security Center Linux Version 15.1 und höher verfügbar.

8. Das Niveau der Anforderungen an den Computerschutz wurde erhöht. Für die hohe Schutzstufe muss jetzt der Schutz von App-Diensten vor externer Steuerung aktiviert werden. Überprüfen Sie den Indikator für die Sicherheitsstufe im oberen Teil des Richtlinienfensters. Bei der mittleren oder niedrigen Sicherheitsstufe können Sie den Schutz der App-Dienste vor externer Steuerung im Fenster mit den Empfehlungen für den Sicherheitsstufen-Indikator aktivieren.

9. Unterstützung für neue Objekterkennungs-Ereignisse, wenn die ausgeführte App in der Konfiguration für Endpoint Detection and Response Agent (EDR Agent) hinzugefügt wurde. Diese Ereignisse wurden bereits in der Konfiguration [KES+built-in agent] unterstützt.

10. Bei der Entwicklung dieser Version von Kaspersky Endpoint Security für Windows haben wir die Änderungen der folgenden privaten Patches berücksichtigt: pf9640, pf9830, pf9831, pf10047, pf10351, pf12102, pf12105, pf13084, pf13089, pf14040, pf14047, pf15026, pf15028, pf16013.

Update 12.4

Kaspersky Endpoint Security 12.4 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Neue Funktionalität zum Schutz der Verbindung zwischen dem Computer und Kaspersky Security Center. Mit der neuen Aufgabe *Schutz der Verbindung zum Administrationsserver* können Sie ein Kennwort für die Verbindung zu einem vertrauenswürdigen Server festlegen. Ohne dieses Kennwort ist es nicht möglich, den Computer erneut zu verbinden oder Befehle von einem anderen Server auszuführen.

2. Neue Option für die Komponente „Kennwortschutz": Benutzer können jetzt auch manuell ausgewählt werden und nicht nur über Active Directory. Sie können also manuell einen Benutzernamen und ein Kennwort angeben und Kaspersky Endpoint Security Zugriffsrechte für dieses Benutzerkonto zuweisen. Darum müssen Sie Ihr KLAdmin-Kennwort nicht mit anderen Benutzern teilen oder neue Active Directory-Benutzerkonten erstellen, um den Zugriff auf die App zu kontrollieren.

3. Unterstützung für Windows 11 23H2.

Update 12.3

Kaspersky Endpoint Security 12.3 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Jetzt können Sie das Programm in der Endpoint Detection and Response Agent-Konfiguration installieren. Diese Konfiguration ermöglicht die Installation des Programms mit einer Auswahl von Komponenten, die für die Detection and Response-Lösungen von Kaspersky erforderlich sind: Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform (EDR). Sie können das Programm in dieser Konfiguration zusammen mit Drittanbieter-Lösungen (z. B. Dr.Web, Dallas Lock oder ESET) installieren. Dadurch können Sie neben Detection and Response-Lösungen von Kaspersky auch Infrastruktur-Sicherheitstools von Drittanbietern nutzen.

2. Die Funktionen von Kaspersky Endpoint Security zur Verwaltung von Bluetooth-Geräten wurden verbessert. Jetzt können Sie Ausnahmen konfigurieren, den Zugriff auf alle Bluetooth-Geräte beschränken und Ausnahmen für Eingabegeräte (drahtlose Tastaturen, Mäuse usw.) festlegen.

3. Die Nutzung der Datenbank für ausführbare Dateien durch die Komponente „Programmkontrolle“ wurde optimiert. Wenn eine Datei vom Computer gelöscht wird, entfernt Kaspersky Endpoint Security jetzt automatisch Informationen über diese Datei aus der Datenbank. Dadurch ist die Datenbank immer auf dem neuesten Stand, und die Ressourcen von Kaspersky Security Center werden geschont.

4. Das Niveau der Anforderungen an den Computerschutz wurde erhöht. Für das hohe Schutzniveau muss jetzt der Kennwortschutz aktiviert werden. Sehen Sie im oberen Teil des Richtlinienfensters nach, welche Sicherheitsstufe angezeigt wird. Bei mittlerem oder niedrigem Schutzniveau können Sie den Kennwortschutz im Fenster mit dem Sicherheitsstufen-Indikator aktivieren.

5. Die Unterstützung des HTTPS-Protokolls wurde hinzugefügt. Dadurch wird die Interaktion der App mit Kaspersky Security Network ermöglicht. Aktivieren Sie die Nutzung von HTTPS in den Eigenschaften des Administrationsservers im Einstellungen des KSN-Proxyservers.

Update 12.2

Kaspersky Endpoint Security 12.2 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Die Unterstützung des WPA3-Protokolls wurde hinzugefügt, um Verbindungen mit WLAN-Netzwerken zu steuern (Gerätekontrolle). Jetzt können Sie das WPA3-Protokoll in den Einstellungen für vertrauenswürdige WLAN-Netzwerke auswählen und die Verbindung mit einem Netzwerk mit einem weniger sicheren Protokoll verweigern.

2. Jetzt können Sie ein Protokoll und Ports für Ausnahmen vom „Schutz vor Netzwerkbedrohungen“ auswählen. Sie können nicht nur die IP-Adressen vertrauenswürdiger Geräte angeben, sondern auch einen Port und ein Protokoll auswählen. Dadurch können Sie einzelne Datenströme ausschließen und Netzwerkangriffe von vertrauenswürdigen IP-Adressen verhindern.

3. Unterschiedliche Reihenfolge der Update-Quellen für die lokale *Update der Datenbanken und Programm-Module-Aufgabe*, wenn eine Richtlinie auf den Computer angewendet wird. Als primäre Update-Quelle wird jetzt standardmäßig der Kaspersky Security Center-Server verwendet, nicht mehr die Kaspersky-Server. Dadurch lässt sich Datenverkehr einsparen, wenn der Benutzer die lokale *Update der Datenbanken und Programm-Module*-Aufgabe ausführt.

Update 12.1

Kaspersky Endpoint Security 12.1 für Windows bietet folgende Neuerungen und Verbesserungen:

1. Ein integrierter Agent für die Lösung Kaspersky Anti Targeted Attack Platform wurde hinzugefügt. Kaspersky Endpoint Agent ist nicht mehr erforderlich, um EDR (KATA) zu verwenden. Alle Funktionen von Kaspersky Endpoint Agent werden von Kaspersky Endpoint Security ausgeführt. Um Richtlinien von Kaspersky Endpoint Agent zu migrieren, verwenden Sie den Migrations-Assistenten. Nach dem App-Update wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent. Kaspersky Endpoint Agent wurde zur Liste der inkompatiblen Software hinzugefügt. Kaspersky Endpoint Security verfügt über integrierte Agenten für alle Detection and Response-Lösungen. Damit ist die Installation von Kaspersky Endpoint Agent zur Integration mit diesen Lösungen nicht mehr erforderlich.

2. Der Azure WVD-Kompatibilitätsmodus wird jetzt unterstützt. Diese Funktion sorgt dafür, dass der Status der virtuellen Azure-Maschine in der Kaspersky Anti Targeted Attack Platform-Konsole korrekt angezeigt wird. Mithilfe des Azure WVD-Kompatibilitätsmodus können Sie diesen virtuellen Computern eine permanente eindeutige Sensor-ID zuweisen.

3. Jetzt können Sie den Benutzerzugriff auf Mobilgeräte in iTunes oder ähnlichen Apps konfigurieren. Sie können also beispielsweise festlegen, dass das Mobilgerät nur in iTunes verwendet werden darf, und die Verwendung des Mobilgeräts als Wechseldatenträger sperren. Die App unterstützt diese Regeln auch für die Anwendung Android Debug Bridge (ADB).

4. Kaspersky Security Center Version 11 wird nicht mehr unterstützt. Upgraden Sie Kaspersky Security auf die neueste Version.

Behobene Probleme

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

Liste der in Version 14.2 behobenen Probleme

Kennzeichnung	Beschreibung
10110351	Die Komponente Gerätekontrolle ermöglicht den Zugriff auf ein MTD-Gerät (SD-Karte), wenn für den Gerätetyp **Wechseldatenträger** die Aktion **Verbieten** ausgewählt ist.
10068496	Auf einem geschützten Gerät kann der Modus für den Schutz vor MAC-Spoofing geändert werden, wenn die Einstellungen für den Schutz vor Netzwerkbedrohungen in der übergeordneten Richtlinie gesperrt sind.
10095087	Wenn die Untersuchung verschlüsselter Verbindungen aktiviert ist, löst der Zugriff auf eine beliebige Website über eine Next-Generation-Firewall (NGFW) mit einem gesperrten Zertifikat eine Benachrichtigung über die Umleitung auf eine Domäne mit einem nicht vertrauenswürdigen Zertifikat aus.
10140912	Wenn das Programm installiert ist, erkennt der Computer das PDA-Gerät BHT1100B mit Windows Mobile nicht.
10141009	Wenn die Komponente Dateiverschlüsselung installiert ist, wird die Anwendung Anthropic Claude möglicherweise nicht gestartet.

Kennzeichnung	Beschreibung
10610853	Nach dem Upgrade auf die neue Version kann die Richtlinie nicht geöffnet werden, da die Einstellungen der Gerätekontrolle in der neuen Version Geräte enthalten, die in der vorherigen Version nicht unterstützt wurden.
10720516	Wenn das Programm installiert ist, lassen sich Anhänge in Dateien im Office-Format möglicherweise nicht öffnen.
10421967	Die Anmeldung bei einem freigegebenen Postfach schlägt fehl, wenn dieses Postfach als separates Konto hinzugefügt wurde.

Liste der im Web-Plug-in 14.2.0.8289 behobenen Probleme

Kennzeichnung	Beschreibung
9946286	Beim Hinzufügen einer Website-Adresse zu einer Web-Kontrolle-Regel kann keine Maske verwendet werden, die keinen Punkt zwischen der Domäne und der Domänenzone enthält.
10054657 10507166	Nach der Migration auf die neue Version können bestimmte Komponenten (z. B. Gerätekontrolle und Programmkontrolle) nicht über eine Richtlinie verwaltet werden.
10084390	In den Einstellungen der Komponente Gerätekontrolle ist der Gerätetyp **Festplatte** doppelt vorhanden, wodurch die Festplatten der Benutzer blockiert werden.
10113718	In einigen Fällen werden benutzerdefinierte Firewall-Regeln nicht angezeigt.
10311613	In den Einstellungen der Komponente Programm-Überwachung kann keine geschützte Ressource mithilfe einer Maske mit dem Zeichen `*` hinzugefügt werden.
10391923	Wenn in der Programmkontrolle eine Programmkategorie auf Basis des MD5-Hashwerts einer Datei erstellt wird, wird keine Warnung angezeigt, dass diese Kategorie ungültig ist und nicht funktioniert.
10571790	Für die Komponente Programmkontrolle wurde der Titel der Liste der Blockierungsregeln im Modus **Alle erlauben, die nicht in der Regelliste angegeben sind** korrigiert.
10592891 10689065	In der vertrauenswürdigen Zone wird bei Ausnahmen im Abschnitt **Ausnahmen für die Schadsoftware-Untersuchung** das Feld **Kommentar** nicht angezeigt.
10613015 10689049 10592534	In der Komponente Gerätekontrolle wird das Feld **Kommentar** für vertrauenswürdige Geräte nicht angezeigt.
10645068 10689057	Die Aufgabe *Schlüssel löschen* wird nicht ausgeführt, wenn eine Lizenzschlüsseldatei im KEY-Format ausgewählt ist.
10685370 10685422	In der Komponente Gerätekontrolle kann kein neues Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt werden, wenn die Liste bereits ein Gerät mit demselben Namen enthält.
10721136	Gruppenaufgaben können nicht gespeichert werden, wenn in den Zeitplaneinstellungen kein Abschlussdatum angegeben ist.
10753509	Wenn die Liste der Benutzer und Gruppen für vertrauenswürdige Geräte in der Komponente Gerätekontrolle geändert wird, können sich die Eintragstypen ändern. Dies kann dazu führen, dass die Einstellungen nicht mehr für das Gerät gelten.
10773402	In einigen Fällen können Änderungen an den Richtlinieneinstellungen aufgrund beschädigter Profile nicht gespeichert werden.
10822620	Die Einstellungen der Komponente Schutz vor Verschlüsselung werden in der Richtlinie nicht angezeigt, und Änderungen an den Benachrichtigungseinstellungen werden nicht gespeichert.
10817035	In einer untergeordneten Richtlinie kann ein vertrauenswürdiges Gerät hinzugefügt werden, selbst wenn diese Einstellung in der übergeordneten Richtlinie gesperrt ist (geschlossenes „Vorhängeschloss“). Das hinzugefügte Gerät wird jedoch nicht gespeichert.
10678009	Im Web-Plug-in von Kaspersky Endpoint Security schlägt das Hinzufügen einer neuen Firewall-Regel zu einer Richtlinie fehl, wenn zuvor eine Regel mit einem IP-Adressbereich erstellt wurde.

Liste der in Version 14.1 behobenen Probleme

Kennzeichnung	Beschreibung
10140523	Die Aktivierung von nativem NVMe in Windows 11 kann zu einem instabilen Programmverhalten führen.
9340076	Auf einem Gerät, auf dem das Programm installiert und die Komponente zur Dateiverschlüsselung aktiviert ist, aktualisiert Windows Explorer die Inhalte eines Netzwerkordners nicht automatisch, nachdem diese von einem anderen Gerät aus geändert wurden.
9722863	Der Bericht zur Gerätekontrolle enthält kein Ereignis zur Trennung eines USB-Tokens.
10006481	Nach der Anwendung einer Regel, die eingehenden Datenverkehr blockiert, können aktive TCP-Verbindungen zu externen Diensten aufgrund einer fehlerhaften Timeout-Berechnung vorzeitig beendet werden.
10140912	Das Programm erkennt das PDA-Gerät BHT1100B nicht.
10157563	Folder Redirection funktioniert nach einem Neustart auf VDI-Workstations möglicherweise nicht.
10158494	Die Gerätekontrolle protokolliert mehrere Verbindungs- und Trennungsereignisse eines Wechseldatenträgers, ohne dass dieser physisch erneut verbunden wird.

Häufige Fragen

ALLGEMEIN

Auf welchen Computern funktioniert Kaspersky Endpoint Security?

Was hat sich seit der letzten Version geändert?

Mit welchen anderen Kaspersky-Apps funktioniert Kaspersky Endpoint Security?

Wie können bei der Verwendung von Kaspersky Endpoint Security die Computer-Ressourcen geschont werden?

SOFTWARE-VERTEILUNG

Wie kann Kaspersky Endpoint Security auf allen Computern eines Unternehmens installiert werden?

Welche Installationseinstellungen können in der Befehlszeile konfiguriert werden?

Wie kann Kaspersky Endpoint Security per Fernzugriff deinstalliert werden?

UPDATE

Welche Methoden gibt es für das Datenbanken-Update?

Was tun, wenn nach einem Update Probleme auftreten?

Wie werden die Datenbanken außerhalb des Unternehmensnetzwerks aktualisiert?

Kann ein Proxyserver für Updates verwendet werden?

SICHERHEIT

Auf welche Weise untersucht Kaspersky Endpoint Security die E-Mail-Nachrichten?

Wie wird eine vertrauenswürdige Datei von der Untersuchung ausgeschlossen?

Wie schütze ich einen Computer vor Viren auf einem Flash-Laufwerk?

Wie kann eine Schadsoftware-Untersuchung ausgeführt werden, ohne dass der Benutzer dies bemerkt?

Wie kann der Schutz durch Kaspersky Endpoint Security vorübergehend angehalten werden?

Wie stelle ich eine Datei wieder her, die von Kaspersky Endpoint Security irrtümlicherweise gelöscht wurde?

Wie wird Kaspersky Endpoint Security davor geschützt, vom Benutzer entfernt zu werden?

INTERNET

Untersucht Kaspersky Endpoint Security verschlüsselte Verbindungen (HTTPS)?

Wie wird festgelegt, dass sich die Benutzer nur mit vertrauenswürdigen WLAN-Netzwerken verbinden können?

Wie können soziale Netzwerke blockiert werden?

PROGRAMMMODULE

Wie werden die Programme ermittelt, die auf dem Benutzercomputer installiert sind (Inventarisierung)?

Wie kann der Start von Computerspielen verhindert werden?

Wie wird überprüft, ob die „Programmkontrolle“ richtig konfiguriert ist?

Wie wird ein Programm zur Liste der vertrauenswürdigen Programme hinzugefügt?

GERÄTE

Wie kann die Verwendung von Flash-Laufwerken verboten werden?

Wie wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt?

Kann man Zugriff auf ein blockiertes Gerät erhalten?

VERSCHLÜSSELUNG

Unter welchen Umständen ist eine Verschlüsselung nicht möglich?

Wie kann mithilfe eines Kennworts der Zugriff auf ein Archiv beschränkt werden?

Kann bei der Verschlüsselung eine Smartcard oder ein Token verwendet werden?

Ist der Zugriff auf verschlüsselte Daten möglich, wenn keine Verbindung zu Kaspersky Security Center besteht?

Was tun, wenn das Betriebssystem nicht mehr funktioniert und die Daten noch verschlüsselt sind?

SUPPORT

Wo befindet sich die Berichtsdatei?

Wie wird eine Ablaufverfolgungsdatei erstellt?

Wie wird die Dump-Aufzeichnung aktiviert?

Kaspersky Endpoint Security für Windows

Kaspersky Endpoint Security für Windows (im Folgenden auch „Kaspersky Endpoint Security“) bietet dem Computer einen komplexen Schutz vor unterschiedlichen Bedrohungsarten, Netzwerkangriffen und betrügerischen Angriffen.

Die App ist nicht für den Einsatz in technologischen Prozessen vorgesehen, die automatisierte Steuerungssysteme beinhalten. Für den Schutz von Geräten in solchen Systemen wird die App Kaspersky Industrial CyberSecurity for Nodes empfohlen.

Technologien zum Erkennen von Bedrohungen



Machine Learning

Kaspersky Endpoint Security verwendet ein Modell, das auf Machine Learning basiert. Das Modell wird von Kaspersky entwickelt. Anschließend werden kontinuierlich Bedrohungsdaten aus KSN in das Modell eingespeist (Modelltraining).



Cloud- Analyse

Kaspersky Endpoint Security erhält von Kaspersky Security Network Daten über Bedrohungen. *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen.



Experten-Analyse

Kaspersky Endpoint Security verwendet Bedrohungsdaten, die von den Virenanalysten von Kaspersky hinzugefügt werden. Die Virenanalysten bewerten Objekte, deren Reputation nicht automatisch ermittelt werden kann.



Verhaltensanalyse

Kaspersky Endpoint Security analysiert die Aktivität von Objekten in Echtzeit.



Automatische Analyse

Kaspersky Endpoint Security erhält Daten vom System für automatische Objektanalyse. Das System verarbeitet alle Objekte, die an Kaspersky gesendet werden. Dann ermittelt das System die Reputation des Objekts und fügt die Daten den Antiviren-Datenbanken hinzu. Wenn das System die Reputation des Objekts nicht ermitteln kann, stellt das System Anfragen an die Kaspersky-Virenanalysten.



Sandbox

Kaspersky Endpoint Security verarbeitet das Objekt auf einer virtuellen Maschine. „Kaspersky Sandbox“ analysiert das Verhalten des Objekts und entscheidet über seine Reputation. Diese Technologie ist nur verfügbar, wenn Sie die Lösung „Kaspersky Sandbox“ verwenden.



Cloud Sandbox

Kaspersky Endpoint Security untersucht Objekte in einer isolierten Umgebung, die von Kaspersky bereitgestellt wird. Die Technologie „Cloud Sandbox“ ist ständig aktiviert und steht allen Benutzern von Kaspersky Security Network zur Verfügung, unabhängig vom Typ der genutzten Lizenz. Wenn Sie die Lösung Endpoint Detection and Response schon bereitgestellt haben, können Sie einen separaten Indikator für durch Cloud Sandbox erkannte Bedrohungen aktivieren.

Auswahlstruktur

Jeder Bedrohungstyp wird von einer bestimmten Programmkomponente verarbeitet. Die Komponenten können unabhängig voneinander aktiviert und deaktiviert sowie über ihre Einstellungen angepasst werden.

Abschnitt	Komponente
Basisschutz	**Schutz vor bedrohlichen Dateien** 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. **Schutz vor Web-Bedrohungen** Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert außerdem Verbindungen zu schädlichen Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse. **Schutz vor E-Mail-Bedrohungen** Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. 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. Die Anwendung unterstützt POP3, SMTP, IMAP und NNTP in den folgenden E-Mail-Clients: • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer Um den Datenverkehr in den E-Mail-Clients Mozilla Thunderbird, MyOffice Mail und R7-Office Organizer zu untersuchen, müssen Sie ein Kaspersky-Zertifikat zum Zertifikatspeicher hinzufügen und den Speicher für eigene Zertifikate auswählen. Der „Schutz vor E-Mail-Bedrohungen“ unterstützt keine anderen Protokolle und E-Mail-Clients. 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 bietet der „Schutz vor E-Mail-Bedrohungen“ eine Erweiterung für Microsoft Office Outlook. Mit dieser Erweiterung können Nachrichten auf der *Ebene des E-Mail-Clients* untersucht werden. Die Erweiterung für den Schutz vor E-Mail-Bedrohungen unterstützt die 32-Bit- und 64-Bit-Versionen von Outlook 2010, 2013, 2016, 2019, 2021, 2024 und 365. Auf Arm-basierten Computern unterstützt die Erweiterung für den Schutz vor E-Mail-Bedrohungen die 32-Bit- und 64-Bit-Versionen von Outlook 2016, Outlook 2021, Outlook 2024 und Outlook 365 für Arm64. **Schutz vor Netzwerkbedrohungen** Die Komponente *Schutz vor Netzwerkbedrohungen* (auch Intrusion Detection System oder IDS genannt) überwacht den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe charakteristisch sind. Wenn das Programm einen Netzwerkangriff auf den Benutzercomputer erkennt, sperrt es die Netzwerkverbindung mit dem angreifenden Computer. Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Programm-Datenbanken enthalten. Die Liste der Netzwerkangriffe, die von der Komponente „Schutz vor Netzwerkbedrohungen“ erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert. **Firewall** 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*. **Schutz vor BadUSB-Angriffen** Die Komponente „Schutz vor BadUSB-Angriffen“ verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden. **AMSI-Schutz**

Abschnitt	Komponente
	Die Komponente "AMSI-Schutz" dient der Unterstützung des Antimalware Scan Interface von Microsoft. Mithilfe *Schnittstelle für Antimalware Scan Interface (AMSI)* können Dritthersteller-Anwendungen, die AMSI unterstützen, Objekte (z. B. PowerShell-Skripte) für eine zusätzliche Untersuchung an Kaspersky Endpoint Security senden und Untersuchungsergebnisse für diese Objekte erhalten.
Erweiterter Schutz 	**Kaspersky Security Network** *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. 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. **Verhaltensanalyse** 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. **Schutz vor Verschlüsselung** Die Komponente „Schutz vor Verschlüsselung“ analysiert die Aktivität in freigegebenen Ordnern. 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. **Exploit-Prävention** 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. **Programm-Überwachung** Die Komponente „Programm-Überwachung“ (HIPS, Host Intrusion Prevention System) hindert Programme daran, systemgefährdende Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und persönliche Daten. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken und des Cloud-Dienstes Kaspersky Security Network **Rollback von schädlichen Aktionen** Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Abschnitt	Komponente
Sicherheitskontrolle 	**Programmkontrolle** 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. **Gerätekontrolle** 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. **Web-Kontrolle** Die „Web-Kontrolle“ verwaltet den Zugriff durch Benutzer auf Webressourcen. Dadurch lässt sich Datenverkehr einsparen und die zweckentfremdete Nutzung der Arbeitszeit reduzieren. Wenn ein Benutzer versucht, eine durch die „Web-Kontrolle“ beschränkte Website zu öffnen, blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an. **Adaptive Kontrolle von Anomalien** Die Komponente „Adaptive Kontrolle von Anomalien“ überwacht und blockiert Aktionen, die für Computer des Unternehmensnetzwerks untypisch sind. Zur Überwachung von untypischen Aktionen verwendet die „Adaptive Kontrolle von Anomalien“ eine Auswahl von Regeln (z. B. die Regel *Start von Windows PowerShell aus einem Office-Programm*). Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für schädliche Aktivitäten erstellt. Sie können ein Verhalten der „Adaptiven Kontrolle von Anomalien“ für jede einzelne Regeln auswählen und beispielsweise den Start von PowerShell-Skripten erlauben, um die Lösung von Unternehmensaufgaben zu automatisieren. Kaspersky Endpoint Security aktualisiert den Regelsatz aus den Programm-Datenbanken. **Protokollanalyse** Die „Protokollanalyse“ überwacht die Integrität der geschützten Umgebung basierend auf der Windows-Ereignisprotokollanalyse. Wenn das Programm ungewöhnliche Verhaltensmerkmale im System erkennt, wird der Administrator informiert, da solches Verhalten auf einen versuchten Cyberangriff hinweisen kann. **Überwachung der Systemintegrität** 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.
Aufgaben 	**Schadsoftware-Untersuchung** Kaspersky Endpoint Security untersucht den Computer auf Viren und andere Bedrohungen. Die „Schadsoftware-Untersuchung“ hilft, eine Ausbreitung von Schadsoftware auszuschließen, die nicht von den Schutzkomponenten erkannt wurde, beispielsweise aufgrund einer niedrigen Sicherheitsstufe. **Update der Datenbanken und Programm-Module** Kaspersky Endpoint Security lädt aktualisierte Datenbanken und Programm-Module. Dadurch befindet sich der Schutz des Computers vor Viren und anderen Schadprogrammen stets auf dem neuesten Stand. Standardmäßig wird das Programm automatisch aktualisiert. Bei Bedarf können Datenbanken und Programm-Module jedoch jederzeit manuell aktualisiert werden. **Rollback des letzten Updates** Kaspersky Endpoint Security macht das letzte Update der Datenbanken und Programm-Module rückgängig. Dadurch besteht die Möglichkeit, bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückzukehren. Dies ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, welche dazu führt, dass Kaspersky Endpoint Security ein harmloses Programm blockiert. **Prüfung der Anwendungsintegrität** Kaspersky Endpoint Security überprüft, ob die Programm-Module, die sich im Installationsordner des Programms befinden, Beschädigungen oder Änderungen aufweisen. Besitzt ein Programm-Modul eine inkorrekte digitale Signatur, so gilt das Modul als beschädigt.
Datenverschlüsselung 	**Verschlüsselung auf Dateiebene** Mit dieser Komponente können Regeln zur Dateiverschlüsselung erstellt werden. Sie können vordefinierte Ordner für die Verschlüsselung auswählen, einen Ordner manuell auswählen oder bestimmte Dateien nach Erweiterung auswählen. **Vollständige Festplattenverschlüsselung** Mit dieser Komponente kann die Festplatte mithilfe der Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung verschlüsselt werden. **Verschlüsselung von Wechseldatenträgern** Mit dieser Komponente können Daten auf Wechseldatenträgern geschützt werden. Sie können die „Vollständige Festplattenverschlüsselung“ (FDE) oder die „Verschlüsselung von Dateien“ (FLE) verwenden.

Abschnitt	Komponente
Detection and Response 	**Endpoint Detection and Response Optimum** Integrierter Agent für die Lösung „Kaspersky Endpoint Detection and Response Optimum“ (im Folgenden auch „EDR Optimum“ genannt). Die Lösung *Kaspersky Endpoint Detection and Response* schützt die IT-Infrastruktur eines Unternehmens vor komplexen Cyberbedrohungen. Diese Lösung kombiniert die automatische Erkennung von Bedrohungen mit der Fähigkeit, auf diese Bedrohungen zu reagieren. Dadurch lassen sich komplexe Angriffen wie neue Exploits, Ransomware, dateilose Angriffe und Methoden mit legitimen Systemtools abwehren. Weitere Informationen zu dieser Lösung finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** Integrierter Agent für die Lösung „Kaspersky Endpoint Detection and Response Expert“ (im Folgenden auch „EDR Expert“ genannt). Im Vergleich zu „EDR Optimum“ bietet „EDR Expert“ eine erweiterte Funktionalität zur Überwachung von und zur Reaktion auf Bedrohungen. Weitere Informationen zu dieser Lösung finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert. **Endpoint Detection and Response Expert (on-premises)** und **Network Detection and Response (KATA)** Integrierte Agenten zur Verwaltung der Komponenten Endpoint Detection and Response und Network Detection and Response, die Teil der Lösung Kaspersky Anti Targeted Attack Platform sind. 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“. **Sandbox** Integrierter Agent für Sandbox. 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. **Managed Detection and Response** Integrierter Agent zur Unterstützung der Lösung „Kaspersky Managed Detection and Response“. Die Lösung *Kaspersky Managed Detection and Response (MDR)* erkennt und analysiert automatisch Sicherheitsvorfälle in Ihrer Infrastruktur. Zu diesem Zweck verwendet MDR von Endpunkten bereitgestellte Telemetriedaten sowie maschinelles Lernen. MDR sendet Vorfalldaten an die Kaspersky-Experten. Die Experten können den Vorfall dann bearbeiten und beispielsweise einen neuen Eintrag zu den Antiviren-Datenbanken hinzufügen. Alternativ können die Experten Tipps zum Umgang mit dem Vorfall geben und beispielsweise vorschlagen, bestimmte Computer vom Netzwerk zu isolieren. Ausführliche Informationen zur Funktionsweise der Lösung finden Sie in der Hilfe zu „Kaspersky Managed Detection and Response“.

Modi des Programms: Standard, EDR Agent, Light Agent

Kaspersky Endpoint Security für Windows ist Bestandteil vieler Kaspersky Lösungen. Je nach Lösung müssen Sie einen Modus für das Programm auswählen.



Standard-Modus

Dies ist der Haupt- und Standard-Modus des Programms. In diesem Modus können Sie das Programm als Teil der Lösungen von Kaspersky EPP (Endpoint Protection Platform) installieren. Kaspersky Endpoint Security im Standard-Modus ist beispielsweise Teil von Kaspersky Endpoint Security for Business. Kaspersky Endpoint Security bietet Workstations und Server umfassenden Schutz vor verschiedenen Bedrohungen, Netzwerkangriffen und Betrugsversuchen. Im Standardmodus sind auch integrierte Agenten für die Integration in die Kaspersky Detection and Response-Lösungen verfügbar, darunter EDR, MDR, KUMA und andere.



EDR Agent

In diesem Modus können die Kaspersky Detection and Response-Lösungen zusammen mit Drittanbieter-EPP-Lösungen bereitgestellt werden. Zu den Detection and Response-Lösungen gehören Kaspersky Managed Detection and Response (MDR) und Kaspersky Anti Targeted Attack Platform (KATA). EDR Agent unterstützt auch die Kaspersky SIEM-Lösung Kaspersky Unified Monitoring and Analysis Platform (KUMA).

In diesem Modus sind standardmäßige Schutzkomponenten wie Schutz vor bedrohlichen Dateien oder Schutz vor Web-Bedrohungen nicht verfügbar. Standardmäßig wird der Schutz des Computers durch die Drittanbieter-EPP-Lösung gewährleistet. EDR Agent überwacht kontinuierlich die auf diesen Computern ausgeführten Prozesse, geöffneten Netzwerkverbindungen und geänderten Dateien und interagiert mit den Detection and Response-Lösungen.



Light Agent

Dieser Modus wird zum Schutz virtueller Umgebungen verwendet. Kaspersky Endpoint Security im Light Agent-Modus ist Teil der Lösung Kaspersky Hybrid Cloud Security. Light Agent schützt virtuelle Maschinen mit Gastbetriebssystemen für Workstations und Server. In diesem Modus stehen die gleichen Schutz- und Kontrollkomponenten zur Verfügung wie im Standard-Modus. Der Unterschied besteht darin, dass Objekte von einer speziellen Komponente der Lösung untersucht werden. Diese ist auf einer separaten virtuellen Maschine (SVM, Secure Virtual Machine) installiert. Um die Sicherheit der Infrastruktur zu gewährleisten, verwendet Light Agent daher die SVM-Ressourcen und nicht die Ressourcen der virtuellen Maschine.

Lieferumfang

Zum Lieferumfang gehören die folgenden Programmpakete:

- **AES256**

  Dieses Programmpaket ist für die Installation auf Computern mit x86/x64-Architektur vorgesehen. Dieses Programmpaket enthält Verschlüsselungs-Tools, die den AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard) mit einer effektiven Schlüssellänge von 256 Bit realisieren.

- **AES56**

  Dieses Programmpaket ist für die Installation auf Computern mit x86/x64-Architektur vorgesehen. Das Programmpaket enthält Verschlüsselungs-Tools, die den AES-Verschlüsselungsalgorithmus mit einer effektiven Schlüssellänge von 56 Bit realisieren.

- **Arm64**

  Dieses Programmpaket ist für die Installation auf ARM-basierten Computern vorgesehen. Dieses Programmpaket ist nicht für die Installation auf Servern vorgesehen.

Stellen Sie vor der Installation sicher, dass das Programmpaket der Architektur Ihres Prozessors entspricht. Wenn das Programmpaket nicht zur Prozessorarchitektur passt, bricht das Installationsprogramm die Installation mit einem Fehler ab.

Das Programmpaket ist ein selbstentpackendes Archiv im EXE-Format. Wenn Sie den Inhalt des Programmpakets ansehen möchten, extrahieren Sie das Archiv in einen separaten Ordner. Jedes Programmpaket enthält die folgenden Dateien:

`kes_win.msi`	Installationspaket für Kaspersky Endpoint Security.
`setup_kes.exe`	Dateien, die für die Installation des Programms mit allen verfügbaren Methoden erforderlich sind.
`kes_win.kud`	Datei zur Erstellung eines Installationspakets für Kaspersky Endpoint Security.
`klcfginst.msi`	Installationspaket für das Verwaltungs-Plug-in der Anwendung in der Kaspersky Security Center-Verwaltungskonsole.
`bases.cab`	Dateien mit Update-Paketen, die bei der Programminstallation verwendet werden
`cleaner_v2.cab` `cleanerapi_v2.cab`	Dateien für die Deinstallation von inkompatibler Software.
`incompatible.txt`	Datei mit einer Liste von Anwendungen, die Kompatibilitätsprobleme mit Kaspersky Endpoint Security verursachen können. Kaspersky garantiert nicht für die Kompatibilität von Kaspersky Endpoint Security mit Anwendungen aus der Liste.
`ksn_<language ID>.txt`	Datei, in der Sie die Bedingungen für die Teilnahme an Kaspersky Security Network lesen können.
`license.txt`	Datei, die den Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie enthält.
`installer.ini`	Datei, die interne Parameter des Programmpakets enthält.
`kes.cab`	Dateien für die grafische Oberfläche der Anwendung.
`aes256.cab` / `aes56.cab`	Dateien für den AES-Verschlüsselungsalgorithmus (nicht im Lieferumfang des Arm64-Programmpakets enthalten).
`package.kcat`	Datei mit Signaturen aus dem Verteilungspaket des Programms. Die digitale Signatur garantiert die Authentizität und Integrität des Verteilungspakets.

Es wird davon abgeraten, die Werte dieser Parameter zu ändern. Falls Sie die Installationseinstellungen ändern möchten, verwenden Sie die Datei setup.ini.

Hard- und Softwarevoraussetzungen

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

Um die Funktionsfähigkeit von Kaspersky Endpoint Security zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Um das Programm zu installieren, benötigen Sie Administratorrechte auf dem Computer.

Allgemeine Mindestanforderungen

Minimale Voraussetzungen	Workstation (x86/x64)	Server (x86/x64)	Arm
Speicher	2 GB	2 GB	2 GB
Prozessor	1 GHz, SSE2-Unterstützung	1,4 GHz, SSE2-Unterstützung	1 GHz, Armv8.1-Architektur
Arbeitsspeicher	Workstation (x86): 1 GB Workstation (x64): 2 GB	2 GB Hinweis: Um die Anwendung mit dem integrierten Agenten für die Integration in Kaspersky Anti Targeted Attack Platform zu installieren, sind auf einem Server 8 GB Arbeitsspeicher erforderlich.	4 GB
Microsoft .NET Framework	4 oder höher	4 oder höher	4.8 oder höher

Arbeitsstationen

Unterstützte Betriebssysteme für Workstations:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Pro für Workstations / Education / Enterprise / Enterprise Multi-Session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise Multi-Session
- Windows 11 für Arm64 Home / Pro / Pro für Workstations / Education / Enterprise

Windows-Betriebssysteme ab Version 11 24H2 unterstützen die Technologie UDP Receive Segment Coalescing Offload (URO). Diese Technologie ist standardmäßig aktiviert, wenn auf dem Computer eine kompatible Netzwerkkarte und kompatible Treiber installiert sind. Wenn URO auf dem Benutzercomputer deaktiviert wird, kann die Leistung des Programms erheblich sinken.

Damit Kaspersky Endpoint Security korrekt funktioniert, muss auf dem Benutzercomputer der Dienst Windows-Sicherheitscenter (wscsvc) ausgeführt werden.

Kaspersky Endpoint Security kann unter Microsoft Windows 7 nicht installiert werden, wenn die Betriebssystem-Updates KB4490628 (12. März 2019) und KB4474419 (23. September 2019) nicht installiert sind. Ausführliche Informationen finden Sie in der Wissensdatenbank der Technischen Supports.

Details über die Unterstützung des Betriebssystems Microsoft Windows 10 finden Sie in der Wissensdatenbank des Technischen Supports.

Details über die Unterstützung des Betriebssystems Microsoft Windows 11 finden Sie in der Wissensdatenbank des Technischen Supports.

Server

Kaspersky Endpoint Security unterstützt die Hauptkomponenten der App auf Computern mit Windows-Serverbetriebssystem. Anstelle von Kaspersky Security for Windows Server können Sie auf den Servern und Clustern Ihres Unternehmens Kaspersky Endpoint Security für Windows verwenden (Cluster-Modus). Das Programm unterstützt auch den Server Core-Modus (siehe bekannte Probleme).

Unterstützte Betriebssysteme für Server:

- Windows Small Business Server 2011 Essentials / Standard (64-Bit)

  Microsoft Small Business Server 2011 Standard (64-Bit) wird nur unterstützt, wenn Service Pack 1 für Microsoft Windows Server 2008 R2 installiert ist.

- Windows MultiPoint Server 2011 (64-Bit)
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2016 Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2019 Essentials / Standard / Datacenter (einschließlich Server Core-Modus)

- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (einschließlich Server Core-Modus)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security kann unter Microsoft Windows Server 2008 R2 nicht installiert werden, wenn die Betriebssystem-Updates KB4490628 (12. März 2019) und KB4474419 (23. September 2019) nicht installiert sind.

Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows Server 2016 und Microsoft Windows Server 2019 finden Sie in der Wissensdatenbank des Technischen Supports.

Einzelheiten zur Unterstützung des Betriebssystems Microsoft Windows Server 2022 finden Sie in der Wissensdatenbank des Technischen Supports.

Nicht unterstützte Betriebssysteme für Server:

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

Virtuelle Plattformen

Unterstützte virtuelle Plattformen für den Programmbetrieb im Standardmodus:

- VMware Workstation Pro 15.5.2
- VMware ESXi 7.0 Patch-Version ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

Das Programm unterstützt virtuelle Maschinen unter Windows 11 Pro Arm64, die mit Hyper-V erstellt wurden.

Virtuelle Maschinen für die Light Agent-Installation

Die Installation von Kaspersky Endpoint Security im Light Agent-Modus auf Arm-basierten virtuellen Maschinen wird nicht unterstützt.

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

Auf virtuellen Maschinen müssen die folgenden Pakete und Dienstprogramme installiert sein:

- Bei Verwendung von Microsoft Hyper-V: Integration Services-Paket.
- Bei Verwendung von VMware vSphere: VMware Tools-Paket.
- Bei Verwendung von XenServer: XenTools-Paket.
- Bei Verwendung von HUAWEI FusionSphere: HUAWEI Tools-Paket.
- Bei Verwendung von KVM-basierten Hypervisoren – QEMU Guest Agent.

Die Anforderungen an die virtuelle Infrastruktur, um das Programm im Light Agent-Modus auszuführen, finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Damit das Programm korrekt funktioniert, verwenden Sie eine virtualisierte Netzwerkschnittstelle mit einer Bandbreite von mindestens 100 Mbit/s.

Terminalserver

Unterstützte Terminalserver-Typen:

- Microsoft Remote Desktop Services basierend auf Windows Server 2008 R2 SP1
- Microsoft Remote Desktop Services basierend auf Windows Server 2012
- Microsoft Remote Desktop Services basierend auf Windows Server 2012 R2
- Microsoft Remote Desktop Services basierend auf Windows Server 2016
- Microsoft Remote Desktop Services basierend auf Windows Server 2019
- Microsoft Remote Desktop Services basierend auf Windows Server 2022
- Microsoft Remote Desktop Services basierend auf Windows Server 2025
- Citrix RDSH in Citrix Virtual Apps and Desktops 7 2507 LTSR enthalten

Kaspersky Security Center Support

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

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

Vergleich der Programmfunktionen im Hinblick auf den Typ des Betriebssystems

Die Auswahl der für Kaspersky Endpoint Security verfügbaren Funktionen ist vom Typ des Betriebssystems abhängig: Workstation oder Server (siehe folgende Tabelle).

Ab der Version Kaspersky Endpoint Security12.8 für Windows können Sie im Installationspaket verschiedene Komponentensätze für verschiedene Betriebssystemtypen konfigurieren. Sie können das Programm also mithilfe desselben Installationspakets auf Workstations und Servern bereitstellen.

Die Installation von Kaspersky Endpoint Security im Light Agent-Modus auf Arm-basierten virtuellen Maschinen wird nicht unterstützt.

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Workstation	Arm-basierte Workstation	Server	Server Core-Modus
Erweiterter Schutz				
Kaspersky Security Network	✓	✓	✓	✓

Funktion	Workstation	Arm-basierte Workstation	Server	Server Core-Modus
Verhaltensanalyse	✓	✓	✓	✓
Schutz vor Verschlüsselung	✓	✓	✓	✓
Exploit-Prävention	✓	✓	✓	✓
Programm-Überwachung	✓	✓	–	–
Rollback von schädlichen Aktionen	✓	✓	✓	✓
Basisschutz				
Schutz vor bedrohlichen Dateien	✓	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓	–
Schutz vor E-Mail-Bedrohungen	✓	✓	✓	–
Firewall	✓	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓	✓
Schutz vor BadUSB-Angriffen	✓	✓	✓	–
AMSI-Schutz	✓	✓	✓	✓
Sicherheitskontrolle				
Protokollanalyse	–	–	✓	–
Programmkontrolle	✓	✓	✓	✓
Gerätekontrolle	✓	✓	✓	✓
Web-Kontrolle	✓	✓	✓	–
Adaptive Kontrolle von Anomalien	✓	✓	–	–
Überwachung der Systemintegrität	–	–	✓	–
Cloud Discovery	✓	✓	–	–
Datenverschlüsselung				
Kaspersky-Festplattenverschlüsselung	✓	–	–	–
BitLocker-Laufwerkverschlüsselung	✓	✓	✓	✓
Verschlüsselung auf Dateiebene	✓	–	–	–
Verschlüsselung von Wechseldatenträgern	✓	–	–	–
Detection and Response				
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
KUMA-Integration	✓	✓	✓	✓

Vergleich der Programmfunktionen in Abhängigkeit der Verwaltungs-Tools

Die Auswahl der verfügbaren Funktionen für Kaspersky Endpoint Security ist von den Verwaltungs-Tools abhängig (s. folgende Tabelle).

Sie können das Programm mithilfe der folgenden Konsolen von Kaspersky Security Center verwalten:

- Verwaltungskonsole. Snap-In für Microsoft Management Console (MMC), das am Administrator-Arbeitsplatz installiert wird.
- Web Console. Komponente von Kaspersky Security Center, die auf dem Administrationsserver installiert wird. Sie können in der Web Console über einen Browser auf einem beliebigen Computer arbeiten.

Sie können das Programm auch mithilfe von Kaspersky Security Center Cloud Console verwalten. *Kaspersky Security Center Cloud Console* ist eine Cloud-Version von Kaspersky Security Center. In diesem Fall sind Administrationsserver und andere Komponenten von Kaspersky Security Center in einer Cloud-Infrastruktur von Kaspersky installiert. Details über die Programmverwaltung mithilfe von „Kaspersky Security Center Cloud Console" finden Sie in der Hilfe zu „Kaspersky Security Center Cloud Console".

Kaspersky Endpoint Security ist Teil der Lösung Kaspersky Next Pro View. Weitere Informationen zu den verfügbaren Funktionen der App, die als Teil dieser Lösung verwendet wird, finden Sie in der Hilfe zu Kaspersky Next.

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Kaspersky Security Center		Kaspersky Security Center
	Verwaltungskonsole	Web Console	Cloud Console
Erweiterter Schutz			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
Verhaltensanalyse	✓	✓	✓
Schutz vor Verschlüsselung			
Exploit-Prävention	✓	✓	✓
Programm-Überwachung	✓	✓	✓
Rollback von schädlichen Aktionen	✓	✓	✓
Basisschutz			
Schutz vor bedrohlichen Dateien	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	✓	✓	✓
Firewall	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓
Schutz vor BadUSB-Angriffen	✓	✓	✓
AMSI-Schutz	✓	✓	✓
Sicherheitskontrolle			
Protokollanalyse	✓	✓	✓
Programmkontrolle	✓	✓	✓
Gerätekontrolle	✓	✓	✓
Web-Kontrolle	✓	✓	✓
Adaptive Kontrolle von Anomalien	✓	✓	✓
Überwachung der Systemintegrität	✓	✓	✓
Cloud Discovery	–	–	✓

Funktion	Kaspersky Security Center		Kaspersky Security Center
	Verwaltungskonsole	Web Console	Cloud Console
Datenverschlüsselung			
Kaspersky-Festplattenverschlüsselung	✓	✓	–
BitLocker-Laufwerkverschlüsselung	✓	✓	✓
Verschlüsselung auf Dateiebene	✓	✓	–
Verschlüsselung von Wechseldatenträgern	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
KUMA-Integration	✓	✓	✓
Aufgaben			
Schlüssel hinzufügen	✓	✓	✓
Auswahl der Programmkomponenten ändern	✓	✓	✓
Inventarisierung	✓	✓	✓
Update	✓	✓	✓
Update-Rollback	✓	✓	✓
Schadsoftware-Untersuchung	✓	✓	✓
Prüfung der Anwendungsintegrität	✓	✓	–
Daten zurücksetzen	✓	✓	✓
Authentifizierungsagenten-Konten verwalten (Kaspersky-Festplattenverschlüsselung)	✓	✓	–
IOC-Untersuchung (EDR)	–	✓	✓
Datei in Quarantäne verschieben (EDR)	–	✓	✓
Datei anfordern (EDR)	–	✓	✓
Datei löschen (EDR)	–	✓	✓
Prozess starten (EDR)	–	✓	✓
Prozess beenden (EDR)	–	✓	✓

Kompatibilität mit anderen Programmen

Kaspersky Endpoint Security ist inkompatibel zu einigen Anwendungen von Kaspersky und von Drittanbietern. Deshalb überprüft Kaspersky Endpoint Security, ob solche Programme auf dem Computer vorhanden sind, bevor das Programm installiert und aktualisiert wird oder die Programmkomponenten geändert werden.

Kompatibilität mit Drittanbieter-Programmen

Kaspersky Endpoint Security ist nicht kompatibel mit Programmen, die zu EPP-Lösungen (Endpoint Protection Platform, EPP) von Drittanbietern gehören. Es kann auch zu Kompatibilitätsproblemen zwischen Kaspersky Endpoint Security und anderen Anwendungen kommen. Um die Kompatibilität zu ermitteln, verwendet Kaspersky Endpoint Security eine von Kaspersky erstellte Liste mit Anwendungen. Diese Liste ist in der Datei incompatible.txt enthalten. Diese Datei ist im Lieferumfang enthalten.

Kaspersky garantiert nicht für die Kompatibilität von Kaspersky Endpoint Security mit Anwendungen aus der Liste. Wenn eine Anwendung aus der Liste gefunden wird, unterbricht das Installationsprogramm die Bereitstellung von Kaspersky Endpoint Security. Möglicherweise löscht das Installationsprogramm einige Anwendung, die sich auf der Liste befinden. Wenn Sie trotz der Risiken Kaspersky Endpoint Security dennoch zusammen mit einer Anwendung aus der Liste auf demselben Computer installieren möchten, können Sie die Computerprüfung überspringen (siehe Anleitung unten).

DATEI „INCOMPATIBLE.TXT“ HERUNTERLADEN

Kompatibilität mit Kaspersky-Programmen

Das Programm Kaspersky Endpoint Security ist nicht mit folgenden Kaspersky-Programmen kompatibel:

- Kaspersky Standard | Plus | Premium.
- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Endpoint Sensor als Teil der Kaspersky Anti Targeted Attack Platform und der Kaspersky Endpoint Detection and Response-Lösungen.
- Kaspersky Endpoint Agent als Teil der Detection and Response-Lösungen von Kaspersky.

  Kaspersky stellt Detection and Response komplett von Kaspersky Endpoint Agent auf die Verwendung mit dem integrierten Kaspersky Endpoint Security-Agenten um. Ab Version 12.1 unterstützt die App alle Detection and Response-Lösungen.

- Kaspersky Security for Virtualization Light Agent.

- Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security für Windows Server

  Ab Kaspersky Endpoint Security 12.0 können Sie von Kaspersky Security für Windows Server zu Kaspersky Endpoint Security für Windows migrieren und haben damit eine einheitliche Lösung zum Schutz von Workstations und Servern.

- Kaspersky Embedded Systems Security.

Falls auf dem Computer Kaspersky-Programme aus dieser Liste installiert sind, werden diese Programme durch Kaspersky Endpoint Security entfernt. Warten Sie bis zum Abschluss des Vorgang, um die Installation von Kaspersky Endpoint Security fortzusetzen.

Überspringen der Suche nach Anwendungen mit möglichen Kompatibilitätsproblemen

Wenn Kaspersky Endpoint Security ein Programm aus der Liste incompatible.txt erkennt, wird die Installation des Programms abgebrochen. Um mit der Installation fortzufahren, müssen Sie die erkannte Anwendung zunächst entfernen. Sofern der Hersteller der Drittanbieter-Software in seiner Dokumentation angibt, dass seine Software mit Endpoint Protection Platform (EPP) kompatibel ist, können Sie Kaspersky Endpoint Security aber trotzdem auf einem Computer installieren, auf dem sich ein Programm dieses Herstellers befindet. Beispiel: Der Dienstanbieter der Lösung Endpoint Detection and Response (EDR) kann erklären, dass sein Produkt mit Drittanbieter-EPP-Systemen kompatibel ist. In diesem Fall müssen Sie die Installation von Kaspersky Endpoint Security ohne eine Überprüfung der bereits installierten Software starten. Geben Sie dazu die folgenden Parameter für das Installationsprogramm an:

- `SKIPPRODUCTCHECK=1` – Deaktiviert die Überprüfung auf installierte Software. Eine Liste der Software, die Kompatibilitätsprobleme verursachen kann, befindet sich in der Datei „incompatible.txt“, die zum Lieferumfang gehört. Ist dieser Parameter nicht angegeben, so wird beim Fund von Software aus der Liste die Installation von Kaspersky Endpoint Security abgebrochen.
- `SKIPPRODUCTUNINSTALL=1` – Deaktiviert das automatische Entfernen gefundener Anwendungen aus der Liste incompatible.txt. Wenn dieser Parameter nicht angegeben ist, versucht Kaspersky Endpoint Security, die Anwendungen zu entfernen, die Kompatibilitätsprobleme verursachen können.
- `CLEANERSIGNCHECK=0` – Deaktiviert die Überprüfung der digitalen Signatur von Anwendungen, die bei der Untersuchung gefunden wurden. Wenn dieser Parameter nicht festgelegt ist, wird die Überprüfung digitaler Signaturen bei der Bereitstellung der App über Kaspersky Security Center deaktiviert. Wenn die App lokal installiert wurde, ist die Überprüfung digitaler Signaturen standardmäßig aktiviert.

Sie können die Parameter in der Befehlszeile angeben, wenn Sie das Programm lokal installieren.

Falls Sie die Suche nach Programmen, die Kompatibilitätsprobleme verursachen können, während der Installation übersprungen haben, führt Kaspersky Endpoint Security diese Prüfung möglicherweise erneut durch, wenn sich die Auswahl der Programmkomponenten ändert. Um die Suche nach installierter Software zu überspringen, müssen Sie die Aufgabe *Auswahl der Programmkomponenten ändern* konfigurieren.

Beispiel:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

Um Kaspersky Endpoint Security per Fernzugriff zu installieren, müssen Sie die entsprechenden Parameter zur Installationspaket-Generierungsdatei `kes_win.kud` im Abschnitt `[Setup]` hinzufügen (siehe unten). Die Datei `kes_win.kud` ist im Lieferumfang enthalten.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

Programm installieren und deinstallieren

Um das Programm Kaspersky Endpoint Security auf einem Computer zu installieren, gibt es folgende Möglichkeiten:

- lokal mithilfe des Installationsassistenten für das Programm.
- lokal aus der Befehlszeile
- per Fernzugriff mithilfe von Kaspersky Security Center.
- per Fernzugriff über den Gruppenrichtlinien-Editor von Microsoft Windows (Details finden Sie auf der Website des technischen Supports von Microsoft).
- per Fernzugriff mithilfe von System Center Configuration Manager

Es gibt mehrere Methoden, um die Einstellungen für die Programminstallation anzupassen. Falls Sie gleichzeitig mehrere Methoden für die Anpassung von Einstellungen verwenden, übernimmt Kaspersky Endpoint Security die Einstellungen mit der höchsten Priorität. Für die Prioritäten verwendet Kaspersky Endpoint Security die folgende Reihenfolge:

1. Einstellungen, die aus der Datei setup.ini stammen.
2. Einstellungen, die aus der Datei installer.ini stammen.
3. Einstellungen, die aus der Befehlszeile stammen.
4. Einstellungen, die aus der Konfigurationsdatei (install.cfg) stammen.

Es wird empfohlen, vor Beginn der Installation von Kaspersky Endpoint Security (auch vor einer Remote-Installation) alle laufenden Programme zu schließen.

Bei der Installation von Kaspersky Endpoint Security zeigt das Betriebssystem möglicherweise eigene Meldungen an. Außerdem können während der Programminstallation die Netzwerk- und Internetverbindung unterbrochen werden.

Bei der Installation, beim Update oder bei der Deinstallation von Kaspersky Endpoint Security können Fehler auftreten. Weitere Informationen zur Behebung dieser Fehler finden Sie in der Wissensdatenbank des Technischen Supports.

Software-Verteilung über Kaspersky Security Center

Es gibt mehrere Methoden, um Kaspersky Endpoint Security auf den Computern im Unternehmensnetzwerk zu verteilen. Sie können die für Ihr Unternehmen geeignete Verteilungsmethode auswählen oder mehrere Verteilungsmethoden gleichzeitig verwenden. Bevor Sie das Programm installieren, müssen Sie sicherstellen, dass der Administrationsagent von Kaspersky Security Center auf dem Computer installiert ist. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer.

Kaspersky Security Center unterstützt die folgenden grundlegenden Verteilungsmethoden:

- Installation des Programms mithilfe des Softwareverteilungs-Assistenten.

  Die standardmäßige Installationsmethode bietet sich an, wenn die standardmäßigen Einstellungen von Kaspersky Endpoint Security für Sie passend sind und Ihr Unternehmen eine einfache Infrastruktur aufweist, die keine speziellen Einstellungen erforderlich macht.

- Installation des Programms mithilfe einer Aufgabe zur Remote-Installation.

  Diese universelle Installationsmethode erlaubt es, die Einstellungen von Kaspersky Endpoint Security anzupassen und die Aufgaben zur Remote-Installation flexibel zu verwalten. Die Installation von Kaspersky Endpoint Security besteht aus den folgenden Schritten:

  1. Erstellung eines Installationspakets;
  2. Erstellung einer Aufgabe zur Remote-Installation.

Kaspersky Security Center unterstützt auch andere Methoden für die Installation von Kaspersky Endpoint Security, beispielsweise die Software-Verteilung im Rahmen eines Abbilds des Betriebssystems. Nähere Informationen zu anderen Methoden der Softwareverteilung finden Sie in der Hilfe zu Kaspersky Security Center.

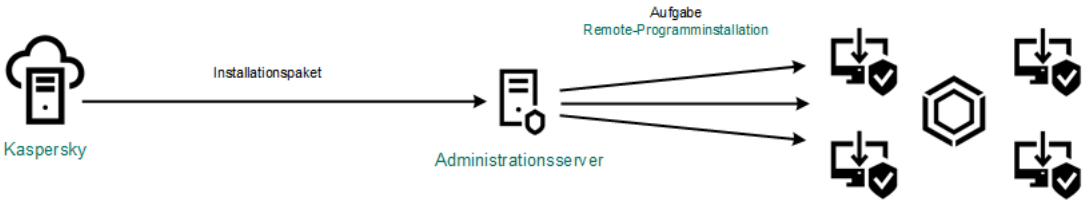
Standardmäßige Installation des Programms

Für die Programminstallation auf den Computern Ihres Unternehmens ist in Kaspersky Security Center ein Assistent für die Verteilung des Schutzes vorgesehen. Der Assistent für die Verteilung des Schutzes bietet die folgenden Basisaktionen:

1. Auswahl eines Installationspakets für Kaspersky Endpoint Security.

   Ein *Installationspaket* ist eine Auswahl von Dateien, welche mithilfe von Kaspersky Security Center für die Remote-Installation eines Kaspersky-Programms erstellt wird. Das Installationspaket enthält eine Auswahl von Einstellungen, welche für die Programminstallation erforderlich sind und die Funktionsfähigkeit direkt nach der Installation gewährleisten. Das Installationspaket wird auf Basis von Dateien mit den Erweiterungen kpd und kud erstellt, die zum Programmpaket gehören. Das Installationspaket für Kaspersky Endpoint Security ist für alle unterstützten Versionen des Betriebssystems Windows und Typen der Prozessorarchitektur gleich.

2. Erstellen der Aufgabe *Remote-Installation einer Anwendung* für den Administrationsservers von Kaspersky Security Center.



Verteilung von Kaspersky Endpoint Security

Start des Assistenten für die Verteilung des Schutzes in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Remote-Installation** aus.
3. Klicken Sie auf den Link **Installationspakete auf den verwalteten Geräten (Workstations) bereitstellen**.

   Dadurch wird der Softwareverteilungs-Assistent gestartet. Folgen Sie den Anweisungen.

Auf dem Client-Computer müssen die folgenden Ports geöffnet werden: TCP 139 und 445, UDP 137 und 138.

Schritt 1. Installationspaket auswählen

Wählen Sie in der Liste der Installationspakete das Paket für Kaspersky Endpoint Security aus. Wenn das Installationspaket für Kaspersky Endpoint Security nicht auf der Liste steht, können Sie das Paket mithilfe des Assistenten erstellen.

Sie können die Einstellungen des Installationspakets im Kaspersky Security Center konfigurieren. Sie können zum Beispiel die Programmkomponenten auswählen, die auf einem Computer installiert werden sollen.

Zusammen mit Kaspersky Endpoint Security wird auch der Administrationsagent installiert. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

Schritt 2.

Wählen Sie die Quelle **Paket von Kaspersky Security Center bereitstellen** aus.

Schritt 3. Geräte für die Installation auswählen

Wählen Sie die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. Auf nicht zugeordneten Geräten ist der Administrationsagent nicht installiert. In diesem Fall wird die Aufgabe einer Auswahl von Geräten zugewiesen. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Einstellungen für die Aufgabe zur Remote-Installation festlegen

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Installationspakets erzwingen**. Wählen Sie die Mittel für die Programminstallation aus:
  - **Unter Nutzung des Administrationsagenten**. Der Administrationsagent ist dafür verantwortlich, das Installationspaket für Kaspersky Endpoint Security auf den Client-Computern bereitzustellen. Wenn der Administrationsagent nicht installiert ist, wird die Aufgabe mit einem Fehler beendet. Fügen Sie in diesem Fall das Installationspaket des Administrationsagenten zur Aufgabe *Remote-Installation einer Anwendung* hinzu und aktivieren Sie die Dateiübermittlung über die Betriebssystemressourcen. Dann wird der Administrationsagent mithilfe der Betriebssystemressourcen installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.
  - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Weitere Informationen über die Verwendung von Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center.
  - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.
- **Verhalten bei Geräten, die durch andere Administrationsserver verwaltet werden**. Wählen Sie eine Installationsmethode für Kaspersky Endpoint Security aus. Wenn in einem Netzwerk mehr als ein Administrationsserver installiert ist, können diese Server ein und denselben Client-Computer sehen. Dies kann beispielsweise dazu führen, dass ein bestimmtes Programm von mehreren Administrationsservern im Remote-Modus auf demselben Client-Computer installiert wird, oder dass andere Konflikte auftreten.

- **Anwendung nicht neu installieren, wenn sie bereits installiert ist**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beispielsweise eine ältere Version des Programms installieren möchten.

- **Installation des Administrationsagenten in Gruppenrichtlinien des Active Directory festlegen**. Manuelle Installation des Administrationsagenten mit Active Directory-Mitteln. Für die Installation des Administrationsagenten muss die Aufgabe zur Remote-Installation mit den Rechten des Domänenadministrators ausgeführt werden.

Schritt 5. Lizenzschlüssel auswählen

Fügen Sie zum Installationspaket einen Schlüssel für die Programmaktivierung hinzu. Dieser Schritt ist optional. Falls sich auf dem Administrationsserver ein Lizenzschlüssel mit automatischer Verteilungsfunktion befindet, wird der Schlüssel später automatisch hinzugefügt. Sie können die App auch später mithilfe der Aufgabe *Schlüssel hinzufügen* aktivieren.

Schritt 6. Einstellungen für den Neustart des Betriebssystems auswählen

Wählen Sie aus, welche Aktion ausgeführt wird, wenn ein Neustart des Computers erforderlich ist. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.

Schritt 7. Inkompatible Programme vor der Programminstallation entfernen

Überprüfen Sie die Liste der inkompatiblen Programme und erlauben Sie die Deinstallation dieser Programme. Wenn auf dem Computer inkompatible Programme installiert sind, wird die Installation von Kaspersky Endpoint Security mit einem Fehler beendet.

Schritt 8. Benutzerkonto für den Zugriff auf Geräte auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 9. Installation starten

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Start des Assistenten für die Verteilung des Schutzes in „Web Console“ und „Cloud Console”

Klicken Sie im Web Console-Hauptfenster auf **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Assistent für die Bereitstellung des Schutzes**.

Dadurch wird der Softwareverteilungs-Assistent gestartet. Folgen Sie den Anweisungen.

Auf dem Client-Computer müssen die folgenden Ports geöffnet werden: TCP 139 und 445, UDP 137 und 138.

Schritt 1. Installationspaket auswählen

Wählen Sie in der Liste der Installationspakete das Paket für Kaspersky Endpoint Security aus. Wenn das Installationspaket für Kaspersky Endpoint Security nicht auf der Liste steht, können Sie das Paket mithilfe des Assistenten erstellen. Um ein Installationspaket zu erstellen, ist es nicht erforderlich, das Programmpaket zu suchen und auf dem Computer zu speichern. In Kaspersky Security Center ist eine Liste der Programmpakete verfügbar, die sich auf den Kaspersky-Servern befinden, und die Erstellung des Installationspakets wird automatisch ausgeführt. Die Liste wird von Kaspersky aktualisiert, wenn neue Programmversionen erschienen sind.

Sie können die Einstellungen des Installationspakets im Kaspersky Security Center konfigurieren. Sie können zum Beispiel die Programmkomponenten auswählen, die auf einem Computer installiert werden sollen.

Schritt 2. Lizenzschlüssel auswählen

Fügen Sie zum Installationspaket einen Schlüssel für die Programmaktivierung hinzu. Dieser Schritt ist optional. Falls sich auf dem Administrationsserver ein Lizenzschlüssel mit automatischer Verteilungsfunktion befindet, wird der Schlüssel später automatisch hinzugefügt. Sie können die App auch später mithilfe der Aufgabe *Schlüssel hinzufügen* aktivieren.

Schritt 3. Administrationsagent auswählen

Wählen Sie die Version des Administrationsagenten aus, der zusammen mit Kaspersky Endpoint Security installiert werden soll. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

Schritt 4. Geräte für die Installation auswählen

Wählen Sie die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. Auf nicht zugeordneten Geräten ist der Administrationsagent nicht installiert. In diesem Fall wird die Aufgabe einer Auswahl von Geräten zugewiesen. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 5. Erweiterte Einstellungen anpassen

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Installationspakets erzwingen**. Wählen Sie die Mittel für die Programminstallation aus:
  - **Unter Nutzung des Administrationsagenten**. Der Administrationsagent ist dafür verantwortlich, das Installationspaket für Kaspersky Endpoint Security auf den Client-Computern bereitzustellen. Wenn der Administrationsagent nicht installiert ist, wird die Aufgabe mit einem Fehler beendet. Fügen Sie in diesem Fall das Installationspaket des Administrationsagenten zur Aufgabe *Remote-Installation einer Anwendung* hinzu und aktivieren Sie die Dateiübermittlung über die Betriebssystemressourcen. Dann wird der Administrationsagent mithilfe der Betriebssystemressourcen installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.
  - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Weitere Informationen über die Verwendung von Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center.
  - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.
- **Anwendung nicht neu installieren, wenn sie bereits installiert ist**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beispielsweise eine ältere Version des Programms installieren möchten.
- **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**. Die Installation von Kaspersky Endpoint Security wird manuell mit den Mitteln des Administrationsagenten oder mit den Mitteln von Active Directory ausgeführt. Für die Installation des Administrationsagenten muss die Aufgabe zur Remote-Installation mit den Rechten des Domänenadministrators ausgeführt werden.

Schritt 6. Einstellungen für den Neustart des Betriebssystems auswählen

Wählen Sie aus, welche Aktion ausgeführt wird, wenn ein Neustart des Computers erforderlich ist. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.

Schritt 7. Inkompatible Programme vor der Programminstallation entfernen

Überprüfen Sie die Liste der inkompatiblen Programme und erlauben Sie die Deinstallation dieser Programme. Wenn auf dem Computer inkompatible Programme installiert sind, wird die Installation von Kaspersky Endpoint Security mit einem Fehler beendet.

Schritt 8. In eine Administrationsgruppe verschieben

Wählen Sie die Administrationsgruppe aus, in welche die Computer nach der Installation des Administrationsagenten verschoben werden sollen. Das Verschieben in eine Administrationsgruppe ist erforderlich, um Richtlinien und Gruppenaufgaben anzuwenden. Wenn ein Computer bereits zu einer Administrationsgruppe gehört, wird der Computer nicht mehr verschoben. Wenn Sie keine Administrationsgruppe auswählen, werden Computer zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt.

Schritt 9. Benutzerkonto für den Zugriff auf Geräte auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 10. Installation starten

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Erstellung eines Installationspakets

Ein *Installationspaket* ist eine Auswahl von Dateien, welche mithilfe von Kaspersky Security Center für die Remote-Installation eines Kaspersky-Programms erstellt wird. Das Installationspaket enthält eine Auswahl von Einstellungen, welche für die Programminstallation erforderlich sind und die Funktionsfähigkeit direkt nach der Installation gewährleisten. Das Installationspaket wird auf Basis von Dateien mit den Erweiterungen kpd und kud erstellt, die zum Programmpaket gehören. Das Installationspaket für Kaspersky Endpoint Security ist für alle unterstützten Versionen des Betriebssystems Windows und Typen der Prozessorarchitektur gleich.

Erstellen eines Installationspakets in der Verwaltungskonsole (MMC)

1. Gehen Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Erweitert** → **Remote-Installation** → **Installationspakete**.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.

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

Der Assistent zur Erstellung eines Installationspakets wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Typ des Installationspakets auswählen

Wählen Sie die Option **Installationspaket für eine Kaspersky-Anwendung erstellen** aus.

Schritt 2. Namen des Installationspakets festlegen

Geben Sie einen Namen für das Installationspaket ein (z. B. *Kaspersky Endpoint Security für Windows 14.2*).

Schritt 3. Programmpaket für die Installation auswählen

Klicken Sie auf **Durchsuchen** und wählen Sie die Datei `kes_win.kud` aus, die zum Lieferumfang gehört.

Aktualisieren Sie bei Bedarf die Antiviren-Datenbanken im Installationspaket mithilfe des Kontrollkästchens **Updates aus der Datenverwaltung ins Installationspaket kopieren**.

Schritt 4. Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie

Lesen und akzeptieren Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie.

Das Installationspaket wird erstellt und zu Kaspersky Security Center hinzugefügt. Mithilfe des Installationspakets können Sie Kaspersky Endpoint Security auf den Computern des Unternehmensnetzwerks installieren oder die Programmversion aktualisieren.

In den Einstellungen des Installationspakets können Sie Programmkomponenten für verschiedene Betriebssystemtypen auswählen. Das Installationspaket enthält zwei Komponentensätze: für Workstations und für Server. Vor der Bereitstellung des Installationspakets ermittelt das Installationsprogramm den Typ des Betriebssystems und installiert nur die Programmkomponenten, die Sie für diesen Betriebssystemtyp ausgewählt haben. Sie können also dasselbe Installationspaket für Workstations und Server verwenden.

Das Installationspaket enthält die Antiviren-Datenbanken aus der Datenverwaltung des Administrationsservers. Sie können die Datenbanken im Installationspaket aktualisieren, um das Volumen des Datenverkehrs beim Datenbanken-Update nach der Installation von Kaspersky Endpoint Security zu reduzieren.

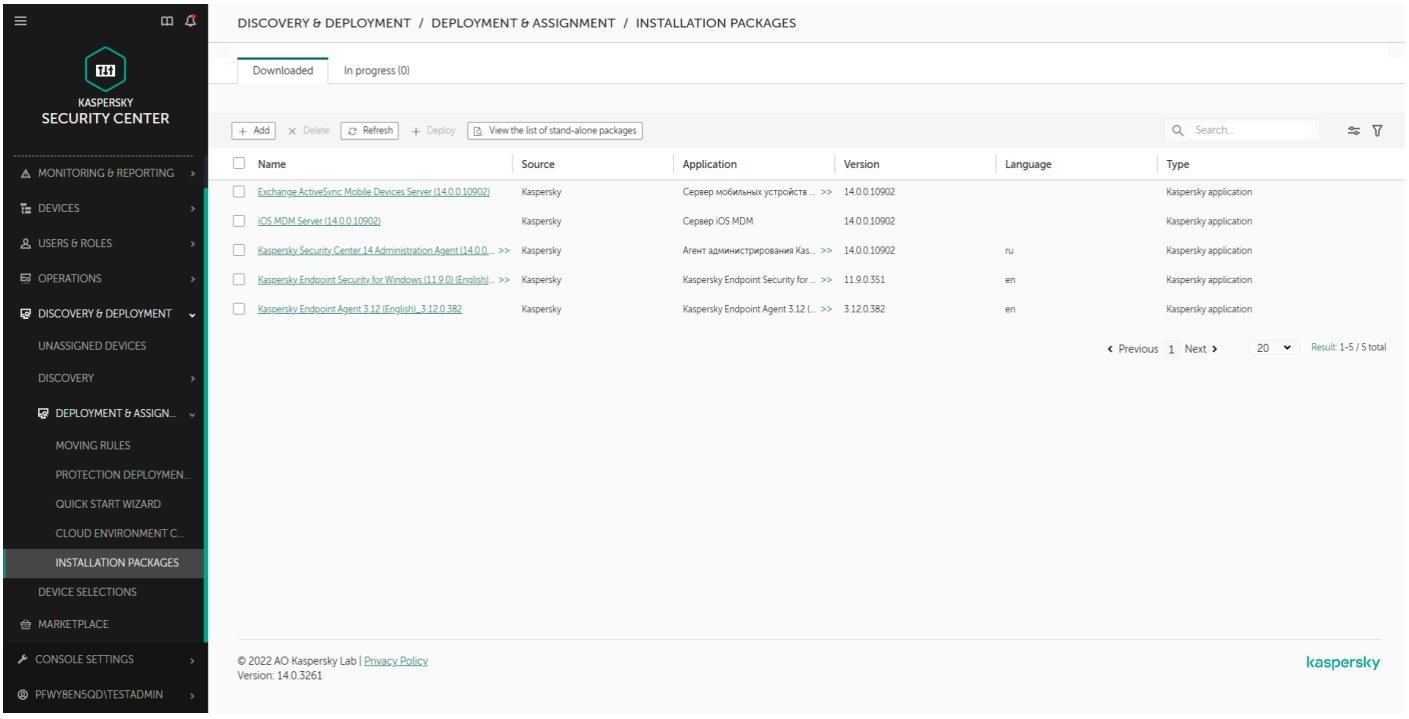
So erstellen Sie ein Installationspaket in der Web Console:

1. Klicken Sie im Web Console-Hauptfenster auf **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent zur Erstellung eines Installationspakets wird gestartet. Folgen Sie den Anweisungen.



Liste der Installationspakete

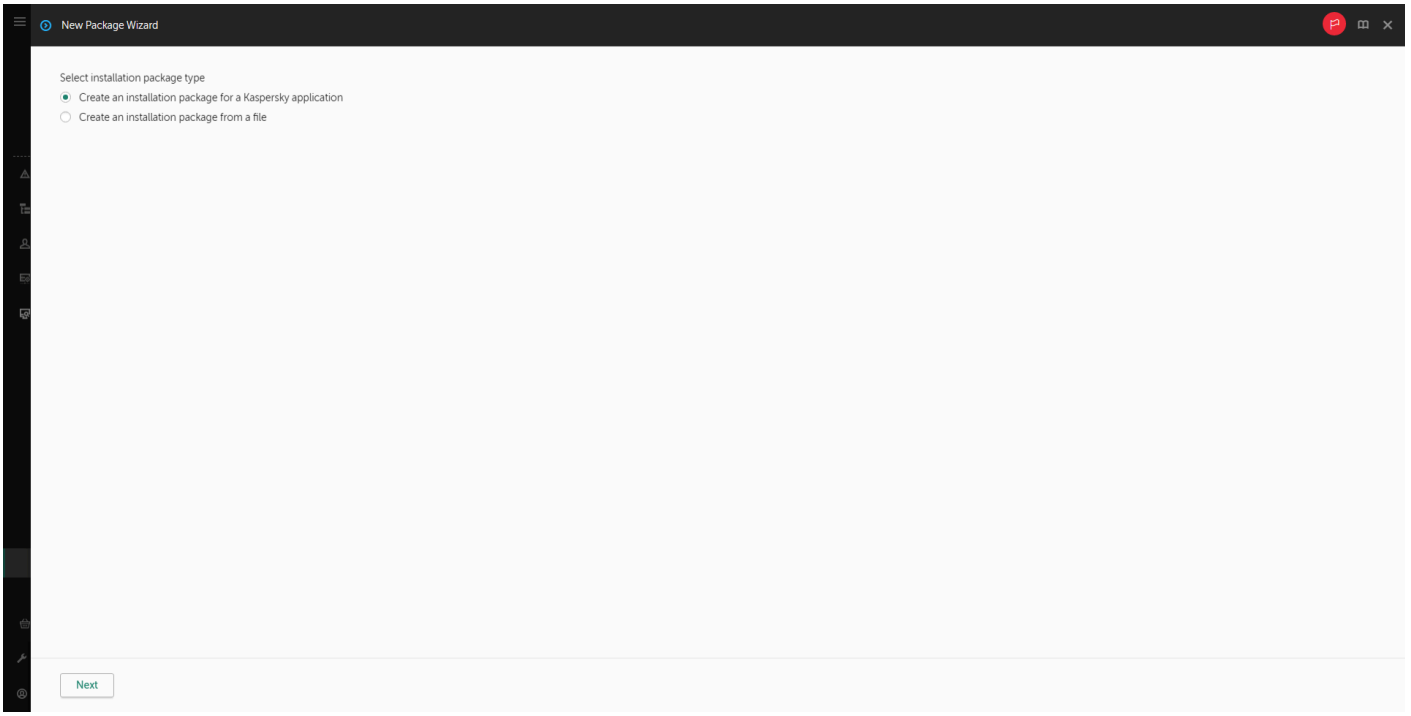
Schritt 1. Typ des Installationspakets auswählen

Wählen Sie die Option **Installationspaket für eine Kaspersky-Anwendung erstellen** aus.

Der Assistent erstellt ein Installationspaket aus dem Programmpaket, das sich auf den Kaspersky-Servern befindet. Die Liste wird automatisch aktualisiert, wenn neue Programmversionen erscheinen. Es wird empfohlen, für die Installation von Kaspersky Endpoint Security diese Variante auszuwählen.

Außerdem können Sie ein Installationspaket aus einer Datei erstellen.

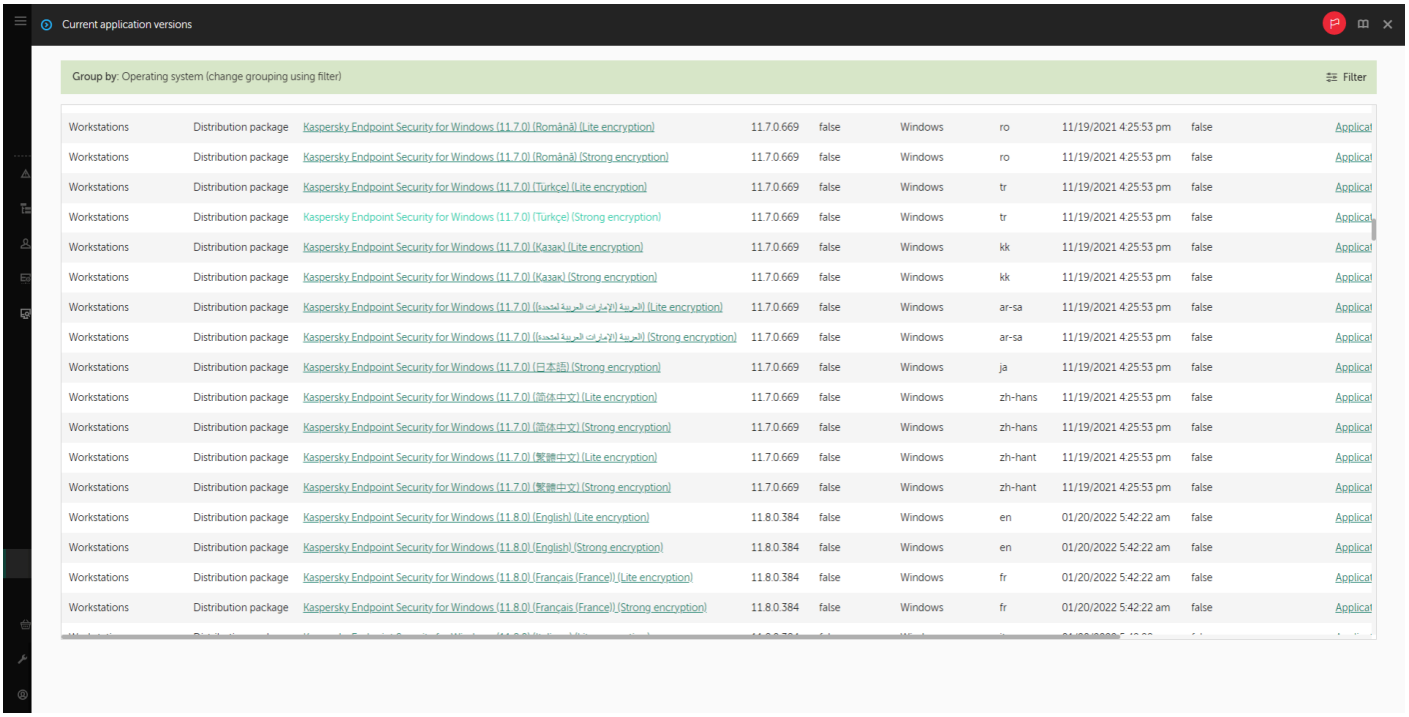
Das Erstellen eines Installationspakets für Kaspersky Endpoint Security aus einer Datei ist nur in Kaspersky Security Center Web Console möglich.



Arten von Installationspaketen

Schritt 2. Installationspakete

Wählen Sie das Installationspaket für Kaspersky Endpoint Security für Windows aus. Der Vorgang zur Erstellung des Installationspakets wird gestartet. Während das Installationspaket erstellt wird, müssen die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie akzeptiert werden.

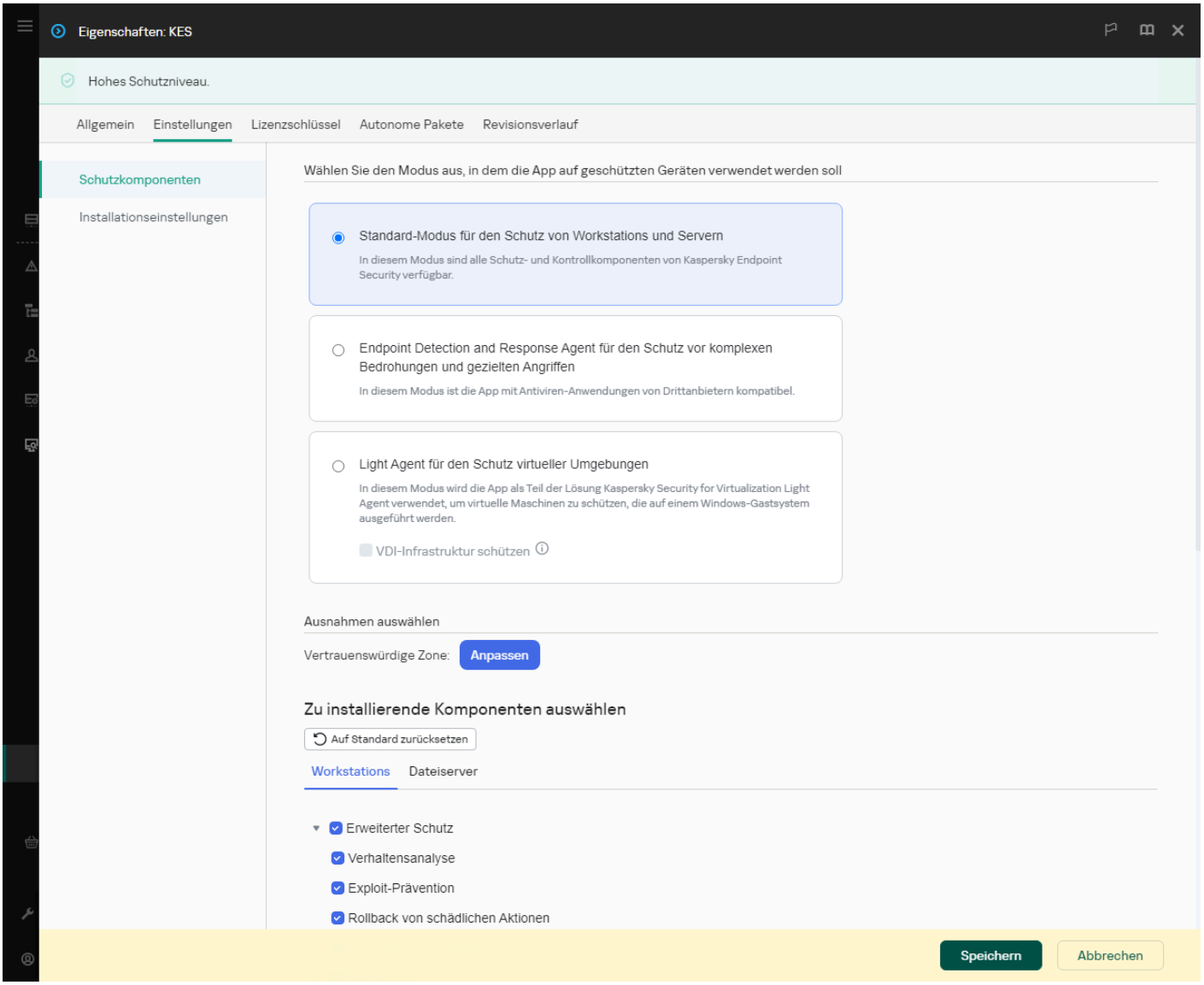


Liste der Installationspakete auf den Kaspersky-Servern

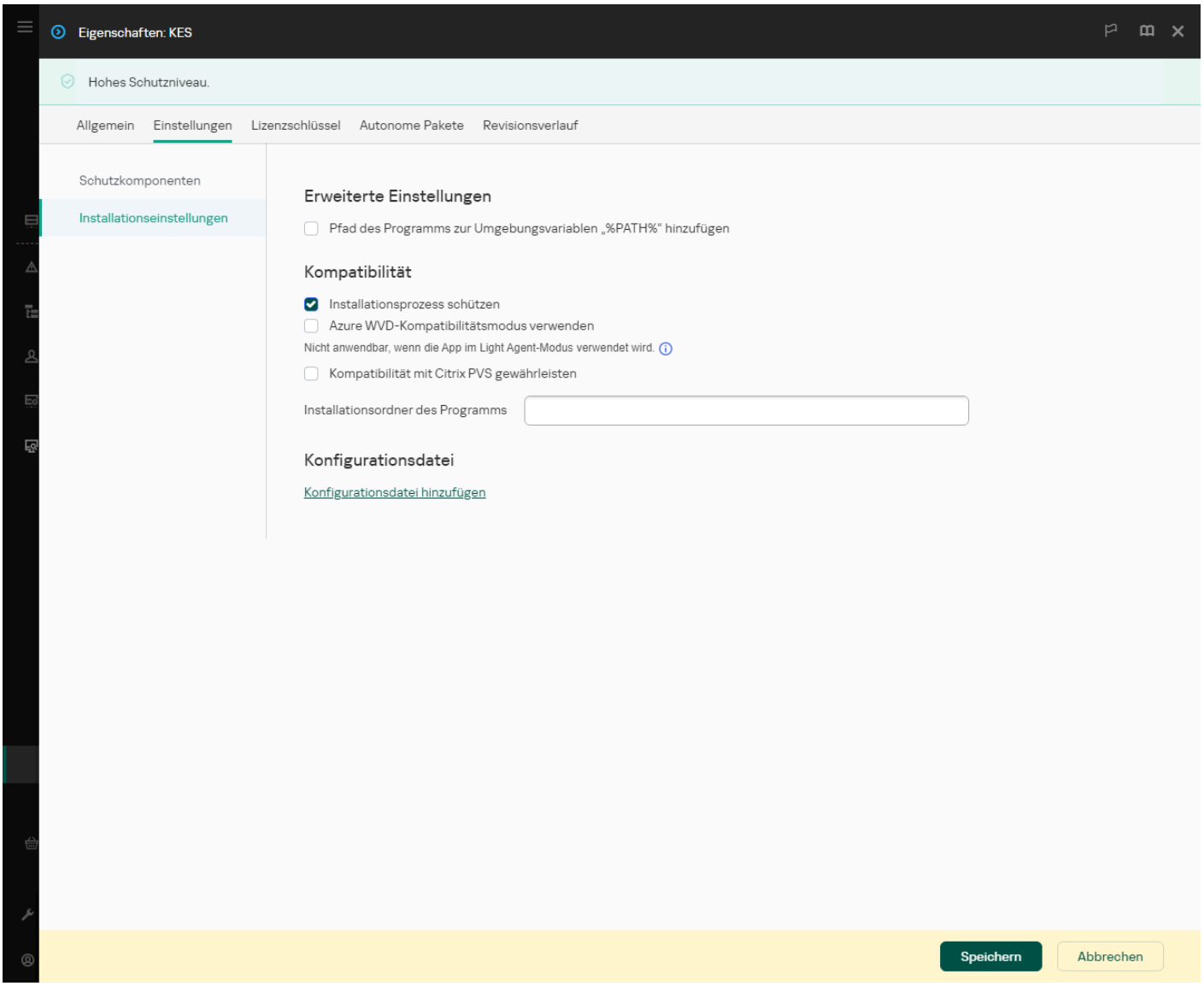
Das Installationspaket wird erstellt und zu Kaspersky Security Center hinzugefügt. Mithilfe des Installationspakets können Sie Kaspersky Endpoint Security auf den Computern des Unternehmensnetzwerks installieren oder die Programmversion aktualisieren.

In den Einstellungen des Installationspakets können Sie Programmkomponenten für verschiedene Betriebssystemtypen auswählen. Das Installationspaket enthält zwei Komponentensätze: für Workstations und für Server. Vor der Bereitstellung des Installationspakets ermittelt das Installationsprogramm den Typ des Betriebssystems und installiert nur die Programmkomponenten, die Sie für diesen Betriebssystemtyp ausgewählt haben. Sie können also dasselbe Installationspaket für Workstations und Server verwenden.

Das Installationspaket enthält die Antiviren-Datenbanken aus der Datenverwaltung des Administrationsservers. Sie können die Datenbanken im Installationspaket aktualisieren, um das Volumen des Datenverkehrs beim Datenbanken-Update nach der Installation von Kaspersky Endpoint Security zu reduzieren.



Im Installationspaket enthaltene Komponenten



Installationseinstellungen des Installationspakets

Einstellungen des Installationspakets

Abschnitt	Beschreibung
Schutzkomponenten	**Standardmodus**. Die Standardkonfiguration. Mit dieser Konfiguration können Sie alle Programmkomponenten verwenden, einschließlich Komponenten, die die Detection and Response-Lösungen unterstützen. Diese Konfiguration bietet einen umfassenden Schutz des Computers vor einer Vielzahl von Bedrohungen, Netzwerkangriffen und Betrugsversuchen. **Endpoint Detection and Response Agent**. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist. **Light Agent für den Schutz virtueller Umgebungen**. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.

Abschnitt	Beschreibung
Ausnahmen	Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Ab Kaspersky Endpoint Security 12.8 für Windows können Sie das Programm im Light Agent-Modus installieren, um virtuelle Umgebungen zu schützen. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren. Sie können die vertrauenswürdige Zone auch später in den Richtlinieneigenschaften konfigurieren: Untersuchungsausnahmen und vertrauenswürdige Programme.
Zu installierende Komponenten auswählen	In diesem Abschnitt können Sie die Programmkomponenten auswählen, die verfügbar sein sollen. Die Auswahl der Programmkomponenten können Sie später mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern* ändern. Sie können separate Komponentensätze für Workstations und Server erstellen. Vor der Bereitstellung des Installationspakets ermittelt das Installationsprogramm den Typ des Betriebssystems und installiert nur die Programmkomponenten, die Sie für diesen Betriebssystemtyp ausgewählt haben. Sie können also dasselbe Installationspaket für Workstations und Server verwenden. Die Auswahl der verfügbaren Komponenten hängt von der Konfiguration des Programms ab: **Standardmodus** Kaspersky Data Encryption, die Verschlüsselung auf Dateiebene und alle integrierten Agenten mit Ausnahme von EDR Optimum werden standardmäßig nicht installiert. Diese Komponenten können in den Einstellungen des Installationspakets hinzugefügt werden. **Endpoint Detection and Response Agent** In dieser Konfiguration sind nur integrierte Agents für die Lösungen von Kaspersky Detection and Response verfügbar. **Light Agent für den Schutz virtueller Umgebungen** In dieser Konfiguration können Sie fast alle Programmkomponenten verwenden, die in der Konfiguration **Standardmodus** verfügbar sind, mit Ausnahme von der Verschlüsselungskomponenten und der Adaptiven Kontrolle von Anomalien.
Lizenzschlüssel	In diesem Abschnitt können Sie das Programm aktivieren. Um das Programm zu aktivieren, müssen Sie einen Lizenzschlüssel auswählen. Vorher müssen Sie den Schlüssel zum Administrationsserver hinzufügen. Nähere Informationen über das Hinzufügen von Schlüsseln zum Kaspersky Security Center Administrationsserver finden Sie in der Hilfe zu Kaspersky Security Center.
Inkompatible Anwendungen	Überprüfen Sie die Liste der inkompatiblen Programme und erlauben Sie die Deinstallation dieser Programme. Wenn auf dem Computer inkompatible Programme installiert sind, wird die Installation von Kaspersky Endpoint Security mit einem Fehler beendet.
Installationseinstellungen	**Pfad der Datei "avp.com" zur Systemvariablen "%PATH%" hinzufügen**. Sie können den Installationspfad der Variablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen. **Installationsprozess schützen**. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein). **Kompatibilität mit Citrix PVS gewährleisten**. Sie können die Unterstützung von Citrix Provisioning Services aktivieren, um Kaspersky Endpoint Security auf einer virtuellen Maschine zu installieren. **Azure WVD-Kompatibilitätsmodus verwenden**. Diese Funktion sorgt dafür, dass der Status der virtuellen Azure-Maschine in der Kaspersky Anti Targeted Attack Platform-Konsole korrekt angezeigt wird. Zur Überwachung der Computerleistung sendet Kaspersky Endpoint Security Telemetriedaten an die KATA-Server. Die Telemetrie umfasst eine ID des Computers (Sensor ID). Mithilfe des Azure WVD-Kompatibilitätsmodus können Sie diesen virtuellen Computern eine permanente eindeutige Sensor ID zuweisen. Wenn der Kompatibilitätsmodus deaktiviert ist, ändert sich die Sensor ID aufgrund der Funktionsweise von virtuellen Azure-Maschinen möglicherweise nach dem Neustart des Computers. Dies kann dazu führen, dass in der Konsole Duplikate von virtuellen Maschinen angezeigt werden. **Installationsordner des Programms**. Sie können den Installationspfad von Kaspersky Endpoint Security auf dem Client-Computer ändern. Das Programm wird standardmäßig im Ordner `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2` installiert. **Konfigurationsdatei**. Installieren des Programms mit vordefinierten Einstellungen. Dazu müssen Sie eine Datei hochladen, welche die Einstellungen für Kaspersky Endpoint Security vorgibt. Sie können eine Konfigurationsdatei auf der lokalen Programmoberfläche erstellen. Der Assistent für das Erstellen eines neuen Pakets unterstützt keine verschlüsselten Konfigurationsdateien. Überspringen Sie beim Exportieren der Konfigurationsdatei den Schritt zur Dateiverschlüsselung.

Datenbanken-Update im Installationspaket

Das Installationspaket enthält die Antiviren-Datenbanken aus der Datenverwaltung des Administrationsservers. Diese Datenbanken waren aktuell, als das Installationspaket erstellt wurde. Nach der Erstellung des Installationspakets können Sie die Antiviren-Datenbanken im Installationspaket aktualisieren. Dadurch lässt sich das Volumen des Datenverkehrs reduzieren, der beim Update der Antiviren-Datenbanken nach der Installation von Kaspersky Endpoint Security anfällt.

Um die Antiviren-Datenbanken in der Administrationsserver-Datenverwaltung zu aktualisieren, verwenden Sie die Administrationsserver-Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Weitere Informationen über das Aktualisieren der Antiviren-Datenbanken in der Administrationsserver-Datenverwaltung finden Sie in der Hilfe zu Kaspersky Security Center.

Die Datenbanken in einem Installationspaket können nur über die Verwaltungskonsole und über „Kaspersky Security Center Web Console“ aktualisiert werden. Die Datenbanken in einem Installationspaket können nicht im Programm Kaspersky Security Center Cloud Console aktualisiert werden.

Über die Verwaltungskonsole (MMC) die Antiviren-Datenbanken im Installationspaket aktualisieren

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.
3. Öffnen Sie die Eigenschaften des Installationspakets.
4. Klicken Sie im Abschnitt **Allgemein** auf **Datenbanken aktualisieren**.

Dadurch werden die Antiviren-Datenbanken im Installationspaket aktualisiert. Als Quelle dient die Datenverwaltung des Administrationsservers. Die Datei `bases.cab`, die zum Lieferumfang gehört, wird durch den Order `bases` ersetzt. In diesem Ordner werden die Daten der Update-Pakete abgelegt.

Über „Web Console“ die Antiviren-Datenbanken im Installationspaket aktualisieren

1. Klicken Sie im Web Console-Hauptfenster auf **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**.

   Eine Liste der in „Web Console“ geladenen Installationspakete geöffnet.
2. Klicken Sie auf den Namen des Installationspakets für Kaspersky Endpoint Security, in dem Sie die Antiviren-Datenbanken aktualisieren möchten.

   Das Eigenschaftenfenster für das Installationspaket wird geöffnet.
3. Klicken Sie auf der Registerkarte **Allgemeine Informationen** auf den Link **Datenbanken aktualisieren**.

Dadurch werden die Antiviren-Datenbanken im Installationspaket aktualisiert. Als Quelle dient die Datenverwaltung des Administrationsservers. Die Datei `bases.cab`, die zum Lieferumfang gehört, wird durch den Order `bases` ersetzt. In diesem Ordner werden die Daten der Update-Pakete abgelegt.

Erstellung einer Aufgabe zur Remote-Installation

Die Aufgabe *Remote-Installation einer Anwendung* ist für die Remote-Installation von Kaspersky Endpoint Security vorgesehen. Mit der Aufgabe *Remote-Installation einer Anwendung* kann das Installationspaket des Programms auf allen Computern des Unternehmens bereitgestellt werden. Bevor das Installationspaket bereitgestellt wird, können Sie die Antiviren-Datenbanken in diesem Paket aktualisieren und in den Eigenschaften des Installationspakets die verfügbaren Programmkomponenten auswählen.

In der Verwaltungskonsole (MMC) einer Aufgabe zur Remote-Installation erstellen

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
3. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie die Option **Kaspersky Security Center Administrationsserver → Remote-Installation einer Anwendung** aus.

Schritt 2. Installationspaket auswählen

Wählen Sie in der Liste der Installationspakete das Paket für Kaspersky Endpoint Security aus. Wenn das Installationspaket für Kaspersky Endpoint Security nicht auf der Liste steht, können Sie das Paket mithilfe des Assistenten erstellen.

Sie können die Einstellungen des Installationspakets im Kaspersky Security Center konfigurieren. Sie können zum Beispiel die Programmkomponenten auswählen, die auf einem Computer installiert werden sollen.

Zusammen mit Kaspersky Endpoint Security wird auch der Administrationsagent installiert. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

Schritt 3. Erweitert

Wählen Sie ein Installationspaket für den Administrationsagenten aus. Die ausgewählte Version des Administrationsagenten wird zusammen mit Kaspersky Endpoint Security installiert.

Schritt 4. Einstellungen

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Installationspakets erzwingen**. Wählen Sie die Mittel für die Programminstallation aus:

  - **Unter Nutzung des Administrationsagenten**. Der Administrationsagent ist dafür verantwortlich, das Installationspaket für Kaspersky Endpoint Security auf den Client-Computern bereitzustellen. Wenn der Administrationsagent nicht installiert ist, wird die Aufgabe mit einem Fehler beendet. Fügen Sie in diesem Fall das Installationspaket des Administrationsagenten zur Aufgabe *Remote-Installation einer Anwendung* hinzu und aktivieren Sie die Dateiübermittlung über die Betriebssystemressourcen. Dann wird der Administrationsagent mithilfe der Betriebssystemressourcen installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.

  - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Weitere Informationen über die Verwendung von Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center.

  - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.

- **Verhalten bei Geräten, die durch andere Administrationsserver verwaltet werden**. Wählen Sie eine Installationsmethode für Kaspersky Endpoint Security aus. Wenn in einem Netzwerk mehr als ein Administrationsserver installiert ist, können diese Server ein und denselben Client-Computer sehen. Dies kann beispielsweise dazu führen, dass ein bestimmtes Programm von mehreren Administrationsservern im Remote-Modus auf demselben Client-Computer installiert wird, oder dass andere Konflikte auftreten.

- **Anwendung nicht neu installieren, wenn sie bereits installiert ist**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beispielsweise eine ältere Version des Programms installieren möchten.

Schritt 5. Einstellungen für den Neustart des Betriebssystems auswählen

Wählen Sie aus, welche Aktion ausgeführt wird, wenn ein Neustart des Computers erforderlich ist. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.

Schritt 6. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. Auf nicht zugeordneten Geräten ist der Administrationsagent nicht installiert. In diesem Fall wird die Aufgabe einer Auswahl von Geräten zugewiesen. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 7: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 8. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 9. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein (z. B. *Kaspersky Endpoint Security für Windows 14.2 installieren*).

Schritt 10. Aufgabenerstellung abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Die Programminstallation wird im unbeaufsichtigten Modus ausgeführt. Nach der Installation wird im Infobereich der Taskleiste des Benutzercomputers das Symbol hinzugefügt. Wenn das Symbol nichts so aussieht, vergewissern Sie sich, dass Sie das Programm aktiviert haben.

Erstellen einer Aufgabe zur Remote-Installation in „Web Console“ und „Cloud Console”

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt **Kaspersky Security Center** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Remote-Installation einer Anwendung**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Installation von Kaspersky Endpoint Security für die Geschäftsführung*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

Schritt 2. Computer für die Installation auswählen

Wählen Sie bei diesem Schritt die Computer aus, auf denen das Programm Kaspersky Endpoint Security installiert werden soll. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe.

Schritt 3. Einstellungen des Installationspaket anpassen

Passen Sie bei diesem Schritt das Installationspaket an:

1. Wählen Sie das Installationspaket für Kaspersky Endpoint Security für Windows (14.2) aus.
2. Wählen Sie ein Installationspaket für den Administrationsagenten aus.

   Die ausgewählte Version des Administrationsagenten wird zusammen mit Kaspersky Endpoint Security installiert. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und dem Client-Computer. Wenn der Administrationsagent bereits auf dem Computer installiert ist, wird die Installation nicht wiederholt.

3. Wählen Sie im Block **Download des Installationspakets erzwingen** die Installationsmethode für das Programm aus:

   - **Unter Nutzung des Administrationsagenten**. Der Administrationsagent ist dafür verantwortlich, das Installationspaket für Kaspersky Endpoint Security auf den Client-Computern bereitzustellen. Wenn der Administrationsagent nicht installiert ist, wird die Aufgabe mit einem Fehler beendet. Fügen Sie in diesem Fall das Installationspaket des Administrationsagenten zur Aufgabe *Remote-Installation einer Anwendung* hinzu und aktivieren Sie die Dateiübermittlung über die Betriebssystemressourcen. Dann wird der Administrationsagent mithilfe der Betriebssystemressourcen installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten installiert.

   - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Das Installationspaket wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Weitere Informationen über die Verwendung von Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center.

   - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Die Dateien werden durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.

4. Legen Sie im Feld **Maximale Anzahl gleichzeitiger Downloads** fest, wie viele Anfragen für den Download eines Installationspakets maximal an den Administrationsserver gestellt werden dürfen. Durch die Beschränkung der Anfragen lässt sich eine Überlastung des Netzwerks vermeiden.

5. Legen Sie im Feld **Maximale Anzahl der Installationsversuche** fest, wie oft versucht werden darf, das Programm zu installieren. Wenn die Installation von Kaspersky Endpoint Security mit einem Fehler beendet wird, startet die Aufgabe die Installation automatisch erneut.

6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Anwendung nicht neu installieren, wenn sie bereits installiert ist**. Dies erlaubt es beispielsweise, eine ältere Version des Programms zu installieren.

7. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Typ des Betriebssystems vor dem Download überprüfen**. Dadurch lässt sich verhindern, dass das Programmpaket heruntergeladen wird, wenn das Betriebssystem des Computers die Softwarevoraussetzungen nicht erfüllt. Wenn Sie sicher sind, dass das Betriebssystem des Computers die Softwarevoraussetzungen erfüllt, kann diese Überprüfung übersprungen werden.

8. Aktivieren Sie bei Bedarf das Kontrollkästchen **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**. Die Installation von Kaspersky Endpoint Security wird manuell mit den Mitteln des Administrationsagenten oder mit den Mitteln von Active Directory ausgeführt. Für die Installation des Administrationsagenten muss die Aufgabe zur Remote-Installation mit den Rechten des Domänenadministrators ausgeführt werden.

9. Aktivieren Sie bei Bedarf das Kontrollkästchen **Benutzer auffordern, laufende Anwendungen zu schließen**. Bei der Installation von Kaspersky Endpoint Security werden die Ressourcen des Computers beansprucht. Vor dem Beginn der Programminstallation schlägt der Installationsassistent dem Benutzer vor, die laufenden Programme zu schließen. Dadurch lassen sich eine Verlangsamung anderer Programme und mögliche Störungen des Computers verhindern.

10. Wählen Sie im Block **Verhalten bei Geräten, die durch andere Administrationsserver verwaltet werden** eine Methode für die Installation von Kaspersky Endpoint Security aus. Wenn in einem Netzwerk mehr als ein Administrationsserver installiert ist, können diese Server ein und denselben Client-Computer sehen. Dies kann beispielsweise dazu führen, dass ein bestimmtes Programm von mehreren Administrationsservern im Remote-Modus auf demselben Client-Computer installiert wird, oder dass andere Konflikte auftreten.

Schritt 4: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Für die Installation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten ist es nicht erforderlich, ein Benutzerkonto auszuwählen.

Schritt 5. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertigstellen**. Die neue Aufgabe wird in der Aufgabenliste angezeigt. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**, um die Aufgabe auszuführen. Die Programminstallation wird im unbeaufsichtigten Modus ausgeführt. Nach der Installation wird im Infobereich der Taskleiste des Benutzercomputers das Symbol hinzugefügt. Wenn das Symbol nichts so aussieht, vergewissern Sie sich, dass Sie das Programm aktiviert haben.

Lokale Programminstallation mithilfe des Assistenten

Die Benutzeroberfläche des Installationsassistenten für das Programm besteht aus einer Abfolge von Fenstern, die den einzelnen Installationsschritten entsprechen. Stellen Sie sicher, dass das Benutzerkonto, unter dem Sie den Setup-Assistenten ausführen, zur Administratorengruppe gehört.

Um mithilfe des Installationsassistenten das Programm zu installieren oder eine ältere Version des Programms zu aktualisieren,

1. Kopieren Sie den Ordner Lieferumfang auf den Benutzercomputer.
2. Führen Sie setup_kes.exe aus.

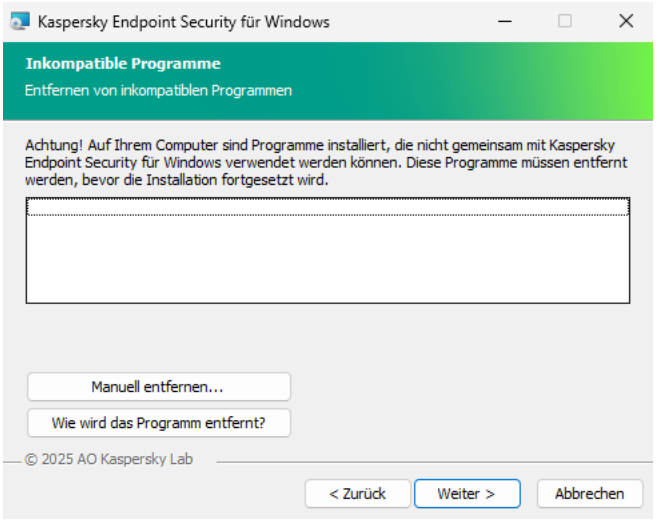
   Der Setup-Assistent wird gestartet.

Vorbereitung der Installation

Bevor Kaspersky Endpoint Security auf einem Computer installiert oder eine Vorgängerversion des Programms aktualisiert wird, werden folgende Voraussetzungen überprüft:

- Ob Software installiert ist, die zu Kompatibilitätsproblemen mit Kaspersky Endpoint Security führen kann (eine Liste der Software finden Sie in der Datei incompatible.txt, die im Lieferumfang enthalten ist).
- Ob die Hard- und Softwarevoraussetzungen erfüllt sind.
- Ob Microsoft .NET Framework vorhanden ist.
- Vorhandensein von Rechten für die Programminstallation

Wenn eine der aufgezählten Voraussetzungen nicht erfüllt ist, erscheint eine entsprechende Meldung auf dem Bildschirm. Beispielsweise eine Benachrichtigung über inkompatible Software (siehe Abbildung unten).



Inkompatible Software löschen

Erfüllt der Computer die erforderlichen Voraussetzungen, so führt der Installationsassistent eine Suche nach Kaspersky-Programmen durch, deren gleichzeitige Verwendung zu Konflikten führen kann. Werden solche Programme gefunden, so werden Sie aufgefordert, diese manuell zu entfernen.

Wenn sich unter den gefundenen Programmen ältere Versionen von Kaspersky Endpoint Security befinden, werden alle Daten, die migriert werden können (z. B. Aktivierungsdaten und Programmversion), gespeichert und bei der Installation von Kaspersky Endpoint Security 14.2 für Windows verwendet. Die vorherige Version des Programms wird automatisch entfernt. Dies bezieht sich auf folgende Programmversionen:

- Kaspersky Endpoint Security 12.3 für Windows (Version 12.3.0.493)
- Kaspersky Endpoint Security 12.4 für Windows (Version 12.4.0.467)
- Kaspersky Endpoint Security 12.5 für Windows (Version 12.5.0.539)
- Kaspersky Endpoint Security 12.6 für Windows (Version 12.6.0.438)
- Kaspersky Endpoint Security 12.7 für Windows (Version 12.7.0.533)
- Kaspersky Endpoint Security 12.8 für Windows (Version 12.8.0.505)
- Kaspersky Endpoint Security 12.9 für Windows (Version 12.9.0.384)
- Kaspersky Endpoint Security 12.10 für Windows (Version 12.10.0.466)
- Kaspersky Endpoint Security 12.11 für Windows (Version 12.11.0.637)
- Kaspersky Endpoint Security 12.12 für Windows (Version 12.12.0.522)
- Kaspersky Endpoint Security 14.0 für Windows (Version 14.0.0.504)
- Kaspersky Endpoint Security 14.1 für Windows (Version 14.1.0.423)

Konfiguration von Kaspersky Endpoint Security



Programmkonfiguration auswählen

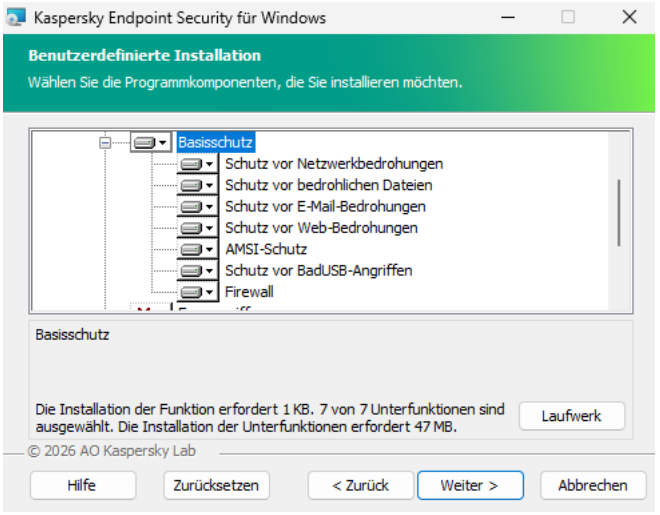
Standardmodus. Die Standardkonfiguration. Mit dieser Konfiguration können Sie alle Programmkomponenten verwenden, einschließlich Komponenten, die die Detection and Response-Lösungen unterstützen. Diese Konfiguration bietet einen umfassenden Schutz des Computers vor einer Vielzahl von Bedrohungen, Netzwerkangriffen und Betrugsversuchen.

Endpoint Detection and Response Agent. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.

Light Agent für den Schutz virtueller Umgebungen. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.

Komponenten von Kaspersky Endpoint Security

Bei der Installation können Sie auswählen, welche Komponenten von Kaspersky Endpoint Security installiert werden sollen (siehe Bild unten). Die Komponente „Schutz vor bedrohlichen Dateien“ ist für die Installation obligatorisch. Sie können die Installation dieser Komponente nicht abwählen.



Auswahl der zu installierenden Anwendungskomponenten

Standardmäßig sind alle Programmkomponenten für die Installation gewählt. Eine Ausnahme bilden folgende Komponenten:

- Kaspersky-Festplattenverschlüsselung
- Verschlüsselung von Dateien
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- Integration mit KUMA

Nach der Programminstallation können Sie die Auswahl der Komponenten ändern. Dazu müssen Sie den Installationsassistenten erneut starten und den Vorgang zur Änderung der Komponentenauswahl auswählen.

Wenn Sie Komponenten von „Detection and Response“ installieren müssen, unterstützt Kaspersky Endpoint Security die folgenden Konfigurationen:

- Nur Endpoint Detection and Response Optimum
- Nur Endpoint Detection and Response Expert (cloud)
- Nur Endpoint Detection and Response Expert (on-premises)

- Nur Network Detection and Response (KATA)
- Nur Sandbox
- Endpoint Detection and Response Optimum und Sandbox
- Endpoint Detection and Response Expert (cloud) und Sandbox
- Endpoint Detection and Response Expert (on-premises) und Sandbox
- Network Detection and Response (KATA) und Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) und Managed Detection and Response

Kaspersky Endpoint Security überprüft die ausgewählten Komponenten, bevor das Programm installiert wird. Wenn die ausgewählte Konfiguration der „Detection and Response"-Komponenten nicht unterstützt wird, kann Kaspersky Endpoint Security nicht installiert werden.

Ordner für die Programminstallation auswählen

Sie können den Installationspfad von Kaspersky Endpoint Security auf dem Client-Computer ändern. Das Programm wird standardmäßig im Ordner `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2` installiert.

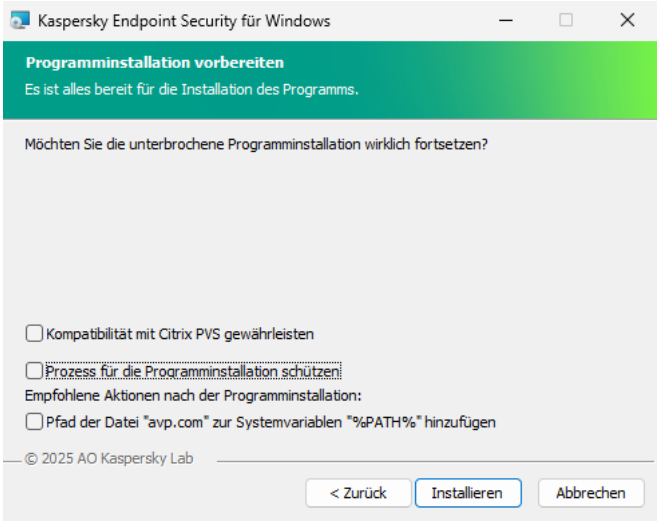
Vertrauenswürdige Zone konfigurieren

Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen.

Ab Kaspersky Endpoint Security 12.8 für Windows können Sie das Programm im Light Agent-Modus installieren, um virtuelle Umgebungen zu schützen. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren.

Sie können die vertrauenswürdige Zone auch später in den Richtlinieneigenschaften konfigurieren: Untersuchungsausnahmen und vertrauenswürdige Programme.

Erweiterte Einstellungen



Erweiterte Installationseinstellungen für das Programm

Prozess für die Programminstallation schützen. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).

Kompatibilität mit Citrix PVS gewährleisten. Sie können die Unterstützung von Citrix Provisioning Services aktivieren, um Kaspersky Endpoint Security auf einer virtuellen Maschine zu installieren.

Pfad der Datei "avp.com" zur Systemvariablen "%PATH%" hinzufügen. Sie können den Installationspfad der Variablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen.

Remote-Installation des Programms mithilfe von System Center Configuration Manager

Die Anleitung ist gültig für die Version System Center Configuration Manager 2012 R2.

Um das Programm ferngesteuert mithilfe von System Center Configuration Manager zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole von Configuration Manager.
2. Wählen Sie im rechten Konsolenbereich im Block **Anwendungsverwaltung** den Abschnitt **Pakete** aus.
3. Klicken Sie im oberen Konsolenbereich in der Symbolleiste auf **Paket wird erstellt**.

   Der *Assistent zum Erstellen von Paketen und Programmen* wird gestartet.

4. Gehen Sie im Assistenten zum Erstellen von Paketen und Programmen wie folgt vor:

   a. Gehen Sie im Abschnitt **Paket** wie folgt vor:

      - Geben Sie im Feld **Name** den Namen des Installationspakets ein.
      - Geben Sie im Feld **Quellordner** den Pfad des Ordners an, in dem sich das Verteilungspaket für Kaspersky Endpoint Security befindet.

   b. Wählen Sie im Abschnitt **Programmtyp** die Variante **Standardprogramm**.

   c. Gehen Sie im Abschnitt **Standardprogramm** wie folgt vor:

      - Geben Sie im Feld **Name** den individuellen Namen des Installationspakets ein (z. B. den Programmnamen mit Versionsangabe).
      - Geben Sie im Feld **Befehlszeile** die Befehlszeilenparameter für die Installation von Kaspersky Endpoint Security an.
      - Geben Sie mithilfe der Schaltfläche **Durchsuchen** den Pfad der ausführbaren Programmdatei an.
      - Vergewissern Sie sich, dass in der Dropdown-Liste **Startmodus** das Element **Mit Administratorrechten starten** ausgewählt ist.

   d. Gehen Sie im Abschnitt **Anforderungen** wie folgt vor:

      - Aktivieren Sie das Kontrollkästchen **Anderes Programm zuerst starten**, damit vor der Installation von Kaspersky Endpoint Security ein anderes Programm gestartet wird.

        Wählen Sie das Programm aus der Dropdown-Liste **Programm** oder geben Sie den Pfad der ausführbaren Datei dieses Programms mithilfe der Schaltfläche **Durchsuchen** an.

      - Wählen Sie im Block **Anforderungen an die Plattform** die Variante **Dieses Programm kann nur auf bestimmten Plattformen ausgeführt werden**, damit das Programm nur auf den angegebenen Betriebssystemen installiert wird.

        Aktivieren Sie in der unten angebrachten Liste die Kontrollkästchen für jene Betriebssysteme, in denen Kaspersky Endpoint Security installiert werden soll.

      Dieser Schritt ist optional.

   e. Überprüfen Sie im Abschnitt **Übersicht** alle angegebenen Werte und klicken Sie auf **Weiter**.

   Das erstellte Installationspaket erscheint im Abschnitt **Pakete** in der Liste für verfügbare Installationspakete.

5. Wählen Sie im Kontextmenü des Installationspakets den Punkt **Verteilen**.

   Der *Assistent zur Software-Verteilung* wird gestartet.

6. Gehen Sie im Assistenten zur Software-Verteilung wie folgt vor:

   a. Gehen Sie im Abschnitt **Allgemein** wie folgt vor:

      - Geben Sie im Feld **Software** den individuellen Namen des Installationspakets an oder wählen Sie mit der Schaltfläche **Durchsuchen** ein Installationspaket aus der Liste.
      - Geben Sie im Feld **Sammlung** den Namen der Gruppe für Computer an, auf denen das Programm installiert werden soll, oder wählen Sie diese Sammlung mithilfe der Schaltfläche **Durchsuchen**.

b. Fügen Sie im Abschnitt **Enthält** die Verteilungspunkte (Weitere Informationen finden Sie in der Dokumentation zu System Center Configuration Manager).

c. Legen Sie erforderlichenfalls im Assistenten zur Software-Verteilung die Werte für weitere Einstellungen fest. Diese Einstellungen sind für die Remote-Installation von Kaspersky Endpoint Security optional.

d. Überprüfen Sie im Abschnitt **Übersicht** alle angegebenen Werte und klicken Sie auf **Weiter**.

Nach Abschluss des Assistenten zur Software-Verteilung wird eine Aufgabe zur Remote-Installation von Kaspersky Endpoint Security erstellt.

Beschreibung der Installationseinstellungen in der Datei setup.ini

Die Datei setup.ini wird verwendet, wenn das Programm aus der Befehlszeile oder mithilfe des Gruppenrichtlinienverwaltungs-Editors für Microsoft Windows installiert wird. Um Einstellungen aus der Datei setup.ini zu übernehmen, legen Sie diese Datei im Ordner mit dem Programmpaket für Kaspersky Endpoint Security ab.

Verwenden Sie die Datei setup.ini nur dann, wenn das Programm im unbeaufsichtigten Modus installiert wird.

In der Datei setup.ini können Sie keinen Pfad für die Konfigurationsdatei install.cfg hinzufügen. Das Programm überspringt die Konfigurationsdatei install.cfg auch, wenn sie im selben Ordner wie das Kaspersky Endpoint Security Verteilungspunkt abgelegt wird. Um Einstellungen aus der Konfigurationsdatei install.cfg zu übernehmen, müssen Sie den Dateipfad im folgenden Befehl zur Programminstallation angeben: `CONFIGPATH=<path to the configuration file>`.

DATEI SETUP.INI HERUNTERLADEN

Die Datei setup.ini besteht aus folgenden Abschnitten:

- `[Setup]` – allgemeine Installationseinstellungen für die App.
- `[Components]` – Auswahl der im Standard-Modus zu installierenden App-Komponenten. Wird keine Komponente angegeben, werden alle für dieses Betriebssystem verfügbaren Komponenten installiert. Der Schutz vor bedrohlichen Dateien ist eine obligatorische Komponente und wird unabhängig davon auf dem Computer installiert, welche Einstellungen in diesem Block angegeben sind.
- `[Tasks]` - Auswahl von Aufgaben, welche in die Aufgabenliste von Kaspersky Endpoint Security aufgenommen werden. Wird keine Aufgabe angegeben, werden alle Aufgaben in die Aufgabenliste von Kaspersky Endpoint Security eingetragen.

Anstelle des Werts `1` können die Werte `yes`, `on`, `enable`, `enabled` oder `true` verwendet werden. Anstelle des Werts `0` können die Werte `no`, `off`, `disable`, `disabled` oder `false` verwendet werden.

Abschnitt	Einstellung	Beschreibung
[Setup]	InstallDir	Pfad des Installationsordners für das Programm.
	ActivationCode	Aktivierungscode für Kaspersky Endpoint Security.
	Eula	Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags. Der Text des Lizenzvertrags ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen des Lizenzvertrags müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
	PrivacyPolicy	Zustimmung zu der Datenschutzrichtlinie. Der Text der Datenschutzrichtlinie gehört zum Lieferumfang von Kaspersky Endpoint Security. Die Datenschutzrichtlinie muss akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
	KSN	Akzeptieren oder Ablehnen der Teilnahme an Kaspersky Security Network (KSN). Ist der Parameter nicht angegeben, so fordert Kaspersky Endpoint Security beim ersten Start des Programms eine Bestätigung der Teilnahme an KSN. Mögliche Werte: • 1 – Zustimmung zur Teilnahme an KSN. • 0 – Ablehnung der Teilnahme an KSN (Standardwert). Das Programmpaket für Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.
	CLEANERSIGNCHECK	Überprüft die digitalen Signaturen der gefundenen Softwaredateien aus der Liste „incompatible.txt“. Zum Entfernen von Software verwendet Kaspersky Endpoint Security die Installationsdatei der Software. Wenn die Installationsdatei keine digitale Signatur hat, betrachtet Kaspersky Endpoint Security die Datei als nicht vertrauenswürdig und beendet das Entfernen inkompatibler Software. Dadurch wird die Ausführung von potenziell schädlichem Code vermieden. Wenn die digitale Signatur der erkannten Software-Datei nicht überprüft werden kann, beendet Kaspersky Endpoint Security die Installation mit einem Fehler. Der Standardwert variiert je nach Methode der Software-Installation: • 0 bedeutet: Die Überprüfung von digitalen Signaturen ist deaktiviert (Standardwert bei Bereitstellung über Kaspersky Security Center). • 1 bedeutet: Die Überprüfung von digitalen Signaturen ist aktiviert (Standardwert bei der lokalen Installation der App).
	Login	Festlegen des Benutzernamens für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Komponente Kennwortschutz). Der Benutzername wird zusammen mit den Parametern Password und PasswordArea festgelegt. Als Standard wird der Benutzername KLAdmin verwendet.
	Password	Festlegen des Kennworts für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Das Kennwort wird zusammen mit den Parametern Login und PasswordArea festgelegt). Falls Sie ein Kennwort angegeben haben, aber mithilfe des Parameters Login keinen Benutzernamen festgelegt haben, wird standardmäßig der Benutzername KLAdmin verwendet.

Abschnitt	Einstellung	Beschreibung
	`PasswordArea`	Gibt den Gültigkeitsbereich des Kennworts für den Zugriff auf Kaspersky Endpoint Security an. Wenn der Benutzer versucht, eine Aktion aus diesem Bereich auszuführen, fragt Kaspersky Endpoint Security die Anmeldedaten des Benutzers ab (Parameter für `Login` und `Password`). Verwenden Sie das Zeichen „`;`“, um mehrere Werte anzugeben. Mögliche Werte: • `SET` – Änderung der Programmeinstellungen. • `EXIT` – Beenden des Programms. • `DISPROTECT` – Schutzkomponenten deaktivieren und Untersuchungsaufgaben abbrechen. • `DISPOLICY` – Richtlinie für Kaspersky Security Center deaktivieren. • `UNINST` – Programm vom Computer entfernen. • `DISCTRL` – Kontrollkomponenten deaktivieren. • `REMOVELIC` – Schlüssel entfernen. • `REPORTS` – Berichte anzeigen. • `EXPORT` – Programmeinstellungen exportieren. Beispiel: `PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`.
	`SelfProtection`	Schutzmechanismus für die Programminstallation aktivieren oder deaktivieren. Mögliche Werte: • `1` – Das Modul für den Schutz der Programminstallation ist aktiviert (Standardwert). • `0` – Das Modul für den Schutz der Programminstallation ist deaktiviert. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).
	`PROTECTOSSERVICES`	Funktionalität zum Schutz von Betriebssystemdiensten. Der Schutz für Betriebssystemdienste verhindert, dass Drittanbieter-Programme den Betrieb von Betriebssystemdiensten stören. Zu diesen Diensten gehört beispielsweise der Autostart-Dienst für Programme. • `1` bedeutet, dass der Schutz für Betriebssystemdienste aktiviert ist (Standardwert). • `0` bedeutet, dass der Schutz für Betriebssystemdienste deaktiviert ist.
	`EnableAzureSupport`	Azure WVD-Kompatibilitätsmodus aktivieren oder deaktivieren. Mögliche Werte: • `1` – Azure WVD-Kompatibilitätsmodus ist aktiviert. • `0` – Azure WVD-Kompatibilitätsmodus ist deaktiviert (Standardwert). Diese Funktion sorgt dafür, dass der Status der virtuellen Azure-Maschine in der Kaspersky Anti Targeted Attack Platform-Konsole korrekt angezeigt wird. Zur Überwachung der Computerleistung sendet Kaspersky Endpoint Security Telemetriedaten an die KATA-Server. Die Telemetrie umfasst eine ID des Computers (Sensor ID). Mithilfe des Azure WVD-Kompatibilitätsmodus können Sie diesen virtuellen Computern eine permanente eindeutige Sensor ID zuweisen. Wenn der Kompatibilitätsmodus deaktiviert ist, ändert sich die Sensor ID aufgrund der Funktionsweise von virtuellen Azure-Maschinen möglicherweise nach dem Neustart des Computers. Dies kann dazu führen, dass in der Konsole Duplikate von virtuellen Maschinen angezeigt werden.
	`Reboot`	Automatischer Neustart des Computers nach der Installation oder Aktualisierung des Programms, falls erforderlich. Wenn dieser Parameter nicht angegeben ist, ist der automatische Neustart des Computers verboten. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.
	`AddEnvironment`	Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, zur Systemvariablen %PATH% hinzufügen. Mögliche Werte: • `1` – Der Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, wird zur Systemvariablen %PATH% hinzugefügt. • `0` – Der Pfad der ausführbaren Dateien, die sich im Installationsordner von Kaspersky Endpoint Security befinden, wird nicht zur Systemvariablen %PATH% hinzugefügt.

Abschnitt	Einstellung	Beschreibung
	AMPPL	Aktivierung oder Deaktivierung des Schutzes für Prozesse von Kaspersky Endpoint Security unter Verwendung der Technologie AM-PPL (Antimalware Protected Process Light). Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019. Mögliche Werte: • 1 – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist aktiviert (Standardwert). • 0 – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist deaktiviert.
	UPGRADEMODE	Modus für das Programm-Upgrade: • Seamless bedeutet, beim Programm-Upgrade wird ein Computerneustart durchgeführt (Standardwert). • Force bedeutet, das Programm-Upgrade wird ohne Neustart durchgeführt. 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. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Der Upgrade-Modus für die App wird in den App-Einstellungen angegeben. Sie können diese Einstellung in den App-Einstellungen oder in der Richtlinie ändern. Wenn die App bereits installiert ist und ein Upgrade durchgeführt wird, hat der in der Datei setup.ini angegebene Parameter eine höhere Priorität als der Parameter, der in den App-Einstellungen oder im Befehlszeilenparameter angegeben ist. Wenn beispielsweise der Upgrade-Modus Force in der Datei setup.ini angegeben ist und der Modus Seamless in den Programmeinstellungen, so wird das Upgrade ohne Neustart installiert (Force). Wenn Sie die Datei setup.ini verwenden und den Parameter UPGRADEMODE nicht angeben, verwendet das Installationsprogramm einen Standardwert (Seamless) und installiert das Upgrade mit einem Computerneustart.
	SetupReg	Aktivierung der Aufnahme von Registrierungsschlüsseln aus der Datei setup.reg in die Registrierung. Parameterwert SetupReg: setup.reg.
	EnableTraces	Anwendungsnachverfolgung aktivieren oder deaktivieren. Nach dem Start von Kaspersky Endpoint Security werden Protokolldateien im Ordner %ProgramData%\Kaspersky Lab\KES.14.2\Traces gespeichert. Mögliche Werte: • 1 – Die Nachverfolgung ist aktiviert. • 0 – Die Nachverfolgung ist deaktiviert (Standardwert).
	TracesLevel	Genauigkeitsstufe der Ablaufverfolgung. Mögliche Werte: • 100 (kritisch). Nur Meldungen über fatale Fehler. • 200 (hoch). Meldungen über alle Fehler, einschließlich fatale. • 300 (Diagnose). Meldungen über alle Fehler, sowie Warnungen. • 400 (wichtig). Meldungen über alle Fehler, Warnungen, sowie zusätzliche Informationen. • 500 (normal). Meldungen über alle Fehler, Warnungen, sowie ausführliche Informationen über die Nutzung des Programms im normalen Modus (Standardwert). • 600 (niedrig). Alle Meldungen.
	RESTAPI	Programmverwaltung über eine REST API. Für die Programmverwaltung über eine REST API muss ein Benutzername angegeben werden (Parameter RESTAPI_User). Mögliche Werte: • 1 – Die Verwaltung über eine REST API ist erlaubt. • 0 – Die Verwaltung über eine REST API ist verboten (Standardwert). Für die Programmverwaltung über eine REST API muss die Verwaltung mithilfe von Administrationssystemen erlaubt sein. Legen Sie dazu den Parameter AdminKitConnector=1 fest. Wenn Sie das Programm über eine REST API verwalten, kann das Programm nicht mithilfe der Kaspersky-Administrationssysteme verwaltet werden.
	RESTAPI_User	Benutzername des Windows-Domänen-Benutzerkontos für die Programmverwaltung über eine REST API. Die Programmverwaltung über eine REST API ist nur für diesen Benutzer verfügbar. Geben Sie den Benutzernamen im Format <DOMAIN>\<UserName> an (z. B. RESTAPI_User=COMPANY\Administrator). Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen. Eine Voraussetzung für die Programmverwaltung über eine REST API ist, dass ein Benutzername hinzugefügt wird.
	RESTAPI_Port	Port für die Programmverwaltung über eine REST API. Als Standard wird Port 6782 verwendet. Stellen Sie sicher, dass der Port frei ist.

Abschnitt	Einstellung	Beschreibung
	`RESTAPI_Certificate`	Zertifikat zur Identifizierung von Anfragen (z. B. `RESTAPI_Certificate=C:\cert.pem`). Für die sichere Interaktion von Kaspersky Endpoint Security mit dem REST-Client muss die Anfrage-Identifikation konfiguriert werden. Dazu müssen Sie ein Zertifikat installieren und anschließend die Nutzdaten jeder Anfrage signieren.
	`StandaloneMode`	Installation der Anwendung im Modus „Endpoint Detection and Response Agent“ (EDR Agent). Das Programm *Endpoint Detection and Response Agent* wird in der IT-Infrastruktur des Unternehmens auf einzelnen Workstations und Servern installiert und unterstützt die Lösungen Kaspersky Managed Detection and Response und Kaspersky Anti Targeted Attack Platform. EDR Agent ist mit Drittanbieter-EPP-Anwendungen kompatibel. Dadurch können Sie neben Detection and Response-Lösungen von Kaspersky auch Infrastruktur-Sicherheitstools von Drittanbietern nutzen. Um EDR Agent zu installieren, wählen Sie im Abschnitt `[Components]` die Komponenten `StandaloneKATA`, `StandaloneNDR` oder `StandaloneMDR` aus. EDR Agent unterstützt keine anderen Anwendungskomponenten. Mögliche Werte: • `1` – Installiert die Anwendung im Modus „EDR-Agent“. • `0` – Installiert die Anwendung im Standardmodus (Standardwert).
	`KSVLAMode`	Installation des Programms im Light Agent-Modus. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. Mögliche Werte: • `1` – Installiert die Anwendung im Modus „Light Agent“. • `0` – Installiert die Anwendung im Standardmodus (Standardwert).
	`InstallOnVDI`	Modus zum Schutz der VDI-Infrastruktur aktivieren, wenn das Programm im Light Agent-Modus installiert wird (`KSVLAMode=1`). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss. Mögliche Werte: • `1` – Modus zum Schutz der VDI-Infrastruktur aktivieren. • `0` – Modus zum Schutz der VDI-Infrastruktur deaktivieren (Standard).
	`KESExclusions`	Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme hinzufügen, wenn das Programm auf dem Server wird installiert. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Zu den vordefinierten Untersuchungsausnahmen für SQL-Server gehören beispielsweise MDF- und LDF-Datenbankdateien. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Mögliche Werte: • `1` – aktiviert vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme. • `0` – deaktiviert vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme.
	`LAExclusions`	Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme hinzufügen, wenn das Programm auf einer virtuellen Maschine (Light Agent-Modus) wird installiert. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren. Mögliche Werte: • `1` – aktiviert vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme. • `0` – deaktiviert vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme.

Abschnitt	Einstellung	Beschreibung
	`EnableUniqueSensorID`	Eindeutige Computer-ID (Sensor ID) erstellen, während das Programm installiert oder aktualisiert wird. Sensor ID wird in der Lösung Kaspersky Anti Targeted Attack Platform verwendet, um Computer zu identifizieren, die Telemetriedaten an den Server senden. Beim Erstellen einer Sensor ID berücksichtigt ein Algorithmus die Konfiguration des Computers, beispielsweise die Motherboard-Seriennummer. In einigen Fällen, beispielsweise bei der Verwendung des Programms in einer virtuellen Umgebung, kann die Sensor ID doppelt vorhanden sein. Dies hat zur Folge, dass Kaspersky Anti Targeted Attack Platform den Computer, von dem Telemetriedaten gesendet werden, nicht identifizieren kann. Um eine eindeutige Sensor ID zu erstellen, müssen Sie den Parameter `EnableUniqueSensorID=1` angeben. In diesem Fall verwendet das Programm beim Erstellen der Sensor ID einen anderen Algorithmus, der andere Daten über den Computer berücksichtigt. Dadurch wird eine eindeutige Sensor ID erzeugt. Dieser Parameter ist standardmäßig nicht festgelegt. Das Programm erbt die Sensor ID in den folgenden Fällen: • Aktualisierung der Programmversion • Migration der Konfiguration [KES+KEA] zur Konfiguration [KES+built-in agent]. Im Rahmen einer Programmreparatur versucht das Installationsprogramm, die Sensor ID zu vererben. Wenn die Sensor ID nicht wiederhergestellt werden kann, erstellt das Programm eine neue Sensor ID.
	`CitrixCompatibility`	Aktivieren der Unterstützung von Citrix Provisioning Services, um Kaspersky Endpoint Security auf einer virtuellen Maschine zu installieren.
`[Components]`	`ALL`	Installation aller Komponenten. Wenn der Parameterwert `1` angegeben ist, werden alle Komponenten installiert. In diesem Fall bleiben die Parameter, die für die Installation der einzelnen Komponenten angegeben sind, unberücksichtigt. Da die Detection and Response-Lösungen auf spezielle Weise unterstützt werden, werden die Komponenten Endpoint Detection and Response Optimum und Sandbox auf dem Computer installiert. Die Komponente Endpoint Detection and Response Expert (cloud) ist nicht mit dieser Konfiguration kompatibel.
	`MailThreatProtection`	Schutz vor E-Mail-Bedrohungen.
	`WebThreatProtection`	Schutz vor Web-Bedrohungen.
	`AMSI`	AMSI-Schutz.
	`HostIntrusionPrevention`	Programm-Überwachung.
	`BehaviorDetection`	Verhaltensanalyse.
	`ExploitPrevention`	Exploit-Prävention.
	`RemediationEngine`	Rollback von schädlichen Aktionen.
	`Firewall`	Firewall.
	`NetworkThreatProtection`	Schutz vor Netzwerkbedrohungen.
	`WebControl`	Web-Kontrolle
	`DeviceControl`	Gerätekontrolle.
	`ApplicationControl`	Programmkontrolle.
	`AdaptiveAnomaliesControl`	Adaptive Kontrolle von Anomalien.
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	Protokollanalyse
	`AntiCryptor`	Schutz vor Verschlüsselung
	`FileThreatProtection`	Schutz vor bedrohlichen Dateien.
	`SystemIntegrityMonitor`	Überwachung der Systemintegrität.
	`FileEncryption`	Bibliotheken für die Verschlüsselung von Dateien.
	`DiskEncryption`	Bibliotheken für die vollständige Festplattenverschlüsselung.
	`MSBitLocker`	Verwaltungsbibliotheken für die BitLocker-Verschlüsselung.

Abschnitt	Einstellung	Beschreibung
	`BadUSBAttackPrevention`	Schutz vor modifizierten USB-Geräten.
	`EDR`	Endpoint Detection and Response Optimum Die Komponente ist nicht kompatibel mit den Komponenten Endpoint Detection and Response Expert (cloud) (`EDRCloud`) und Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) Die Komponente ist nicht kompatibel mit den Komponenten Endpoint Detection and Response Optimum (`EDR`) und Endpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) Die Komponente ist nicht kompatibel mit den Komponenten Endpoint Detection and Response Expert (cloud) (`EDRCloud`) und Endpoint Detection and Response Optimum (`EDR`).
	`SB`	Kaspersky Sandbox oder KATA Sandbox. *Kaspersky Sandbox* ist eine eigenständige Detection and Response-Lösung von Kaspersky. *KATA Sandbox* ist eine Komponente der Lösung Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) Die Komponente ist nicht kompatibel mit den Komponenten Endpoint Detection and Response Expert (cloud) (`EDRCloud`) und Endpoint Detection and Response Optimum (`EDR`).
	`AdminKitConnector`	Programmverwaltung mithilfe von Administrationssystemen. Zu den Administrationssystemen zählt beispielsweise Kaspersky Security Center. Sie können Kaspersky-Administrationssysteme oder Lösungen von Drittanbietern verwenden. Kaspersky Endpoint Security bietet eine entsprechende API. Mögliche Werte: • `1` – Die Programmverwaltung mithilfe von Administrationssystemen ist erlaubt (Standardwert). • `0` – Die Programmverwaltung ist nur über die lokale Schnittstelle erlaubt.
	`KUMAIntegration`	Integration mit KUMA.
	`StandaloneKATA`	Installieren der App im Modus zur Integration von Endpoint Detection and Response Agent (EDR Agent) in die Lösung Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	Installieren der App im Modus zur Integration von Endpoint Detection and Response Agent (EDR Agent) in die Lösung Kaspersky Managed Detection and Response.
	`StandaloneNDR`	Installieren der App im Modus zur Integration von Endpoint Detection and Response Agent (EDR Agent) in die Lösung Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	Installieren der App im Modus zur Integration von Endpoint Detection and Response Agent (EDR Agent) in KUMA.
`[Tasks]`	`ScanMyComputer`	Aufgabe zur vollständigen Untersuchung. Mögliche Werte: • `1` – Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen. • `0` – Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.

Abschnitt	Einstellung	Beschreibung
	`ScanCritical`	Aufgabe zur Untersuchung wichtiger Bereiche. Mögliche Werte: • `1` – Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen. • `0` – Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.
	`Updater`	Update-Aufgabe. Mögliche Werte: • `1` – Die Aufgabe wird in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen. • `0` – Die Aufgabe wird nicht in die Aufgabenliste für Kaspersky Endpoint Security aufgenommen.

Prozesse von Kaspersky Endpoint Security für Windows

Kaspersky Endpoint Security for Windows startet die in der folgenden Tabelle beschriebenen Prozesse.

Prozesse von Kaspersky Endpoint Security für Windows

Dateiname	Ziel
avp.exe	Arbeitsprozess von Kaspersky Endpoint Security für Windows.
avpsus.exe	Mit diesem Prozess können kritische und genehmigte Updates für Programm-Module installiert und zurückgesetzt werden.

Auswahl der Programmkomponenten ändern

Bei der Programminstallation können Sie die Komponenten auswählen, die verfügbar sein sollen. Sie können die Zusammensetzung des Programms wie folgt ändern:

- Lokal mithilfe des Installationsassistenten für das Programm.

  Die Zusammensetzung des Programms wird mit den üblichen Mitteln des Windows-Betriebssystems geändert, also über die Systemsteuerung. Starten Sie den Installationsassistenten und wählen Sie das Ändern der Auswahl der Programmkomponenten aus. Folgen Sie den Anweisungen auf dem Bildschirm.

  > Diese Methode ist nicht verfügbar, wenn die Anwendung über Kaspersky Security Center installiert wurde. Sie können die Auswahl der Anwendungskomponenten erst dann in der Systemsteuerung ändern, nachdem Sie die Anwendung lokal installiert haben.

- per Fernzugriff mithilfe von Kaspersky Security Center.

  Um die Auswahl der Komponenten von Kaspersky Endpoint Security nach der Programminstallation zu ändern, können Sie die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Für eine Änderung der Auswahl der Programmkomponenten gelten die folgenden Besonderheiten:

- Auf einem Computer mit dem Betriebssystem Windows Server können nicht alle Komponenten von Kaspersky Endpoint Security installiert werden (z. B. ist die Komponente „Adaptive Kontrolle von Anomalien“ nicht verfügbar).
- Wenn Festplatten auf dem Computer durch die vollständige Festplattenverschlüsselung (FDE) verschlüsselt sind, kann die Komponente „Vollständige Festplattenverschlüsselung“ nicht entfernt werden. Um die Komponente „Vollständige Festplattenverschlüsselung“ zu entfernen, entschlüsseln Sie alle Festplatten des Computers.
- Wenn auf dem Computer verschlüsselte Dateien (FLE) vorhanden sind oder der Benutzer verschlüsselte Wechseldatenträger (FDE oder FLE) verwendet, ist ein Zugriff auf die Daten und Wechseldatenträger nicht mehr möglich, nachdem die Datenverschlüsselungskomponenten entfernt wurden. Sie können Zugriff auf die Daten und Wechseldatenträger erhalten, wenn Sie die Datenverschlüsselungskomponenten neu installieren.
- Wenn das Programm im Light Agent-Modus in einer VDI-Infrastruktur installiert ist, wird das Ändern der Komponentenauswahl nicht unterstützt.

Hinzufügen oder Löschen von Programmkomponenten in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Zu installierende Komponenten auswählen** aus.

Schritt 2. Einstellungen für die Aufgabe zum Ändern der Programmkomponenten

Wählen Sie die Konfiguration des Programms aus:

- **Standardmodus für den Schutz von Hosts**. Die Standardkonfiguration. Mit dieser Konfiguration können Sie alle Programmkomponenten verwenden, einschließlich Komponenten, die die Detection and Response-Lösungen unterstützen. Diese Konfiguration bietet einen umfassenden Schutz des Computers vor einer Vielzahl von Bedrohungen, Netzwerkangriffen und Betrugsversuchen.

- **Endpoint Detection and Response Agent für den Schutz vor komplexen Bedrohungen und gezielten Angriffen**. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.

  Wenn Sie die Programmkonfiguration für den EDR-Agenten ändern, damit dieser mit MDR funktioniert, stellen Sie sicher, dass die für den Empfang von Telemetriedaten verantwortlichen Komponenten aktiviert sind.

- **Light Agent für den Schutz virtueller Umgebungen**. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.

Wählen Sie die Programmkomponenten aus, die auf dem Benutzercomputer verfügbar sein sollen.

Schritt 3. Erweiterte Einstellungen

Konfigurieren Sie die erweiterten Einstellungen für die Aufgabe (siehe Tabelle unten).

Schritt 4. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 5. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 6. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgaben ein, z. B. *Komponente „Programmkontrolle“ hinzufügen*.

Schritt 7. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Hinzufügen oder Löschen von Programmkomponenten in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2.0**.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Auswahl der Programmkomponenten ändern**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Komponente „Programmkontrolle" hinzufügen*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Sie können beispielsweise eine bestimmte Administrationsgruppe auswählen oder eine Auswahl erstellen.

Schritt 3. Erstellung der Aufgabe abschließen

Aktivieren Sie das Kontrollkästchen **Nach Abschluss der Erstellung Aufgabendetails öffnen** und schließen Sie den Assistenten ab.

Wählen Sie in den Eigenschaften der Aufgabe die Registerkarte **Anwendungseinstellungen** aus. Wählen Sie nun die Konfiguration des Programms aus:

- **Standard-Modus für den Schutz von Workstations und Servern**. Die Standardkonfiguration. Mit dieser Konfiguration können Sie alle Programmkomponenten verwenden, einschließlich Komponenten, die die Detection and Response-Lösungen unterstützen. Diese Konfiguration bietet einen umfassenden Schutz des Computers vor einer Vielzahl von Bedrohungen, Netzwerkangriffen und Betrugsversuchen.

- **Endpoint Detection and Response Agent für den Schutz vor komplexen Bedrohungen und gezielten Angriffen**. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.

  Wenn Sie die Programmkonfiguration für den EDR-Agenten ändern, damit dieser mit MDR funktioniert, stellen Sie sicher, dass die für den Empfang von Telemetriedaten verantwortlichen Komponenten aktiviert sind.

- **Light Agent für den Schutz virtueller Umgebungen**. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.

Wählen Sie die Programmkomponenten aus, die auf dem Benutzercomputer verfügbar sein sollen. Konfigurieren Sie die erweiterten Einstellungen für die Aufgabe (siehe Tabelle unten).

Dadurch wird auf den Benutzercomputern die Auswahl der Komponenten von Kaspersky Endpoint Security im unbeaufsichtigten Modus geändert. Auf der lokalen Programmoberfläche werden die Einstellungen für die verfügbaren Komponenten angezeigt. Programmkomponenten, die nicht ausgewählt wurden, sind deaktiviert und die Einstellungen für diese Komponenten sind nicht verfügbar.

Bei der Installation, beim Update oder bei der Deinstallation von Kaspersky Endpoint Security können Fehler auftreten. Weitere Informationen zur Behebung dieser Fehler finden Sie in der Wissensdatenbank des Technischen Supports.

Einstellung	Beschreibung
Aufgabeneinstellungen	**Auf inkompatible Drittersteller-Programme überprüfen**. Kaspersky Endpoint Security überprüft standardmäßig, ob die installierten Programme kompatibel sind. Eine Liste der Software, die Kompatibilitätsprobleme verursachen kann, befindet sich in der Datei incompatible.txt. Diese Datei gehört zum Lieferumfang. Wenn die Untersuchung von installierten Programmen aktiviert ist und ein Programm aus der Liste gefunden wird, hält Kaspersky Endpoint Security die Aufgabe an. Wenn in der Herstellerdokumentation der Drittanbieter-Programme angegeben ist, dass diese mit Endpoint Protection Platform (EPP) kompatibel sind, können Sie die Untersuchung von installierten Programmen deaktivieren. **Inkompatible Programme von Drittherstellern entfernen**. Automatisches Entfernen von Programmen, die in der Datei incompatible.txt enthalten sind, bevor die Auswahl der Komponenten geändert wird. Wenn diese Funktionalität aktiviert ist, versucht Kaspersky Endpoint Security, die inkompatiblen Programme zu entfernen, damit die Aufgabe fortgesetzt werden kann. **Azure WVD-Kompatibilitätsmodus verwenden**. Diese Funktion sorgt dafür, dass der Status der virtuellen Azure-Maschine in der Kaspersky Anti Targeted Attack Platform-Konsole korrekt angezeigt wird. Zur Überwachung der Computerleistung sendet Kaspersky Endpoint Security Telemetriedaten an die KATA-Server. Die Telemetrie umfasst eine ID des Computers (Sensor ID). Mithilfe des Azure WVD-Kompatibilitätsmodus können Sie diesen virtuellen Computern eine permanente eindeutige Sensor ID zuweisen. Wenn der Kompatibilitätsmodus deaktiviert ist, ändert sich die Sensor ID aufgrund der Funktionsweise von virtuellen Azure-Maschinen möglicherweise nach dem Neustart des Computers. Dies kann dazu führen, dass in der Konsole Duplikate von virtuellen Maschinen angezeigt werden.
Ausnahmen	Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Ab Kaspersky Endpoint Security 12.8 für Windows können Sie das Programm im Light Agent-Modus installieren, um virtuelle Umgebungen zu schützen. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren. Sie können die vertrauenswürdige Zone auch später in den Richtlinieneigenschaften konfigurieren: Untersuchungsausnahmen und vertrauenswürdige Programme.
Getrennter Modus / Kombinierter Modus	Sie können die Auswahl der Komponenten für Workstations und Server separat festlegen – **Getrennter Modus**. Vor der Bereitstellung des Installationspakets ermittelt das Installationsprogramm den Typ des Betriebssystems und installiert nur die Programmkomponenten, die Sie für diesen Betriebssystemtyp ausgewählt haben. Sie können also dasselbe Installationspaket für Workstations und Server verwenden. **Kombinierter Modus** bietet eine gemeinsame Liste von Komponenten für Workstations und Server. Die Verfügbarkeit der einzelnen Komponenten ist vom Betriebssystemtyp abhängig. In diesem Modus sollte ein separates Installationspaket für Workstations und ein separates Installationspaket für Server erstellt werden. Eine gemeinsame Komponentenliste für das Installationspaket kann nur im Standardmodus konfiguriert werden.
Kennwort für das Ändern der Programmkomponentenauswahl verwenden	Normalerweise aktivieren Administratoren den Kennwortschutz, um den Zugriff auf Kaspersky Endpoint Security einzuschränken. Das heißt, um die Auswahl der App-Komponenten zu ändern, müssen Sie die Anmeldedaten eines Benutzers eingeben, der die Berechtigung **App entfernen/ändern/reparieren** hat. Sie können beispielsweise das KL Admin-Konto verwenden.
Kennwort verwenden, um Kaspersky Endpoint Agent und Kaspersky Security für Windows Server zu deinstallieren	Normalerweise aktivieren Administratoren den Kennwortschutz in den Einstellungen dieser Aufgaben, um den Zugriff auf Kaspersky Endpoint Agent (KEA) und Kaspersky Security für Windows Server (KSWS) einzuschränken. Wenn Sie von der [KES+KEA]-Konfiguration zu [KES+built-in agent] migrieren oder wenn Sie von KSWS zu KES migrieren, müssen Sie darum ein Kennwort eingeben, um diese Apps zu entfernen.

Upgrade einer älteren Programmversion

Das Upgrade einer Vorgängerversion des Programms besitzt die folgenden Besonderheiten:

- Vor Beginn des Programm-Upgrades sollten Sie alle laufenden Programme schließen.
- Vor dem Upgrade blockiert Kaspersky Endpoint Security die Funktionalität zur vollständigen Festplattenverschlüsselung. Falls die Funktionalität zur vollständigen Festplattenverschlüsselung nicht blockiert werden kann, wird die Upgrade-Installation nicht gestartet. Nach dem Programm-Upgrade wird die Funktionalität zur vollständigen Festplattenverschlüsselung wiederhergestellt.
- Um die Sprache des Programms zu ändern, wählen Sie in der Aufgabe *Remote-Installation einer Anwendung* das Installationspaket mit der gewünschten Lokalisierung aus und aktualisieren Sie das Programm. Die Möglichkeit, die Programmsprache zu ändern, wurde erstmals in Kaspersky Endpoint Security für Windows 14.2 eingeführt.

Kaspersky Endpoint Security unterstützt ein Update der folgenden Programmversionen:

- Kaspersky Endpoint Security 12.3 für Windows (Version 12.3.0.493)
- Kaspersky Endpoint Security 12.4 für Windows (Version 12.4.0.467)
- Kaspersky Endpoint Security 12.5 für Windows (Version 12.5.0.539)
- Kaspersky Endpoint Security 12.6 für Windows (Version 12.6.0.438)
- Kaspersky Endpoint Security 12.7 für Windows (Version 12.7.0.533)
- Kaspersky Endpoint Security 12.8 für Windows (Version 12.8.0.505)
- Kaspersky Endpoint Security 12.9 für Windows (Version 12.9.0.384)
- Kaspersky Endpoint Security 12.10 für Windows (Version 12.10.0.466)
- Kaspersky Endpoint Security 12.11 für Windows (Version 12.11.0.637)
- Kaspersky Endpoint Security 12.12 für Windows (Version 12.12.0.522)
- Kaspersky Endpoint Security 14.0 für Windows (Version 14.0.0.504)
- Kaspersky Endpoint Security 14.1 für Windows (Version 14.1.0.423)

Bei der Installation, beim Update oder bei der Deinstallation von Kaspersky Endpoint Security können Fehler auftreten. Weitere Informationen zur Behebung dieser Fehler finden Sie in der Wissensdatenbank des Technischen Supports.

Methoden für das Programm-Upgrade

Um das Programm Kaspersky Endpoint Security auf einem Computer zu aktualisieren, gibt es folgende Möglichkeiten:

- Verwendung des Kaspersky-Update-Dienstes (Seamless Update – SMU).
- lokal mithilfe des Installationsassistenten für das Programm.
- lokal aus der Befehlszeile
- per Fernzugriff mithilfe von Kaspersky Security Center.
- per Fernzugriff über den Gruppenrichtlinien-Editor von Microsoft Windows (Details finden Sie auf der Website des technischen Supports von Microsoft).
- per Fernzugriff mithilfe von System Center Configuration Manager

Ist im Unternehmensnetzwerk das Programm mit einem Komponentensatz verteilt, der sich vom Standardsatz unterscheidet, so unterscheidet sich das Programm-Upgrade über die Verwaltungskonsole (MMC) vom Programm-Upgrade über die Web Console. Beim Update von Kaspersky Endpoint Security sind die folgenden Besonderheiten zu berücksichtigen:

- Kaspersky Security Center Web Console.

  Wenn Sie ein Installationspaket für die neue Programmversion mit dem standardmäßigen Komponentensatz erstellt haben, wird der Komponentensatz auf dem Benutzercomputer nach dem Upgrade nicht verändert. Um Kaspersky Endpoint Security mit dem standardmäßigen Komponentensatz zu verwenden, gehen Sie wie folgt vor: Öffnen Sie die Eigenschaften des Installationspakets, ändern Sie den Komponentensatz, setzen Sie den Komponentensatz auf den ursprünglichen Zustand zurück und speichern Sie die Änderungen.

- Kaspersky Security Center Verwaltungskonsole.

  Nach dem Upgrade entspricht der Komponentensatz des Programms dem Komponentensatz im Installationspaket. Wenn die neue Programmversion den standardmäßigen Komponentensatz besitzt, wird beispielsweise der integrierte MDR-Agent vom Computer gelöscht, da diese Komponente nicht zum Standardsatz gehört. Um das Programm weiterhin mit dem bisherigen Komponentensatz zu verwenden, müssen die erforderlichen Komponenten in den Einstellungen des Installationspakets ausgewählt werden.

Programm-Upgrade ohne Neustart

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.

Nach einem Upgrade des Programms, einer Patch-Installation, einer Änderung der Programmkomponenten oder einer Wiederherstellung wird Kaspersky Endpoint Security neu gestartet, um die neue Version zu verwenden. Der Neustart von Kaspersky Endpoint Security kann bis zu einer Minute dauern. In diesem Zeitraum ist das Schutzniveau des Computers reduziert. Nach dem Neustart des Programms wird die Schutzstufe des Computers wiederhergestellt.

So wählen Sie über die Verwaltungskonsole (MMC) den Modus für das Programm-Upgrade aus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Programmeinstellungen** aus.
5. Aktivieren oder deaktivieren Sie im Block **Erweiterte Einstellungen** das Kontrollkästchen **Programm-Updates ohne Neustart installieren**, um den Modus für das Programm-Upgrade zu konfigurieren.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie über die „Web Console“ den Modus für das Programm-Upgrade aus

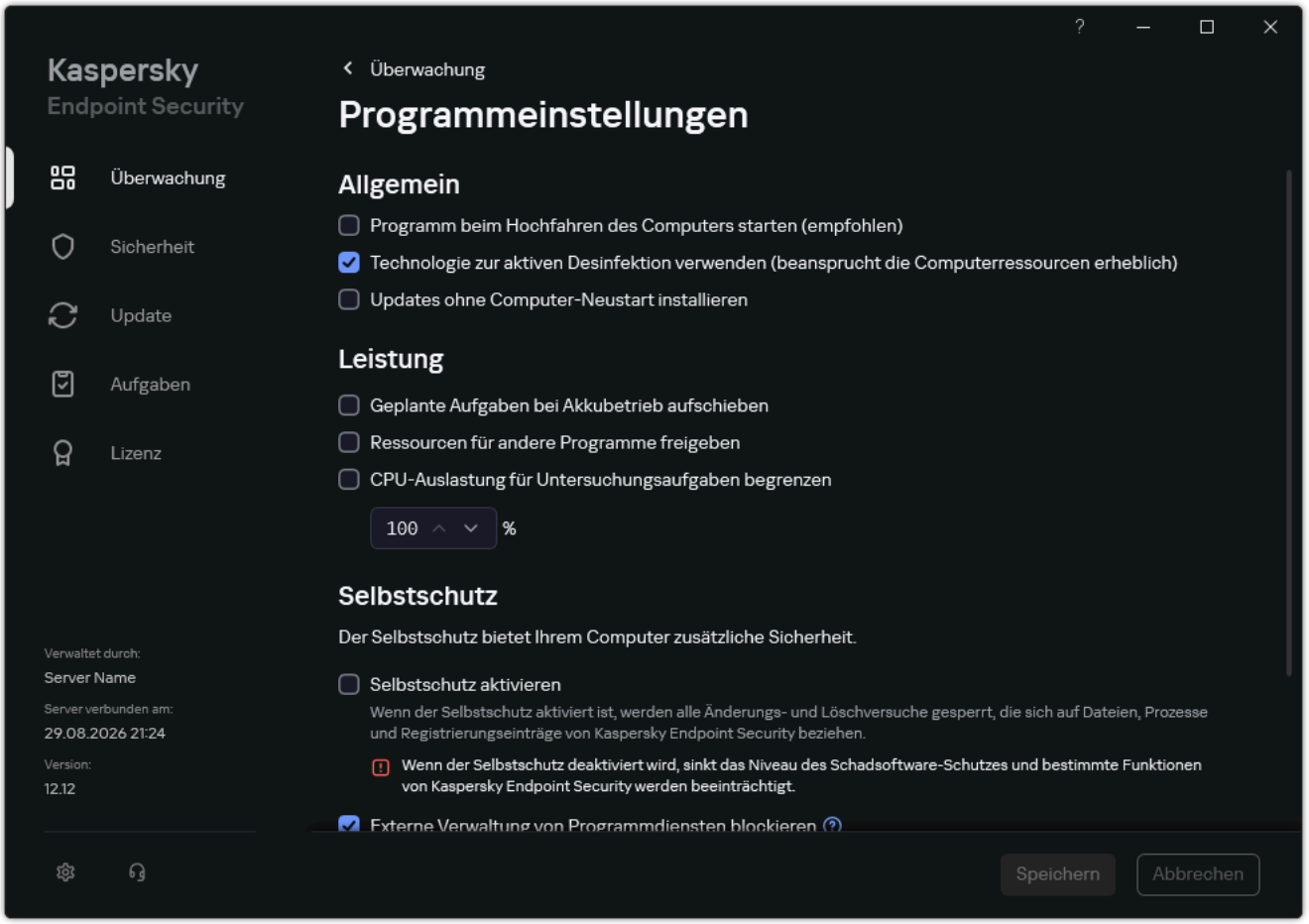
1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.
5. Aktivieren oder deaktivieren Sie im Block **Einstellungen für das Programm-Update** das Kontrollkästchen **Programm-Updates ohne Neustart installieren**, um den Modus für das Programm-Upgrade zu konfigurieren.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie über die Benutzeroberfläche den Modus für das Programm-Upgrade aus

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Aktivieren oder deaktivieren Sie im Block **Allgemein** das Kontrollkästchen **Updates ohne Computer-Neustart installieren**, um den Modus für das Programm-Upgrade zu konfigurieren.

4. Speichern Sie die vorgenommenen Änderungen.

Sie können den Modus für das Programm-Upgrade auch beim Installieren des Programms über die Befehlszeile (mithilfe der Option `UPGRADEMODE`) auswählen.

Nachdem das Programm-Upgrade ohne Neustart abgeschlossen wurde, wurde die neue Version von Kaspersky Endpoint Security auf dem Computer installiert. Die vorherige Version des Programms wird automatisch gelöscht.

Sie können ein Programm-Upgrade erst starten, nachdem das vorherige Upgrade vollständig abgeschlossen wurde.

Sie können den Upgrade-Status von Kaspersky Endpoint Security überprüfen. Verwenden Sie dazu den Versionsbericht der Kaspersky-App in der Kaspersky Security Center-Konsole.

SMU-Update der Anwendung

Um das Programm mithilfe des Kaspersky-Update-Dienstes zu aktualisieren (Seamless Update; SMU), müssen Sie das Installationsprogramm nicht ausführen. Dies ist ein Unterschied zu anderen Update-Methoden. Kaspersky Endpoint Security empfängt die neue Programmversion zusammen mit den Antiviren-Datenbanken aus derselben Quelle.

Mithilfe eines SMU-Update können Sie das Programm auf allen Computern Ihres Unternehmens auf die neueste Version aktualisieren. Es wird empfohlen, die neue Version des Programms auf einigen Computern zu testen, bevor ein SMU-Update übernommen wird. Dazu müssen Sie das Programm auf diesen Computern manuell aktualisieren (z. B. lokal über den Installationsassistenten). Wenn Sie ein SMU-Update ausführen, können Sie keine einzelnen Computer auswählen.

Der Update-Zeitplan für das Programm wird vom Kaspersky-Team festgelegt. Um einen reibungslosen Betrieb der neuen Programmversion zu gewährleisten, stellt Kaspersky die Updates schrittweise zur Verfügung. Das bedeutet, dass Sie Ihr SMU-Update möglicherweise erst bis zu zwei Monate später erhalten, nachdem eine neue Version veröffentlicht wird.

Sie können das SMU-Update des Programms mithilfe der Aufgabe *Update der Datenbanken und Programm-Module* verwalten. Damit die neue Programmversion im Paket mit den Antiviren-Datenbanken enthalten ist, müssen Sie das Update der *Programm-Module* in den Einstellungen der Aufgabe *Update der Datenbanken und Programm-Module* zulassen. In in den Einstellungen der Aufgabe *Update der Datenbanken und Programm-Module* können Sie auch die Aktualisierung des Programms ohne Neustart erlauben.

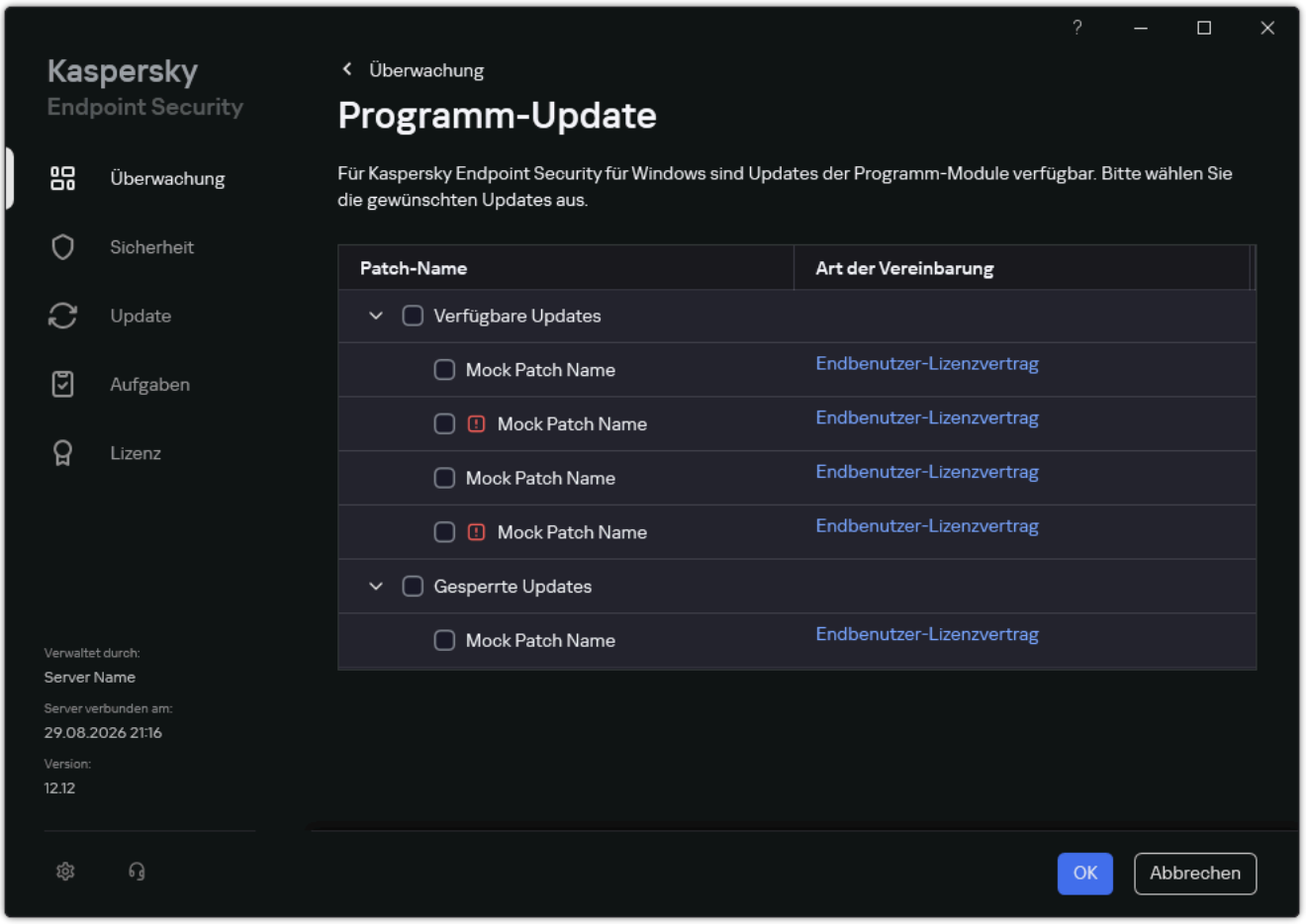
Schritte eines SMU-Programm-Updates

1. **Nach der Veröffentlichung einer neuen Programmversion verteilt Kaspersky das Update.**
2. **Der Benutzer stimmt dem Programm-Update zu.**

   Wenn der Computer mit Kaspersky Security Center verbunden ist, ist das Update in Kaspersky Security Center im Abschnitt **Update der Kaspersky-Datenbanken und Programm-Module** verfügbar. Weitere Informationen über die Genehmigung von Updates finden Sie in der Hilfe zu Kaspersky Security Center.

   Wenn der Computer nicht mit Kaspersky Security Center verbunden ist, steht das Update im Benachrichtigungsbereich der Programmoberfläche zur Verfügung: . Um das Update zu genehmigen, wählen Sie eine Programmversion aus und akzeptieren die Bedingungen der Vereinbarung (siehe Abbildung unten).
3. **Kaspersky Endpoint Security führt die Aufgabe *Update der Datenbanken und Programm-Module* nach dem festgelegten Zeitplan aus.**

Daraufhin aktualisiert Kaspersky Endpoint Security das Programm im unbeaufsichtigten Modus.



Verfügbare Programm-Updates

Die App entfernen

Wenn Kaspersky Endpoint Security entfernt wird, sind der Computer und die Benutzerdaten ungeschützt.

Bei der Installation, beim Update oder bei der Deinstallation von Kaspersky Endpoint Security können Fehler auftreten. Weitere Informationen zur Behebung dieser Fehler finden Sie in der Wissensdatenbank des Technischen Supports.

Das Programm per Fernzugriff über Kaspersky Security Center entfernen

Sie können das Programm ferngesteuert entfernen mithilfe der Aufgabe *Remote-Deinstallation einer Anwendung*. Wenn diese Aufgabe ausgeführt wird, lädt Kaspersky Endpoint Security ein Hilfsprogramm für die Programm-Deinstallation auf den Benutzercomputer herunter. Nach Abschluss der Programm-Deinstallation wird das Hilfsprogramm automatisch gelöscht.

Entfernen des Programms über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
3. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie die Option **Kaspersky Security Center Administrationsserver → Erweitert → Remote-Deinstallation einer Anwendung**.

Schritt 2. Auswahl des zu entfernenden Programms

Wählen Sie den Punkt **Anwendung deinstallieren, das von Kaspersky Security Center unterstützt wird**.

Schritt 3. Einstellungen für die Aufgabe zum Entfernen des Programms

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** aus.

Schritt 4. Einstellungen des Deinstallations-Hilfsprogramms

Passen Sie die folgenden erweiterten Programmeinstellungen an:

- **Download des Deinstallations-Tools erzwingen**. Wählen Sie aus, auf welche Weise das Hilfsprogramm bereitgestellt werden soll:
  - **Unter Nutzung des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten deinstalliert.
  - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Das Hilfsprogramm wird durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.
  - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Das Tool wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Weitere Informationen über die Verwendung von Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center.
- **Typ des Betriebssystems vor dem Download überprüfen**. Deaktivieren Sie dieses Kontrollkästchen bei Bedarf. Dadurch lässt sich verhindern, dass das Deinstallations-Hilfsprogramm heruntergeladen wird, wenn das Betriebssystem des Computers die Softwarevoraussetzungen nicht erfüllt. Wenn Sie sicher sind, dass das Betriebssystem des Computers die Softwarevoraussetzungen erfüllt, kann diese Überprüfung übersprungen werden.

Wenn der Vorgang zur Programm-Deinstallation durch ein Kennwort geschützt ist, gehen Sie wie folgt vor:

1. Aktivieren Sie das Kontrollkästchen **Deinstallationskennwort verwenden**.
2. Klicken Sie auf **Bearbeiten**.
3. Geben Sie das Kennwort des Benutzerkontos KLAdmin ein.

Schritt 5. Einstellungen für den Neustart des Betriebssystems auswählen

Nach der Programm-Deinstallation ist ein Neustart erforderlich. Wählen Sie aus, welche Aktion zum Neustart des Computers ausgeführt werden soll.

Schritt 6. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 7: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Es ist nicht erforderlich, für die Deinstallation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten, ein Benutzerkonto auszuwählen.

Schritt 8. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 9. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein (z. B. *Kaspersky Endpoint Security 14.2 entfernen*).

Schritt 10. Aufgabenerstellung abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Die Programm-Deinstallation wird im unbeaufsichtigten Modus ausgeführt.

So entfernen Sie das Programm über die Web Console und die Cloud Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt **Kaspersky Security Center** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Remote-Deinstallation einer Anwendung**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, z. B. *Deinstallation von Kaspersky Endpoint Security auf den Computern des Technischen Supports*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Sie können beispielsweise eine bestimmte Administrationsgruppe auswählen oder eine Auswahl erstellen.

Schritt 3. Einstellungen für die Programm-Deinstallation anpassen

Passen Sie bei diesem Schritt die Einstellungen für die Programm-Deinstallation an:

1. Wählen Sie den Typ **Verwaltete Anwendung deinstallieren** aus.
2. Wählen Sie das **Programm** Kaspersky Endpoint Security für Windows aus.

3. **Download des Deinstallations-Tools erzwingen**. Wählen Sie aus, auf welche Weise das Hilfsprogramm bereitgestellt werden soll:

   - **Unter Nutzung des Administrationsagenten**. Wenn der Administrationsagent nicht auf dem Computer installiert ist, wird zuerst der Administrationsagent mithilfe von Betriebssystemmitteln installiert. Danach wird Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten deinstalliert.

   - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Das Hilfsprogramm wird durch Betriebssystemmittel mithilfe des Administrationsservers an die Client-Computer zugestellt. Diese Variante kann ausgewählt werden, wenn auf dem Client-Computer kein Administrationsagent installiert ist, der Client-Computer sich aber im gleichen Netzwerk befindet wie der Administrationsserver.

   - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**. Das Tool wird durch Betriebssystemmittel über Verteilungspunkte an die Client-Computer übertragen. Diese Variante kann ausgewählt werden, wenn im Netzwerk mindestens ein Verteilungspunkt vorhanden ist. Weitere Informationen über die Verwendung von Verteilungspunkten finden Sie in der Hilfe zu Kaspersky Security Center.

4. Legen Sie im Feld **Maximale Anzahl gleichzeitiger Downloads** fest, wie viele Anfragen für den Download des Hilfsprogramms zur Programm-Deinstallation maximal an den Administrationsserver gestellt werden dürfen. Durch die Beschränkung der Anfragen lässt sich eine Überlastung des Netzwerks vermeiden.

5. Legen Sie im Feld **Maximale Anzahl der Deinstallationsversuche** fest, wie oft versucht werden darf, das Programm zu deinstallieren. Wenn die Deinstallation von Kaspersky Endpoint Security mit einem Fehler beendet wird, startet die Aufgabe die Deinstallation automatisch erneut.

6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Typ des Betriebssystems vor dem Download überprüfen**. Dadurch lässt sich verhindern, dass das Deinstallations-Hilfsprogramm heruntergeladen wird, wenn das Betriebssystem des Computers die Softwarevoraussetzungen nicht erfüllt. Wenn Sie sicher sind, dass das Betriebssystem des Computers die Softwarevoraussetzungen erfüllt, kann diese Überprüfung übersprungen werden.

Schritt 4: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie ein Benutzerkonto für die Installation des Administrationsagenten mithilfe von Betriebssystemmitteln aus. In diesem Fall sind für den Zugriff auf den Computer Administratorrechte erforderlich. Sie können mehrere Benutzerkonten hinzufügen. Wenn ein Benutzerkonto nicht die erforderlichen Rechte besitzt, verwendet der Installationsassistent das nächste Benutzerkonto. Es ist nicht erforderlich, für die Deinstallation von Kaspersky Endpoint Security mit den Mitteln des Administrationsagenten, ein Benutzerkonto auszuwählen.

Schritt 5. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertigstellen**. Die neue Aufgabe wird in der Aufgabenliste angezeigt.

Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**, um die Aufgabe auszuführen. Die Programm-Deinstallation wird im unbeaufsichtigten Modus ausgeführt. Nach dem Abschluss der Deinstallation fragt Kaspersky Endpoint Security, ob der Computer neu gestartet werden soll.

Falls der Vorgang zur Programm-Deinstallation kennwortgeschützt ist, geben Sie in den Eigenschaften der Aufgabe *Remote-Deinstallation des Programms* das Kennwort des Benutzerkontos KLAdmin ein. Ohne Kennwort wird die Aufgabe nicht ausgeführt.

Um in der Aufgabe „Remote-Deinstallation des Programms" das Kennwort des Benutzerkontos KLAdmin zu verwenden, gehen Sie wie folgt vor:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Security Center-Aufgabe **Remote-Deinstallation einer Anwendung**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Aktivieren Sie das Kontrollkästchen **Deinstallationskennwort verwenden**.

5. Geben Sie das Kennwort des Benutzerkontos KLAdmin ein.

6. Speichern Sie die vorgenommenen Änderungen.

Den Computer neu starten, um die Deinstallation abzuschließen. Dazu zeigt der Administrationsagent ein Pop-up-Fenster an.

Das Programm per Fernzugriff über Active Directory entfernen

Sie können das Programm per Fernzugriff über eine Microsoft Windows-Gruppenrichtlinie deinstallieren. Wenn Sie das Programm deinstallieren möchten, müssen Sie die Gruppenrichtlinien-Verwaltungskonsole (gpmc.msc) öffnen und den Editor für Gruppenrichtlinien verwenden, um eine Aufgabe zum Entfernen des Programms zu erstellen (weitere Informationen finden Sie auf der Website des Technischen Supports von Microsoft).

Wenn der Vorgang zur Programm-Deinstallation durch ein Kennwort geschützt ist, ist folgendes Vorgehen notwendig:

1. Erstellen Sie eine BAT-Datei mit den folgenden Inhalten:

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   <GUID> ist die einmalige Programm-ID. Die Programm-GUID können Sie in der Wissensdatenbank des Technischen Supports oder mithilfe des folgenden Befehls ermitteln:

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   Beispiel

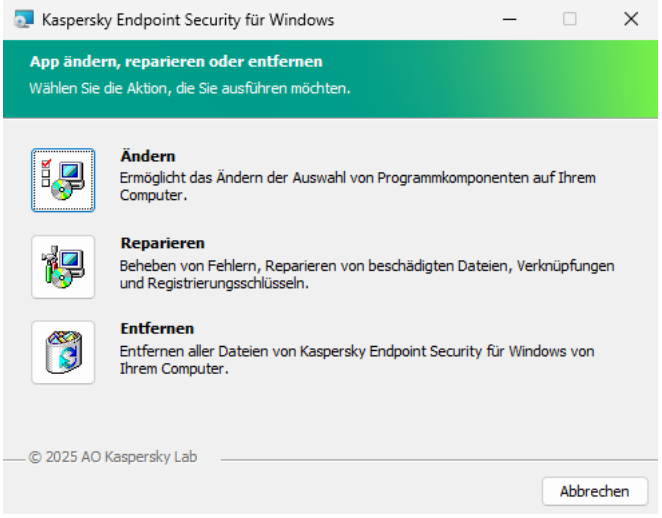
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. Erstellen Sie in der Gruppenrichtlinien-Verwaltungskonsole (gpmc.msc) eine Microsoft Windows-Richtlinie für die Computer.

3. Verwenden Sie die neue Richtlinie, um die erstellte BAT-Datei auf den Computern auszuführen.

Die Anwendung lokal entfernen

Sie können die Anwendung auch lokal mithilfe des Setup-Assistenten entfernen. Kaspersky Endpoint Security wird mit den gewöhnlichen Mitteln des Windows-Betriebssystems entfernt: über die Systemsteuerung. Der Setup-Assistent wird gestartet. Folgen Sie den Anweisungen auf dem Bildschirm.



Auswählen des Programmentfernungsvorgangs

Hier können Sie festlegen, welche vom Programm verwendeten Daten Sie beibehalten möchten, um sie später bei einer Neuinstallation des Programms (z. B. Installation einer neueren Version) wiederzuverwenden. Wenn Sie keine Daten angeben, wird das Programm vollständig entfernt (siehe Bild unten).



Speichern von Daten nach dem Entfernen

Sie können folgende Daten speichern:

- **Aktivierungsdaten** sind Daten, die es erlauben, das Programm künftig nicht erneut zu aktivieren. Kaspersky Endpoint Security fügt automatisch einen Lizenzschlüssel hinzu, falls die Lizenz zum Zeitpunkt der Installation nicht abgelaufen ist.

- **Backup-Dateien** sind Dateien, die vom Programm untersucht und ins Backup verschoben wurden.

  Der Zugriff auf Backup-Dateien, die nach der Deinstallation des Programms gespeichert bleiben, ist nur mit der Programmversion möglich, in welcher die Dateien gespeichert wurden.

  Falls Sie Backup-Objekte nach der Programm-Deinstallation verwenden möchten, müssen Sie diese vor der Deinstallation des Programms wiederherstellen. Die Kaspersky-Experten raten jedoch davon ab, Objekte aus dem Backup wiederherzustellen, da dadurch der Computer beschädigt werden kann.

- **Programmeinstellungen** sind Einstellungen für die Programmausführung, die im Verlauf der Programmnutzung angepasst wurden.

- **Lokaler Speicher für Chiffrierschlüssel** enthält Daten, die den Zugriff auf jene Dateien und Datenträger ermöglichen, die vor der Programm-Deinstallation verschlüsselt wurden. Um auf verschlüsselte Dateien und Datenträger zuzugreifen, vergewissern Sie sich, dass Sie bei der erneuten Installation von Kaspersky Endpoint Security die Funktionalität zur Datenverschlüsselung ausgewählt haben. Für den Zugriff auf früher verschlüsselte Dateien und Datenträger sind keine weiteren Maßnahmen erforderlich.

Kaspersky Endpoint Security speichert Daten im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

Sie können die Anwendung auch lokal über die Befehlszeile entfernen.

Lizenzverwaltung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für Kaspersky Endpoint Security zusammenhängen.

Über den Endbenutzer-Lizenzvertrag

Der *Lizenzvertrag* ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig durch, bevor Sie beginnen, mit dem Programm zu arbeiten.

Die Lizenzbedingungen können Sie wie folgt einsehen:

- Im interaktiven Modus während der Installation von Kaspersky Endpoint Security.
- Im Dokument license.txt. Dieses Dokument gehört zum Lieferumfang des Programms und befindet sich auch im Installationsordner des Programms `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES`.

Wenn Sie bei der Programminstallation den Lizenzbedingungen zustimmen, gilt Ihr Einverständnis mit den Lizenzbedingungen als erteilt. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird.

Die Lizenz berechtigt Sie, das Programm gemäß den Bedingungen des Endbenutzer-Lizenzvertrags zu nutzen und technischen Support zu erhalten. Der Umfang der verfügbaren Funktionen und die Nutzungsdauer des Programms sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen:

- *Testlizenz* - kostenlose Lizenz zum Kennenlernen des Programms.

  Die Testlizenz ist in der Regel nur für eine kurze Zeit gültig. Nach Ablauf der Testlizenz stellt Kaspersky Endpoint Security die Funktion ein. Um das Programm weiterhin nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Sie können das Programm nur ein Mal mit der Testlizenz aktivieren. Wenn das Programm bereits mit einer kommerziellen Lizenz aktiviert wurde, kann es nicht mehr mit einer Testlizenz aktiviert werden.

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

  Die im Rahmen einer kommerziellen Lizenz verfügbare Programmfunktionalität ist von der Auswahl des Produkts abhängig. Das ausgewählte Produkt ist im Lizenzzertifikat angegeben. Informationen über die verfügbaren Produkte finden Sie auf der Website von Kaspersky.

Wenn die kommerzielle Lizenz abläuft, werden wichtige Funktionen der App deaktiviert. Um das Programm weiterhin nutzen zu können, müssen Sie Ihre Lizenz verlängern. Wenn Sie Ihre Lizenz nicht verlängern möchten, müssen Sie die App von Ihrem Computer entfernen.

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 das Abo

Ein Abonnement für Kaspersky Endpoint Security ist ein Auftrag, nach dem das Programm mit bestimmten Einstellungen (Abo-Laufzeit, Anzahl der geschützten Geräte) genutzt werden kann. Ein Abo für Kaspersky Endpoint Security kann bei einem Provider registriert werden (z. B. bei einem Internet-Provider). Das Abo kann manuell oder automatisch verlängert oder auch gekündigt werden. Das Abonnement kann auf der Webseite des Dienstanbieters verwaltet werden.

Es gibt beschränkte (z. B. auf ein Jahr) und unbefristete (ohne Ablaufdatum) Abos. Um Kaspersky Endpoint Security weiterhin zu nutzen, müssen Sie ein beschränktes Abonnement rechtzeitig verlängern. Ein unbefristetes Abo wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Provider überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abo-Verlängerung gewährt, während der die Programmfunktionalität erhalten bleibt. Das Angebot und die Dauer einer Nachfrist sind vom Dienstanbieter abhängig.

Um Kaspersky Endpoint Security im Rahmen eines Abonnements zu nutzen, müssen Sie den Aktivierungscode anwenden, den Sie vom Dienstanbieter erhalten haben. Nachdem der Aktivierungscode angewendet wurde, wird der aktive Schlüssel hinzugefügt. Der aktive Schlüssel bestimmt die Lizenz für die Verwendung des Programms im Rahmen des Abonnements. Im Rahmen eines Abonnements können Sie das Programm nicht mit einer Schlüsseldatei aktivieren. Der Dienstanbieter kann nur einen Aktivierungscode zur Verfügung stellen. Im Rahmen eines Abonnements kann kein Reserveschlüssel hinzugefügt werden.

Auf Grundlage eines Abos erworbene Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Endpoint Security genutzt werden.

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.

Für Schlüssel, die im Rahmen eines Abonnements hinzugefügt werden, gibt es kein Lizenzzertifikat.

Einen Lizenzschlüssel können Sie zur App hinzufügen, indem Sie eine Schlüsseldatei anwenden oder einen Aktivierungscode eingeben.

Kaspersky kann einen Schlüssel blockieren, wenn die Bedingungen des Lizenzvertrags verletzt werden. Wenn ein Schlüssel gesperrt ist, müssen Sie einen anderen Schlüssel hinzufügen, damit das Programm funktioniert.

Ein Schlüssel kann entweder ein aktiver Schlüssel oder ein Reserveschlüssel sein.

Ein *aktiver Schlüssel* ist ein Schlüssel, der momentan für das Programm verwendet wird. Als aktiver Schlüssel kann entweder ein Schlüssel für eine Testlizenz oder für eine kommerzielle Lizenz hinzugefügt werden. Im Programm kann es nur einen aktiven Schlüssel geben.

Ein *Reserveschlüssel* gewährt das Recht auf die Programmnutzung, wird aber momentan nicht verwendet. Nach Ablauf des aktiven Schlüssels wird automatisch der Reserveschlüssel aktiviert. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn ein aktiver Schlüssel vorhanden ist.

Ein Schlüssel für eine Testlizenz kann nur als aktiver Schlüssel hinzugefügt werden. Er kann nicht als Reserveschlüssel hinzugefügt werden. Ein aktiver Schlüssel kann nicht durch einen Schlüssel für eine Testlizenz ersetzt werden.

Wenn ein Schlüssel zur Liste der verbotenen Schlüssel hinzugefügt wird, bleibt der Funktionsumfang des Programms, der durch die zur Aktivierung des Programms verwendete Lizenz definiert ist, acht Tage lang verfügbar. Das Programm benachrichtigt den Benutzer, dass der Schlüssel zur Liste der verbotenen Schlüssel hinzugefügt wurde. Nach Ablauf von acht Tagen entspricht die Programmfunktionalität jener Situation, in der die Lizenz abgelaufen ist. Sie können die Schutz- und Kontrollkomponenten verwenden und eine Untersuchung ausführen. Dabei werden die Programm-Datenbanken verwendet, die bei Ablauf der Lizenz installiert waren. Außerdem verschlüsselt das Programm weiterhin Dateien, die geändert werden und vor Ablauf der Lizenz verschlüsselt worden sind. Neue Dateien werden aber nicht mehr verschlüsselt. Kaspersky Security Network kann nicht genutzt 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 Ihre angegebene E-Mail-Adresse gesendet, nachdem Sie Kaspersky Endpoint Security gekauft haben.

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, ist für den Zugriff auf die Kaspersky-Aktivierungsserver eine Internetverbindung erforderlich.

Wenn das Programm mithilfe eines Aktivierungscodes aktiviert wird, wird ein aktiver Schlüssel hinzugefügt. Ein Reserveschlüssel kann nur mithilfe eines Aktivierungscodes hinzugefügt werden, nicht mithilfe einer Schlüsseldatei.

Wenn ein Aktivierungscode nach der Programmaktivierung verloren geht, können Sie den Aktivierungscode wiederherstellen. Der Aktivierungscode kann beispielsweise für die Registrierung bei Kaspersky CompanyAccount erforderlich sein. Falls Sie den Aktivierungscode nach der Programmaktivierung verlieren, wenden Sie sich an den Kaspersky-Partner, bei dem Sie die Lizenz gekauft 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 das Programm mithilfe einer Schlüsseldatei zu aktivieren, ist kein Zugriff auf die Kaspersky-Aktivierungsserver erforderlich.

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

Es bestehen folgende Möglichkeiten, um eine Schlüsseldatei wiederherzustellen:

- Kontaktaufnahme mit dem Verkäufer.
- Auf der Kaspersky-Website mithilfe des vorhandenen Aktivierungscodes eine Schlüsseldatei anfordern.
- Eine Schlüsseldatei von einem anderen Administrationsserver abrufen.

Wenn das Programm mithilfe einer Schlüsseldatei aktiviert wird, wird ein aktiver Schlüssel hinzugefügt. Ein Reserveschlüssel kann nur mithilfe einer Schlüsseldatei hinzugefügt werden, nicht mithilfe eines Aktivierungscodes.

Vergleich der Programmfunktionalität abhängig vom Lizenztyp für Arbeitsstationen

Der auf Arbeitsstationen verfügbare Funktionsumfang von Kaspersky Endpoint Security ist vom Lizenztyp abhängig (s. Tabelle unten).

Beachten Sie auch den Vergleich der Programmfunktionalität für Server.

Einen Vergleich der Programmfunktionalität unter Berücksichtigung des Kaspersky Next-Lizenztyps finden Sie in der Hilfe zu Kaspersky Next.

Vergleich der Funktionen von Kaspersky Endpoint Security

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Erweiterter Schutz								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Verhaltensanalyse	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Verschlüsselung	✓	✓	✓	✓	✓	✓	✓	✓
Exploit-Prävention	✓	✓	✓	✓	✓	✓	✓	✓
Programm-Überwachung	✓	✓	✓	✓	✓	✓	✓	✓
Rollback von schädlichen Aktionen	✓	✓	✓	✓	✓	✓	✓	✓
Basisschutz								
Schutz vor bedrohlichen Dateien	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Web-Bedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor BadUSB-Angriffen	✓	✓	✓	✓	✓	✓	✓	✓
AMSI-Schutz	✓	✓	✓	✓	✓	✓	✓	✓
Sicherheitskontrolle								
Protokollanalyse	–	–	–	–	–	–	–	–
Programmkontrolle	✓	✓	✓	✓	✓	✓	✓	✓
Gerätekontrolle	✓	✓	✓	✓	✓	✓	✓	✓
Web-Kontrolle	✓	✓	✓	✓	✓	✓	✓	✓
Adaptive Kontrolle von Anomalien	–	✓	✓	✓	✓	✓	–	✓

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Überwachung der Systemintegrität	–	–	–	–	–	–	–	–
Virtuelle Datentresore								
Kaspersky-Festplattenverschlüsselung	–	✓	✓	✓	✓	✓	–	✓
BitLocker-Laufwerkverschlüsselung	–	✓	✓	✓	✓	✓	–	✓
Verschlüsselung von Dateien	–	✓	✓	✓	✓	✓	–	✓
Wechseldatenträger verschlüsseln	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–
Kaspersky Sandbox *(Eine Lizenz für „Kaspersky Sandbox" muss separat gekauft werden.)*	✓	✓	✓	✓	✓	✓	✓	✓
Integration mit KUMA *(Lizenz für die KUMA-Integration muss separat erworben werden)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent-Modus *(um das Programm zu aktivieren, müssen Sie der SVM, mit der der Light Agent verbunden ist, einen Lizenzschlüssel hinzufügen)*	–	–	–	–	–	–	✓	✓

Vergleich der Programmfunktionalität abhängig vom Lizenztyp für Server

Der auf Servern verfügbare Funktionsumfang von Kaspersky Endpoint Security ist vom Lizenztyp abhängig (s. Tabelle unten).

Beachten Sie auch den Vergleich der Programmfunktionalität für Arbeitsstationen.

Einen Vergleich der Programmfunktionalität unter Berücksichtigung des Kaspersky Next-Lizenztyps finden Sie in der Hilfe zu Kaspersky Next.

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Erweiterter Schutz								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
Verhaltensanalyse	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Verschlüsselung	✓	✓	✓	✓	✓	✓	✓	✓
Exploit-Prävention	✓	✓	✓	✓	✓	✓	✓	✓
Programm-Überwachung	–	–	–	–	–	–	–	–
Rollback von schädlichen Aktionen	✓	✓	✓	✓	✓	✓	✓	✓
Basisschutz								
Schutz vor bedrohlichen Dateien	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Web-Bedrohungen	–	✓	✓	✓	✓	✓	✓	✓
Schutz vor E-Mail-Bedrohungen	–	✓	✓	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor Netzwerkbedrohungen	✓	✓	✓	✓	✓	✓	✓	✓
Schutz vor BadUSB-Angriffen	✓	✓	✓	✓	✓	✓	✓	✓
AMSI-Schutz	✓	✓	✓	✓	✓	✓	✓	✓
Sicherheitskontrolle								
Protokollanalyse	–	–	–	–	–	–	–	✓
Programmkontrolle	–	✓	✓	✓	✓	✓	–	✓
Gerätekontrolle	–	✓	✓	✓	✓	✓	✓	✓
Web-Kontrolle	–	✓	✓	✓	✓	✓	✓	✓
Adaptive Kontrolle von Anomalien	–	–	–	–	–	–	–	–
Überwachung der Systemintegrität	–	–	–	–	–	–	–	✓
Virtuelle Datentresore								
Kaspersky-Festplattenverschlüsselung	–	–	–	–	–	–	–	–
BitLocker-Laufwerkverschlüsselung	–	✓	✓	✓	✓	✓	–	✓
Verschlüsselung auf Dateiebene	–	–	–	–	–	–	–	–
Wechseldatenträger verschlüsseln	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓	–	–

Funktion	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
Kaspersky Sandbox *(Eine Lizenz für „Kaspersky Sandbox" muss separat gekauft werden.)*	✓	✓	✓	✓	✓	✓	✓	✓
Integration mit KUMA *(Lizenz für die KUMA-Integration muss separat erworben werden)*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent-Modus *(um das Programm zu aktivieren, müssen Sie der SVM, mit der der Light Agent verbunden ist, einen Lizenzschlüssel hinzufügen)*	–	–	–	–	–	–	✓	✓

Programm aktivieren

Durch die *Aktivierung* erlangt die Lizenz, die zur Nutzung der Premiumversion des Programms berechtigt, ihre Gültigkeit für den entsprechenden Zeitraum. Beim Aktivierungsvorgang des Programms wird ein Lizenzschlüssel hinzugefügt.

Sie können das Programm auf eine der folgenden Weisen aktivieren:

- Lokal über die Benutzeroberfläche mithilfe des Aktivierungs-Assistenten. Auf diese Weise können Sie einen aktiven Schlüssel und einen Reserveschlüssel hinzufügen.
- Per Fernzugriff über die Software-Suite Kaspersky Security Center.
  - Mithilfe der Aufgabe *Schlüssel hinzufügen*.

    Auf diese Weise kann der Schlüssel auf einem konkreten Computer oder auf den Computern, die zu einer Administrationsgruppe gehören, hinzugefügt werden. Auf diese Weise können Sie einen aktiven Schlüssel und einen Reserveschlüssel hinzufügen.
  - Durch die Verteilung eines Schlüssels, der sich auf dem Administrationsserver für Kaspersky Security Center befindet, an die Computer.

    Mit dieser Methode kann ein Schlüssel automatisch auf bereits mit Kaspersky Security Center verbundenen Computern und auf neuen Computern hinzugefügt werden. Um diese Methode zu verwenden, müssen Sie zuerst einen Schlüssel zum Kaspersky Security Center Administrationsserver hinzufügen. Nähere Informationen über das Hinzufügen von Schlüsseln zum Kaspersky Security Center Administrationsserver finden Sie in der Hilfe zu Kaspersky Security Center.

    Ein Aktivierungscode, der mit einem Abo erworben wurde, wird zuerst verteilt.

- Durch Hinzufügen des Schlüssels zum Installationspaket für Kaspersky Endpoint Security.

  Mit dieser Methode können Sie während der Bereitstellung von Kaspersky Endpoint Security den Schlüssel in den Eigenschaften des Installationspakets hinzufügen. Das Programm wird nach der Installation automatisch aktiviert.

- Mithilfe der Befehlszeile.

Wenn das Programm ferngesteuert oder bei der Programminstallation im Silent-Modus mit einem Aktivierungscode aktiviert wird, kann es aufgrund der Auslastung der Kaspersky-Aktivierungsserver zu Verzögerungen kommen. Sollte eine sofortige Programmaktivierung notwendig sein, so können Sie die laufende Aktivierung abbrechen und das Programm mithilfe des Aktivierungs-Assistenten aktivieren.

Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz von virtuellen Umgebungen verwendet wird, müssen Sie das Programm nicht separat aktivieren.

Programm aktivieren

Aktivieren des Programms in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Schlüssel hinzufügen** aus.

Schritt 2. Schlüssel hinzufügen

Geben Sie einen Aktivierungscode ein oder wählen Sie eine Schlüsseldatei aus.

Weitere Informationen über das Hinzufügen von Schlüsseln zur Datenverwaltung von Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 5. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, beispielsweise *Aktivierung von Kaspersky Endpoint Security für Windows*.

Schritt 6. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch wird auf den Benutzercomputern das Programm Kaspersky Endpoint Security im unbeaufsichtigten Modus aktiviert.

Aktivieren des Programms in „Web Console“ und „Cloud Console”

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Schlüssel hinzufügen**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Aktivierung von Kaspersky Endpoint Security für Windows*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus. Weiter zum nächsten Schritt

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Lizenz auswählen

Wählen Sie eine Lizenz aus, mit der Sie das Programm aktivieren möchten. Weiter zum nächsten Schritt

Sie können Schlüssel zur Web Console hinzufügen (**Vorgänge** → **Lizenzierung**).

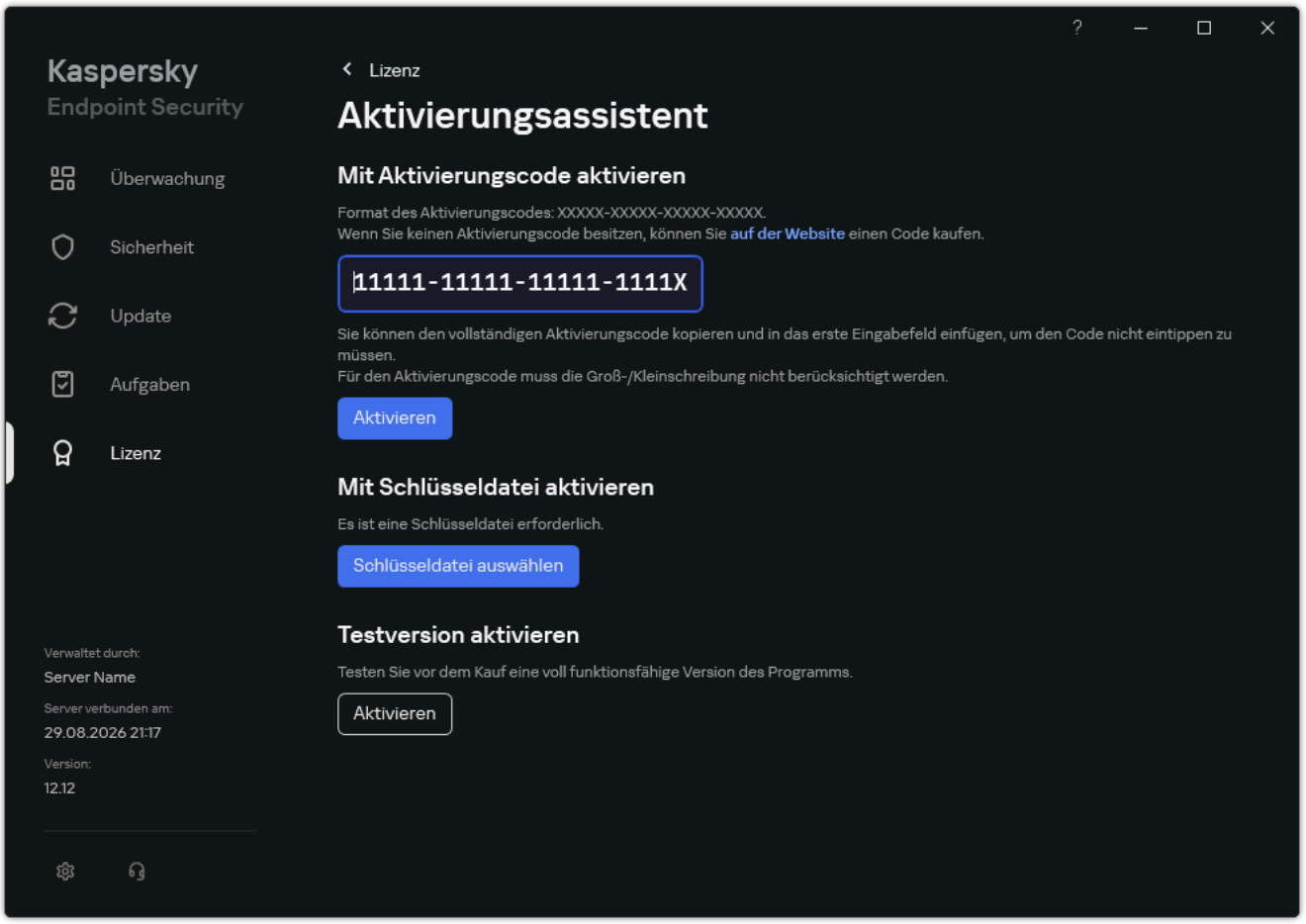
Schritt 4. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertigstellen**. Die neue Aufgabe wird in der Aufgabenliste angezeigt. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**, um die Aufgabe auszuführen. Dadurch wird auf den Benutzercomputern das Programm Kaspersky Endpoint Security im unbeaufsichtigten Modus aktiviert.

So aktivieren Sie die Anwendung über die Benutzeroberfläche

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Lizenz**.
2. Klicken Sie auf **Das Programm mit einer neuen Lizenz aktivieren**.

   Der Aktivierungsassistent für das Programm wird gestartet. Folgen Sie den Anweisungen des Aktivierungsassistenten.



Programm aktivieren

In den Eigenschaften der Aufgabe *Schlüssel hinzufügen* können Sie auf dem Computer einen Reserveschlüssel hinzufügen. Ein *Reserveschlüssel* wird aktiviert, wenn der aktive Schlüssel abläuft. Mit einem Reserveschlüssel lässt sich verhindern, dass die Programmfunktionalität beim Ablauf der Lizenz beschränkt wird.

Automatisches Hinzufügen eines Lizenzschlüssels für Computer über die Verwaltungskonsole (MMC)

1. Gehen Sie in der Verwaltungskonsole zum Ordner **Lizenzen für Kaspersky-Software**.

   Die Liste der Lizenzschlüssel wird geöffnet.
2. Öffnen Sie die Eigenschaften des Lizenzschlüssels.
3. Aktivieren Sie im Abschnitt **Allgemein** das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.
4. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird der Schlüssel automatisch an die passenden Computer verteilt. Wenn ein Schlüssel automatisch als aktiver Schlüssel oder als Reserveschlüssel verteilt wird, wird die Lizenzbeschränkung für die Anzahl der Computer berücksichtigt. Diese Beschränkung ist in den Schlüsseleigenschaften angegeben. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Schlüssels an die Computer automatisch beendet. Die Anzahl der Computer, auf denen der Schlüssel hinzugefügt wurde, sowie andere Daten können in den Schlüsseleigenschaften im Abschnitt **Geräte** eingesehen werden.

Automatisches Hinzufügen eines Lizenzschlüssels über „Web Console“ und „Cloud Console”

1. Klicken Sie im Web Console-Hauptfenster auf **Vorgänge** → **Lizenzierung** → **Lizenzen**.

   Die Liste der Lizenzschlüssel wird geöffnet.

2. Öffnen Sie die Eigenschaften des Lizenzschlüssels.

3. Aktivieren Sie auf der Registerkarte **Allgemein** den Schalter **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

4. Speichern Sie die vorgenommenen Änderungen.

   Dadurch wird der Schlüssel automatisch an die passenden Computer verteilt. Wenn ein Schlüssel automatisch als aktiver Schlüssel oder als Reserveschlüssel verteilt wird, wird die Lizenzbeschränkung für die Anzahl der Computer berücksichtigt. Diese Beschränkung ist in den Schlüsseleigenschaften angegeben. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Schlüssels an die Computer automatisch beendet. Die Anzahl der Computer, auf denen der Schlüssel hinzugefügt wurde, sowie andere Daten können in den Schlüsseleigenschaften auf der Registerkarte **Geräte** eingesehen werden.

Wenn Sie die App mithilfe eines *Aktivierungscodes* aktivieren, ist für die Verbindung zu den Kaspersky-Aktivierungsservern ein Internetzugang erforderlich. Wenn Sie die App mit einer *Schlüsseldatei* aktivieren, ist kein Internetzugang erforderlich. Wenn sich die Computer in einem isolierten Netzwerksegment ohne Internetzugang befinden und die App mithilfe eines Codes aktiviert werden soll, müssen Sie die Verwendung des Kaspersky Security Center-Administrationsservers als Proxyserver erlauben. Dann kann die App über den Administrationsserver mit Internetzugang auf die Aktivierungsserver zugreifen.

So erlauben Sie in der Verwaltungskonsole (MMC), dass der Administrationsserver als Proxyserver für die App-Aktivierung verwendet werden darf

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Programmeinstellungen** aus.

4. Aktivieren Sie das Kontrollkästchen **Kaspersky Security Center als Proxyserver für die Aktivierung verwenden**.

5. Speichern Sie die vorgenommenen Änderungen.

So erlauben Sie in der Web Console und Cloud Console, dass der Administrationsserver als Proxyserver für die App-Aktivierung verwendet werden darf

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **KSC-Integration**.

5. Aktivieren Sie das Kontrollkästchen **Kaspersky Security Center als Proxyserver für die Aktivierung verwenden**.

6. Speichern Sie die vorgenommenen Änderungen.

Wenn Sie die App nicht mit einem *Aktivierungscode* aktivieren können, versuchen Sie, über die Kaspersky-Lösung eine *Schlüsseldatei* anzufordern und die App mit einer anderen Methode zu aktivieren.

Überwachung der Lizenznutzung

Es gibt folgende Möglichkeiten, um die Verwendung von Lizenzen zu kontrollieren:

- Öffnen Sie den *Bericht über die Lizenzschlüsselnutzung* für die Infrastruktur des Unternehmens (**Überwachung** → **Berichte**).
- Status der Computer auf der Registerkarte **Verwaltete Geräte** → **Geräte** anzeigen. Wenn das Programm nicht aktiviert ist, hat der Computer den Status ⚠ *Das Programm ist nicht aktiviert*.
- Informationen über die Lizenz in den Computereigenschaften anzeigen.
- Die wichtigsten Eigenschaften anzeigen (**Vorgänge** → **Lizenzierung**).

Besonderheiten bei der Aktivierung der Anwendung als Teil von Kaspersky Security Center Cloud Console

Für Kaspersky Security Center Cloud Console ist eine Testversion vorgesehen. Die *Testversion* ist eine spezielle Version von Kaspersky Security Center Cloud Console. Sie dient dazu, die Funktionen von Kaspersky Security Center Cloud Console kennenzulernen. In dieser Version können Sie einen Arbeitsbereich für einen Zeitraum von 30 Tagen verwenden. Im Rahmen der Testlizenz für Kaspersky Security Center Cloud Console werden alle verwalteten Programme automatisch ausgeführt, einschließlich Kaspersky Endpoint Security. Nachdem die Testlizenz für Kaspersky Security Center Cloud Console abläuft, kann Kaspersky Endpoint Security nicht im Rahmen einer eigenen Testlizenz aktiviert werden. Details über die Lizenzverwaltung von Kaspersky Security Center finden Sie in der Hilfe zu „Kaspersky Security Center Cloud Console“.

> Die Testversion von Kaspersky Security Center Cloud Console erlaubt es nicht, anschließend zur kommerziellen Version zu wechseln. Ein beliebiger Test-Arbeitsbereich wird mit seinem gesamten Inhalt nach Ablauf von 30 Tagen gelöscht.

Einen Lizenzschlüssels entfernen

Um einen Lizenzschlüssel zu entfernen, müssen Sie auf Ihren Computern eine spezielle Aufgabe ausführen. Sie können einen Lizenzschlüssel entfernen, beispielsweise um die verfügbaren Lizenzen neu zu organisieren. Wenn die Lizenz abläuft, werden Sie von Kaspersky Endpoint Security benachrichtigt. Wenn Sie einen Lizenzschlüssel hinzugefügt haben, mit dem Sie das Programm für einen kurzen Zeitraum testen können (z. B. EDR Optimum-Add-on), können Sie diesen Lizenzschlüssel entfernen, um Benachrichtigungen zu löschen und den Status Ihres Computers zu korrigieren.

Mit der Aufgabe *Schlüssel löschen* können Sie beliebige Lizenzschlüssel vom Computer entfernen. Sie können sowohl aktive Lizenzschlüssel als auch Reserve-Lizenzschlüssel entfernen. Neben dem Lizenzschlüssel zur Aktivierung von Kaspersky Endpoint Security können Sie einzelne Lizenzschlüssel von Kaspersky Detection and Response-Lösungen entfernen (z. B. EDR Optimum-Add-on).

So entfernen Sie einen Lizenzschlüssel in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Schlüssel löschen** aus.

Schritt 2. Lizenz auswählen

Wählen Sie den Lizenzschlüssel aus, den Sie löschen möchten. Sie können einen Lizenzschlüssel aus dem Kaspersky Security Center-Schlüsselspeicher oder eine Schlüsseldatei auswählen.

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder bei Computerleerlauf.

Schritt 5. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, z. B. *Schlüssel für Beta entfernen*.

Schritt 6. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So entfernen Sie einen Lizenzschlüssel in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Schlüssel löschen**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Schlüssel für Beta entfernen*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus. Weiter zum nächsten Schritt

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Lizenz auswählen

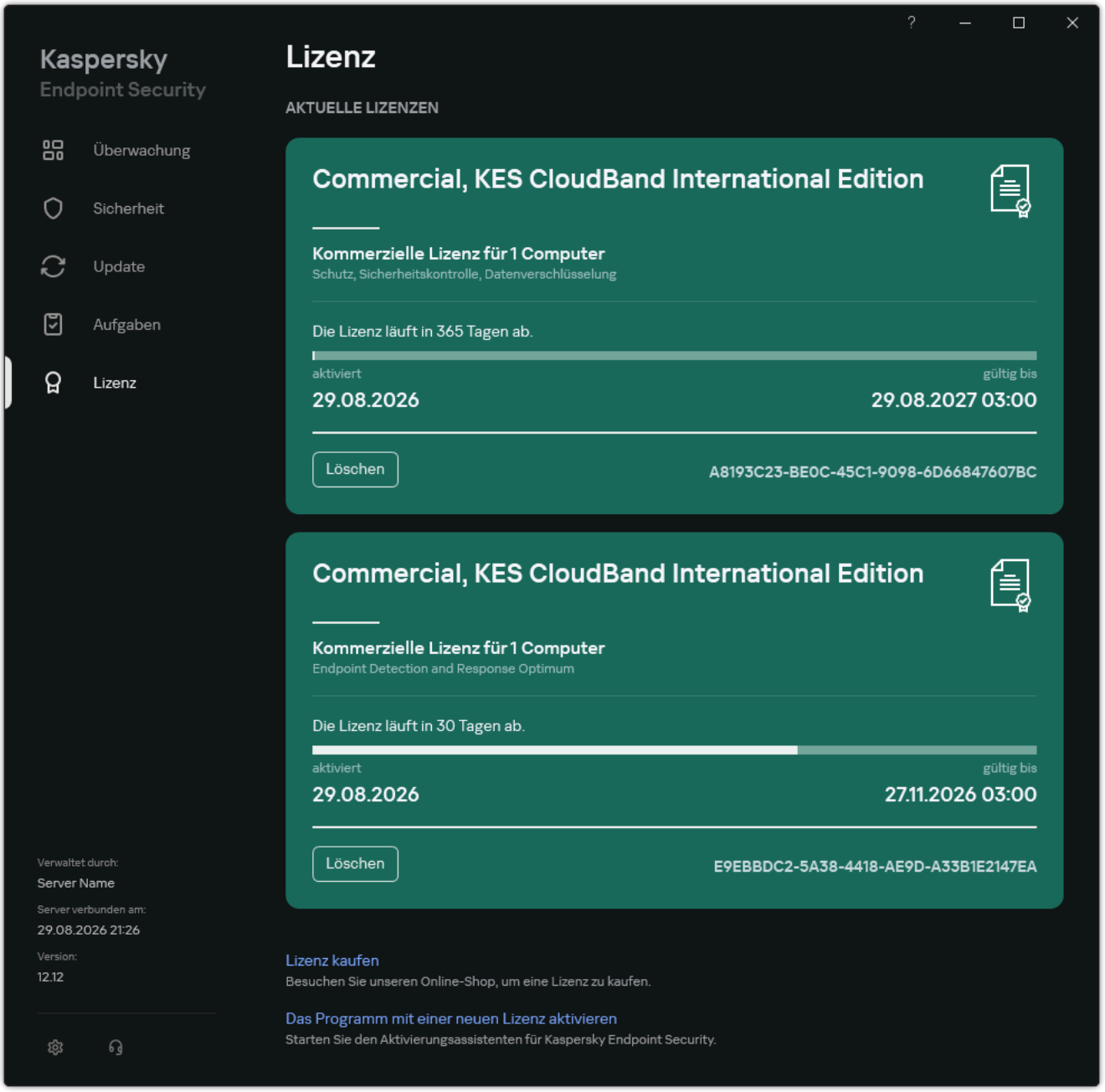
Wählen Sie den Lizenzschlüssel aus, den Sie löschen möchten. Sie können einen Lizenzschlüssel aus dem Kaspersky Security Center-Schlüsselspeicher oder eine Schlüsseldatei auswählen. Weiter zum nächsten Schritt

Schritt 4. Erstellung der Aufgabe abschließen

Beenden Sie den Assistenten durch Klick auf **Fertigstellen**. Die neue Aufgabe wird in der Aufgabenliste angezeigt. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**, um die Aufgabe auszuführen.

So entfernen Sie einen Lizenzschlüssel in der Programmoberfläche

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Lizenz**.
2. Wählen Sie den Schlüssel aus, den Sie löschen möchten, und klicken Sie auf **Löschen**.



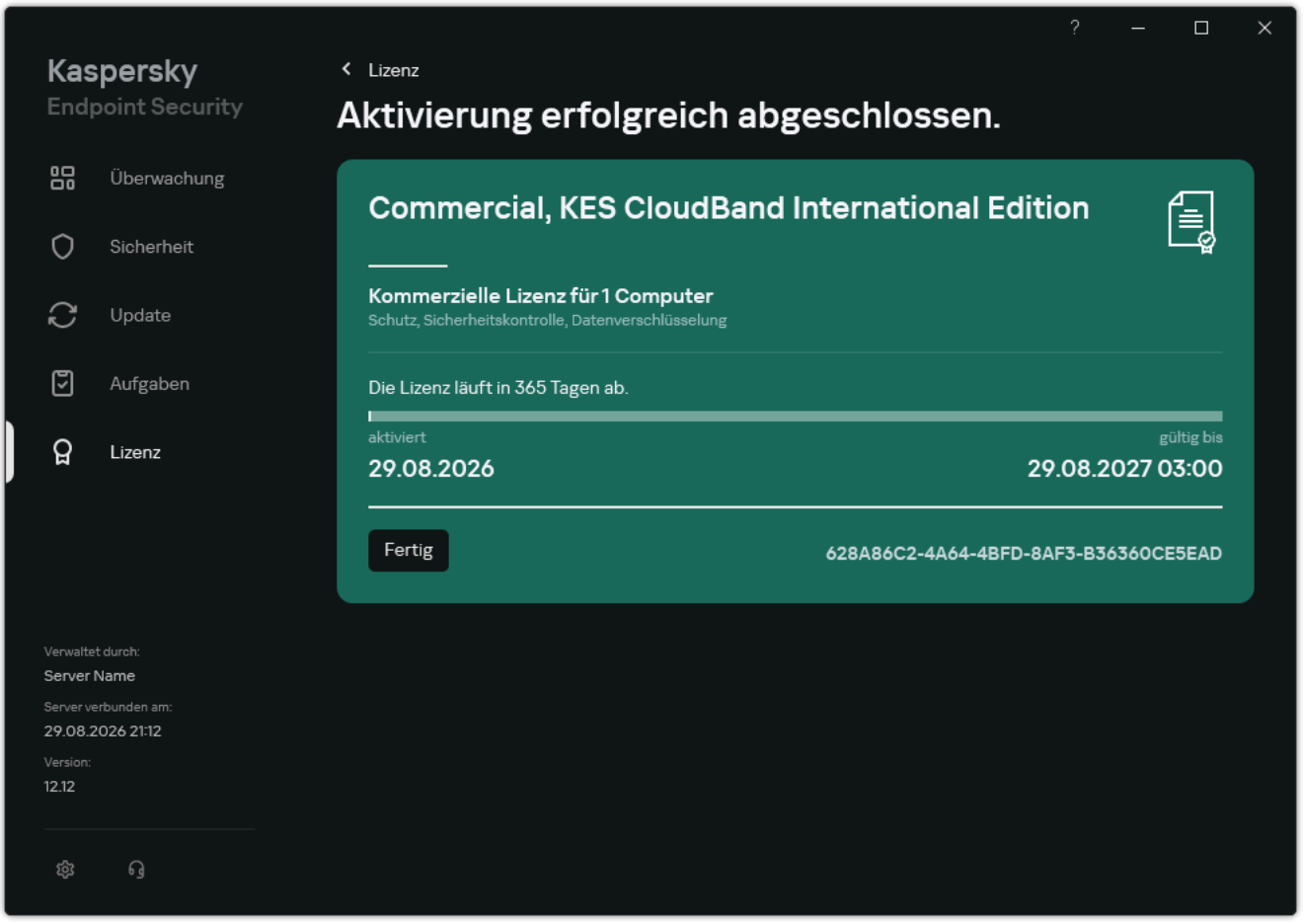
Fenster Lizenzverwaltung

Sie können einen Lizenzschlüssel auch über die Befehlszeile entfernen.

Lizenz-Info anzeigen

Um Informationen über die Lizenz anzuzeigen,

Gehen Sie im Programmhauptfenster zum Abschnitt **Lizenz** (siehe Bild unten).



Fenster Lizenzverwaltung

Dieser Abschnitt enthält die folgenden Details:

- *Status des Schlüssels*. Auf dem Computer können mehrere Schlüssel vorhanden sein. Ein Schlüssel kann entweder ein aktiver Schlüssel oder ein Reserveschlüssel sein. Im Programm kann es nur einen aktiven Schlüssel geben. Ein Reserveschlüssel kann erst zum aktiven Schlüssel werden, nachdem der aktive Schlüssel abläuft oder nachdem der aktive Schlüssel durch Klick auf **Löschen** gelöscht wurde.

- *Programmname*. Vollständiger Name des erworbenen Kaspersky-Programm.

- *Lizenztyp*. Es sind folgende Lizenztypen vorgesehen: Test und kommerziell.

- *Funktionalität*. Programmfunktionen, die im Rahmen Ihrer Lizenz verfügbar sind. Es sind die folgenden Funktionen vorgesehen: Schutz, Sicherheitskontrolle, Datenverschlüsselung und andere. Eine Liste der verfügbaren Funktionen ist auch im Lizenzzertifikat verfügbar.

- *Zusatzinformationen über die Lizenz*. Startdatum und Enddatum der Gültigkeitsdauer der Lizenz (nur für den aktiven Schlüssel), verbleibende Gültigkeitsdauer der Lizenz.

  Die Uhrzeit für den Ablauf der Gültigkeitsdauer der Lizenz wird in der Zeitzone angezeigt, die im Betriebssystem festgelegt ist.

- *Schlüssel*. Ein Schlüssel ist eine einmalige alphanumerische Zeichenfolge, die auf einem Aktivierungscode oder einer Schlüsseldatei basiert.

Im Fenster der Lizenzverwaltung sind außerdem die folgenden Aktionen verfügbar:

- **Lizenz kaufen** / **Lizenz verlängern**. Öffnet die Website des Online-Shops von Kaspersky. Dort können Sie eine Lizenz kaufen oder die Gültigkeitsdauer der Lizenz verlängern. Dazu müssen Sie die Daten Ihres Unternehmens eingeben und den Auftrag bezahlen.

- **Das Programm mit einer neuen Lizenz aktivieren**. Startet den Aktivierungsassistenten für das Programm. Der Assistent ermöglicht es, einen Schlüssel mithilfe des Aktivierungscodes oder der Schlüsseldatei hinzuzufügen. Mithilfe des Assistenten zur Programmaktivierung können ein aktiver Schlüssel und ein einziger Reserveschlüssel hinzugefügt werden.

Lizenz kaufen

Sie können die Lizenz auch nach der Installation des Programms erwerben. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode oder eine Schlüsseldatei, um das Programm zu aktivieren.

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Lizenz**.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wenn keine Schlüssel hinzugefügt wurden oder nur ein Schlüssel für eine Testlizenz hinzugefügt wurde, klicken Sie auf **Lizenz kaufen**.

   - Klicken Sie auf die Schaltfläche **Lizenz verlängern**, wenn ein Schlüssel für die kommerzielle Lizenz hinzugefügt wurde.

   Die Website des Kaspersky-Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

Abo verlängern

Wenn das Programm im Abo genutzt wird, greift Kaspersky Endpoint Security bis zum Ablauf des Abos in bestimmten Zeitabständen automatisch auf den Aktivierungsserver zu.

Wenn Sie das Programm mit einem unbefristeten Abo nutzen, überprüft Kaspersky Endpoint Security im Hintergrundmodus automatisch, ob auf dem Aktivierungsserver ein aktualisierter Schlüssel vorliegt. Wenn auf dem Aktivierungsserver ein Schlüssel liegt, ersetzt das Programm den vorherigen Schlüssel durch den neuen. Ein unbefristetes Abo für Kaspersky Endpoint Security wird ohne Ihr Eingreifen verlängert.

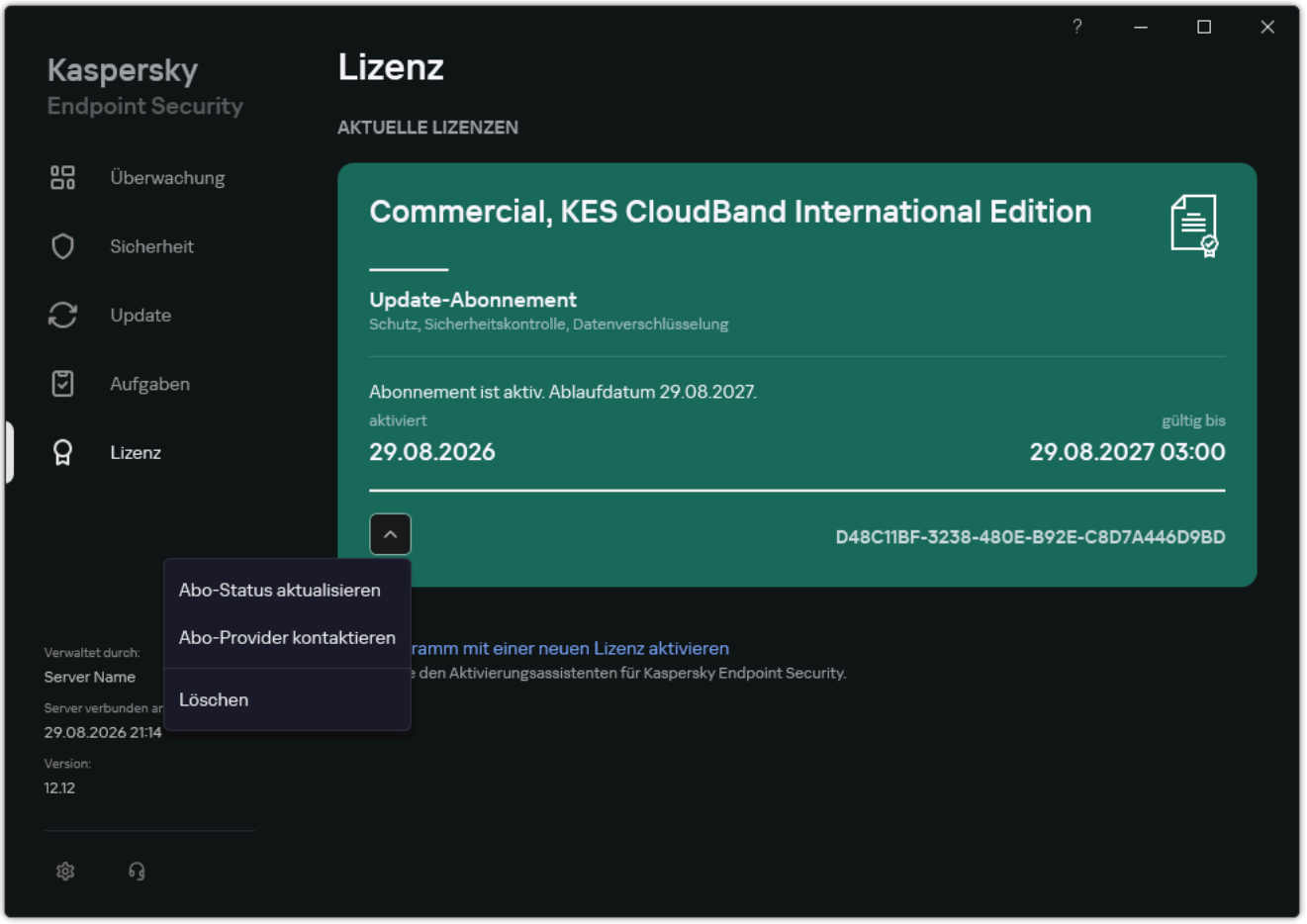
Wenn Sie das Programm im Rahmen eines befristeten Abonnements nutzen, werden Sie an dem Tag, an dem das Abonnement oder die Nachfrist für die Abo-Verlängerung nach dem Ablauf des Abonnements endet, von Kaspersky Endpoint Security darüber informiert und die Versuche zur automatischen Abo-Verlängerung werden eingestellt. Hierbei verhält sich Kaspersky Endpoint Security genau so wie nach dem Ablauf einer kommerziellen Lizenz für die Programmnutzung, d. h. das Programm funktioniert weiterhin, wird aber nicht mehr aktualisiert und kann nicht auf Kaspersky Security Network zugreifen.

Sie können das Abonnement auf der Website des Dienstanbieters verlängern.

Um von der Programmoberfläche aus auf die Provider-Webseite zu gelangen, gehen Sie wie folgt vor:

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Lizenz**.
2. Klicken Sie auf **Abo-Provider kontaktieren**.

Sie können den Abonnementstatus manuell aktualisieren. Dies kann erforderlich sein, wenn das Abonnement nach Ablauf der Nachfrist verlängert wurde und das Programm den Abo-Status nicht automatisch aktualisiert.



Abo verlängern

Erste Schritte

Nach der Installation von Kaspersky Endpoint Security können Sie das Programm mithilfe der folgenden Schnittstellen verwalten:

- Lokale Programmoberfläche.
- Kaspersky Security Center Verwaltungskonsole.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Verwaltungskonsole

Mit Kaspersky Security Center können folgende Funktionen ferngesteuert werden: Kaspersky Endpoint Security installieren und entfernen, starten und beenden; Programmeinstellungen anpassen, Auswahl der Programmkomponenten ändern, Schlüssel hinzufügen, Update- und Untersuchungsaufgaben starten und beenden.

Das Programm Kaspersky Security Center wird mithilfe des Verwaltungs-Plug-ins von Kaspersky Endpoint Security verwaltet.

Weitere Informationen zur Verwaltung des Programms über Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

„Kaspersky Security Center Web Console“ und „Kaspersky Security Center Cloud Console“

Kaspersky Security Center Web Console (im Folgenden auch *Web Console* genannt). Dabei handelt es sich um eine Webschnittstelle zur Verwaltung eines Schutzsystems auf der Basis von Kaspersky-Anwendungen. Sie können in Kaspersky Security Center Web Console über einen Browser auf einem beliebigen Gerät arbeiten. Ausführliche Informationen zu „Kaspersky Security Center Web Console“ finden Sie in der Hilfe zu Kaspersky Security Center.

Kaspersky Security Center Cloud Console (im Folgenden „*Cloud Console*“) ist eine Cloud-Lösung für den Schutz und die Kontrolle eines Unternehmensnetzwerks. Ausführliche Informationen über Kaspersky Security Center Cloud Console finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console.

Mithilfe von Web Console und Cloud Console können Sie die folgenden Aktionen ausführen:

- Status des Sicherheitssystems Ihres Unternehmens kontrollieren
- Kaspersky-Programme auf den Geräten Ihres Netzwerks installieren
- Installierte Programme verwalten
- Berichte über den Zustand des Sicherheitssystems einsehen

Die Verwaltung des Programms Kaspersky Endpoint Security über Web Console, Cloud Console und über die Verwaltungskonsole von Kaspersky Security Center weist Unterschiede auf. Auch die jeweilige Liste der verfügbaren Komponenten und Aufgaben unterscheidet sich.

Über das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows

Das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows gewährleistet die Interaktion von Kaspersky Endpoint Security mit Kaspersky Security Center. Mithilfe des Verwaltungs-Plug-ins kann Kaspersky Endpoint Security für Windows unter Verwendung der folgenden Tools verwaltet werden: Richtlinien, Aufgaben und lokale Programmeinstellungen. Für die Interaktion mit „Kaspersky Security Center Web Console“ ist ein Web-Plug-in vorgesehen.

Die Version des Verwaltungs-Plug-ins kann sich von der Version des Programms Kaspersky Endpoint Security unterscheiden, die auf dem Client-Computer installiert ist. Verfügt die installierte Version des Verwaltungs-Plug-ins über weniger Funktionen als die installierte Version von Kaspersky Endpoint Security, so werden die fehlenden Funktionen nicht mit dem Verwaltungs-Plug-in verwaltet. Diese Einstellungen können vom Benutzer in der lokalen Oberfläche von Kaspersky Endpoint Security geändert werden.

Das Web-Plug-in ist nicht standardmäßig in „Kaspersky Security Center Web Console“ installiert. Das Web-Plug-in muss auf einem Computer installiert werden, auf dem Kaspersky Security Center Web Console installiert ist. Dabei sind die Funktionen des Web-Plug-ins für alle Administratoren verfügbar, die Zugriff auf „Web Console“ im Browser haben. Die Liste der installierten Web-Plug-ins können Sie in der Web Console-Benutzeroberfläche einsehen (**Konsolen-Einstellungen** → **Web-Plug-ins**).

Wenn Sie Kaspersky Endpoint Security als Teil der Lösung Kaspersky Endpoint Detection and Response Optimum verwenden, müssen Sie das Verwaltungs-Plug-in von Kaspersky Endpoint Detection and Response installieren. Sie benötigen das Verwaltungs-Plug-in, um Alarm-Details anzuzeigen. *Alarm-Details* ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Um Aufgaben zur Reaktion auf Bedrohungen zu erstellen, benötigen Sie daher das Verwaltungs-Plug-in von Kaspersky Endpoint Security, und um Alarm-Details anzuzeigen, benötigen Sie das Verwaltungs-Plug-in für EDR.

Installation des Web-Plug-ins

Es gibt folgende Möglichkeiten, um das Web-Plug-in zu installieren:

- Installieren des Web-Plug-ins mithilfe des Schnellstartassistenten für „Kaspersky Security Center Web Console“.

  „Web Console“ schlägt bei der ersten Verbindung von „Web Console“ mit dem Administrationsserver automatisch vor, den Schnellstartassistenten zu starten. Den Schnellstartassistenten können Sie auch über die Web Console-Benutzeroberfläche ausführen (**Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Schnellstartassistent**). Der Schnellstartassistent kann auch überprüfen, ob die installierten Web-Plug-ins aktuell sind, und kann die dafür erforderlichen Updates herunterladen. Weitere Informationen zum Schnellstartassistenten für „Kaspersky Security Center Web Console“ finden Sie in der Hilfe zu Kaspersky Security Center.

- Installieren des Web-Plug-ins aus der Liste der verfügbaren Programmpakete in „Web Console“.

  Um das Web-Plug-in zu installieren, wählen Sie das Verteilungspaket des Kaspersky Endpoint Security-Web-Plug-ins auf der „Web Console“-Benutzeroberfläche aus (**Konsolen-Einstellungen → Web-Plug-ins**). Die Liste der verfügbaren Programmpakete wird automatisch aktualisiert, wenn neue Versionen von Kaspersky-Programmen erscheinen.

- Download des Programmpakets von einer externen Quelle in die „Web Console“.

  Um das Web-Plug-in zu installieren, fügen Sie das zip-Archiv des Verteilungspakets für das Kaspersky Endpoint Security-Web-Plug-in auf der Web Console-Benutzeroberfläche hinzu (**Konsolen-Einstellungen → Web-Plug-ins**). Das Programmpaket des Web-Plug-ins können Sie beispielsweise von der Kaspersky-Website herunterladen.

Ab Kaspersky Endpoint Security 12.11 für Windows ändert sich die Installation des Web-Plug-ins. Das Programmpaket enthält jetzt zwei Web-Plug-ins: *Kaspersky Endpoint Security für Windows 14.2.0* und *Unified Protection and Management Plug-in*. Dies hängt mit der Umstellung auf ein einheitliches Web-Plug-in für die Verwaltung von Kaspersky-Programmen zusammen. Aufgrund des einheitlichen Web-Plug-ins kann eine einzige Richtlinie zur Verwaltung mehrerer Kaspersky-Programme (z. B. Kaspersky Endpoint Security für Windows, macOS und Linux) erstellt werden. Die Umstellung auf das einheitliche Web-Plug-in zieht sich möglicherweise über mehrere Versions-Updates hin. Nach Abschluss der Umstellung enthält das Programmpaket nur noch das *Unified Protection and Management Plug-in*.

Upgrade des Verwaltungs-Plug-ins

Um das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows zu aktualisieren, muss die neueste Version des Verwaltungs-Plug-ins geladen werden (sie gehört zum Lieferumfang) und der Plug-in-Installationsassistent muss ausgeführt werden.

Wenn eine neue Version des Web-Plug-ins für „Web Console“ verfügbar ist, wird die Benachrichtigung *Updates für die verwendeten Plug-ins sind verfügbar* angezeigt. Sie können aus der „Web Console“-Benachrichtigung zum Upgrade des Web-Plug-ins wechseln. Auf der „Web Console“-Benutzeroberfläche (**Konsolen-Einstellungen → Web-Plug-ins**) können Sie auch manuell prüfen, ob Updates für das Web-Plug-in vorliegen. Im Verlauf des Updates wird die vorhergehende Version des Web-Plug-ins automatisch entfernt.

Beim Update des Web-Plug-ins werden bereits vorhandene Elemente (z. B. Richtlinien oder Aufgaben) gespeichert. Neue Einstellungen für Elemente, die neue Funktionen von Kaspersky Endpoint Security realisieren, erscheinen in den vorhandenen Elementen und besitzen Standardwerte.

Es gibt folgende Möglichkeiten, um das Web-Plug-in zu aktualisieren:

- Web-Plug-in in der Liste der Web-Plug-ins im Online-Modus aktualisieren.

  Um das Web-Plug-in zu aktualisieren, müssen Sie das Verteilungspaket des Kaspersky Endpoint Security-Web-Plug-ins auf der „Web Console“-Benutzeroberfläche auswählen (**Konsolen-Einstellungen → Web-Plug-ins**). „Web Console“ prüft, ob auf den Kaspersky-Servern Updates vorliegen und lädt die erforderlichen Updates herunter.

- Web-Plug-in aus einer Datei aktualisieren.

  Um das Web-Plug-in zu aktualisieren, müssen Sie das ZIP-Archiv des Verteilungspakets für das Kaspersky Endpoint Security-Web-Plug-in auf der „Web Console“-Benutzeroberfläche auswählen (**Konsolen-Einstellungen → Web-Plug-ins**). Das Programmpaket des Web-Plug-ins können Sie beispielsweise von der Kaspersky-Website herunterladen. Sie können das Web-Plug-in für Kaspersky Endpoint Security nur auf die neueste Version aktualisieren. Eine Aktualisierung des Web-Plug-ins auf eine ältere Version ist nicht möglich.

Wenn ein beliebiges Element geöffnet wird (z. B. eine Richtlinie oder eine Aufgabe), überprüft das Web-Plug-in die Kompatibilitätsinformationen. Wenn die Version des Web-Plug-ins mit der in den Kompatibilitätsinformationen angegeben Version übereinstimmt oder höher ist, können Sie die Einstellungen dieses Elements ändern. Andernfalls kann das ausgewählte Element nicht mithilfe des Web-Plug-ins geändert werden. Es wird empfohlen, das Web-Plug-in zu aktualisieren.

Besonderheiten für die Verwendung unterschiedlicher Versionen des Verwaltungs-Plug-ins

Sie können Kaspersky Endpoint Security nur dann über das Kaspersky Security Center verwalten, wenn Sie über ein Verwaltungs-Plug-In verfügen, dessen Version gleich oder höher ist als die Version, die in den Informationen zur Kompatibilität von Kaspersky Endpoint Security mit dem Verwaltungs-Plug-In angegeben ist. Die minimal erforderliche Version des Verwaltungs-Plug-Ins können Sie in der Datei installer.ini einsehen, die im Lieferumfang enthalten ist.

Wenn ein beliebiges Element geöffnet wird (z. B. eine Richtlinie oder eine Aufgabe), überprüft das Verwaltungs-Plug-in die Kompatibilitätsinformationen. Wenn die Version des Verwaltungs-Plug-ins mit der in den Kompatibilitätsinformationen angegeben Version übereinstimmt oder höher ist, können Sie die Einstellungen dieses Elements ändern. Andernfalls kann das gewählte Element mithilfe des Verwaltungs-Plug-ins nicht geändert werden. Es wird empfohlen, das Verwaltungs-Plug-in zu aktualisieren.

Wenn das Verwaltungs-Plug-in für Kaspersky Endpoint Security in der Verwaltungskonsole installiert ist, gelten für die Installation der neuen Version des Verwaltungs-Plug-ins die folgenden Besonderheiten:

- Die ältere Version des Verwaltungs-Plug-ins für Kaspersky Endpoint Security wird entfernt.
- Die neue Version des Verwaltungs-Plug-ins für Kaspersky Endpoint Security unterstützt die Verwaltung der älteren Version von Kaspersky Endpoint Security für Windows auf den Benutzercomputern.
- Sie können mithilfe der neuen Version des Verwaltungs-Plug-ins die Einstellungen in Richtlinien, Aufgaben usw. ändern, die mit der älteren Version des Verwaltungs-Plug-ins erstellt wurden.
- Für neue Einstellungen werden von der neuen Version des Verwaltungs-Plug-ins die Standardwerte festgelegt, sobald eine Richtlinie, ein Richtlinienprofil oder eine Aufgabe zum ersten Mal gespeichert wird.

  Es wird empfohlen, nach dem Update des Verwaltungs-Plug-ins die Werte der neuen Einstellungen in den Richtlinien und Richtlinienprofilen zu überprüfen und zu speichern. Sollten Sie dies nicht tun, so besitzen die neuen Einstellungsblöcke von Kaspersky Endpoint Security auf dem Benutzercomputer die Standardwerte und können geändert werden (Attribut). Mit der Überprüfung sollte bei den Richtlinien und Richtlinienprofilen der höheren Ebene einer Hierarchie begonnen werden. Außerdem wird empfohlen, ein Benutzerkonto zu verwenden, für das Zugriffsrechte auf alle funktionalen Bereich von Kaspersky Security Center vorhanden sind.

  Über neue Programmfunktionen können Sie sich in den Versionshinweisen oder in der Hilfe zum Programm informieren.

- Wenn in der neuen Version des Verwaltungs-Plug-ins eine neue Einstellung zu einem Einstellungsblock hinzugefügt wurde, bleibt der Status des Attributs / für diesen Einstellungsblock unverändert.

Besondere Überlegungen bei der Verwendung verschlüsselter Protokolle für die Interaktion mit externen Diensten

Kaspersky Endpoint Security und Kaspersky Security Center verwenden einen verschlüsselten Kommunikationskanal mit TLS (Transport Layer Security), um mit externen Diensten von Kaspersky zusammenzuarbeiten. Kaspersky Endpoint Security verwendet externe Dienste für die folgenden Funktionen:

- Update der Datenbanken und Programm-Module;
- Aktivierung des Programms mit einem Aktivierungscode (Aktivierung 2.0);
- Verwendung von Kaspersky Security Network

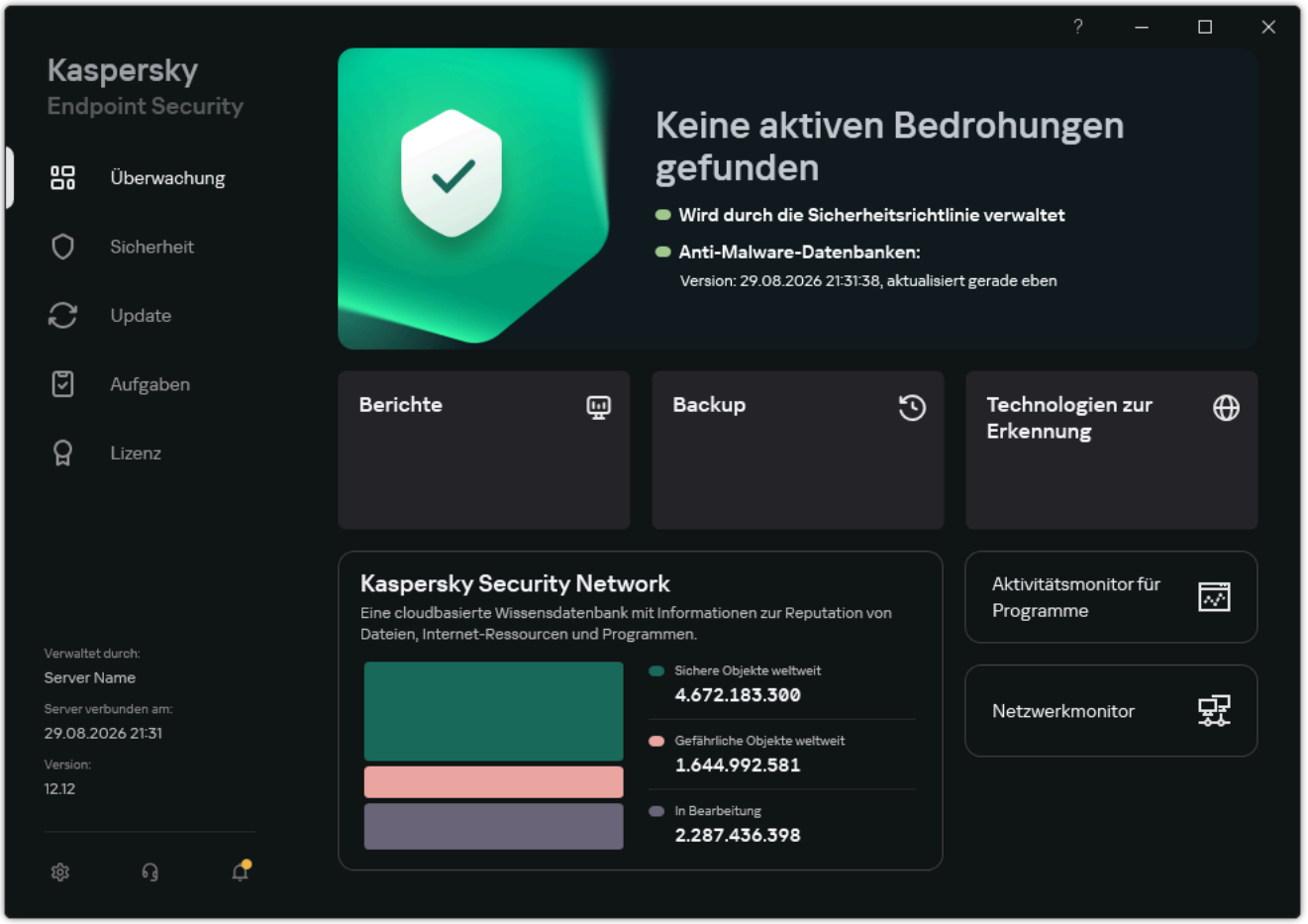
Die Verwendung von TLS sichert das Programm durch die Bereitstellung der folgenden Funktionen:

- Verschlüsselung. Der Inhalt der Nachrichten ist vertraulich und wird nicht an Drittnutzer weitergegeben.
- Integrität. Der Empfänger der Nachricht ist sicher, dass der Inhalt der Nachricht seit der Weiterleitung durch den Absender nicht geändert wurde.
- Authentifizierung. Der Empfänger ist sicher, dass die Kommunikation nur mit einem vertrauenswürdigen Kaspersky-Server hergestellt wird.

Kaspersky Endpoint Security verwendet Zertifikate mit öffentlichen Schlüsseln zur Serverauthentifizierung. Für die Verwendung von Zertifikaten ist eine Public Key Infrastructure erforderlich. Eine Zertifizierungsstelle ist Teil einer PKI. Kaspersky verwendet seine eigene Zertifizierungsstelle, da die Kaspersky-Dienste hochtechnisch und nicht öffentlich sind. Wenn Stammzertifikate von Thawte, VeriSign, GlobalTrust und anderen widerrufen werden, bleibt die Kaspersky-PKI in diesem Fall weiterhin betriebsbereit.

Umgebungen, die über MITM (Software- und Hardware-Tools, die das Parsen des HTTPS-Protokolls unterstützen) verfügen, werden von Kaspersky Endpoint Security als unsicher eingestuft. Bei der Arbeit mit Kaspersky-Diensten können Fehler auftreten. Beispielsweise kann es Fehler bei der Verwendung von Self-Signed Certificate geben. Diese Fehler können auftreten, weil ein HTTPS-Inspektionstool aus Ihrer Umgebung die Kaspersky PKI nicht erkennt. Um diese Probleme zu beheben, müssen Sie Ausnahmen für die Interaktion mit externen Diensten konfigurieren.

Programmoberfläche



Programmhauptfenster

Überwachung	• **Berichte**. Zeigen Sie Ereignisse an, die bei der Nutzung des Programms, einzelner Komponenten und Aufgaben aufgetreten sind. • **Backup**. Eine Liste der gespeicherten Kopien von infizierten Dateien anzeigen, die vom Programm gelöscht wurden. • **Technologien zur Erkennung**. Hier finden Sie Informationen über Technologien zur Erkennung von Bedrohungen und die Anzahl der von diesen Technologien erkannten Bedrohungen. • **Kaspersky Security Network**. Status der Verbindung zwischen Kaspersky Endpoint Security und Kaspersky Security Network sowie globale KSN-Statistiken. *Kaspersky Security Network (KSN)* ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. 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. • **Aktivitätsmonitor für Programme**. Informationen über den Betrieb der installierten Programme anzeigen. Der Aktivitätsmonitor für Programme überwacht Datei-, Registrierungs- und Systemereignisse, die im Betriebssystem auftreten und sich auf ein Programm beziehen. • **Netzwerkmonitor**. Informationen über die Netzwerkaktivität des Computers in Echtzeit anzeigen. • **Verschlüsselung**. Überwacht den Vorgang der Festplattenverschlüsselung und -entschlüsselung in Echtzeit. Encryption Monitor ist verfügbar, wenn die Komponente „Kaspersky-Festplattenverschlüsselung“ oder „BitLocker-Laufwerkverschlüsselung“ installiert ist.
Sicherheit	Betriebsstatus der installierten Komponenten. Sie können die Komponenten konfigurieren oder Berichte anzeigen.
Update	Die Update-Aufgaben für Kaspersky Endpoint Security verwalten. Sie können Antiviren-Datenbanken und Programm-Module aktualisieren und das letzte Update zurücksetzen. Ein Administrator kann den Abschnitt für den Benutzer ausblenden oder die Aufgabenverwaltung einschränken.
Aufgaben	Die Untersuchungsaufgaben von Kaspersky Endpoint Security verwalten. Sie können eine Schadsoftware-Untersuchung und eine Integritätsprüfung des Programms durchführen. Ein Administrator kann Aufgaben vor einem Benutzer verbergen oder die Verwaltung von Aufgaben einschränken.

Lizenz	Lizenzverwaltung des Programms. Sie können eine Lizenz erwerben, die Anwendung aktivieren oder ein Abonnement verlängern. Sie können auch Informationen über die aktuelle Lizenz anzeigen.
	Programmeinstellungen anpassen. Ein Administrator kann Änderungen an Einstellungen im Kaspersky Security Center verbieten.
	Informationen über das Programm: aktuelle Version von Kaspersky Endpoint Security, Datum der Veröffentlichung der Datenbank, Schlüssel und andere Informationen. Sie können auch zu den Kaspersky-Informationsquellen navigieren, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Kauf, zur Installation und zur Verwendung des Programms bieten.
	Nachrichten, die Informationen über verfügbare Updates und Anträge auf Zugang zu verschlüsselten Dateien und Geräten enthalten.

Programmsymbol im Infobereich

Sofort nach der Installation von Kaspersky Endpoint Security erscheint das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.

Wenn das App-Symbol im Infobereich der Taskleiste ausgeblendet ist, hat der Administrator die Anzeige der App-Benutzeroberfläche in der Richtlinie deaktiviert.

Das Symbol übernimmt folgende Funktionen:

- Es dient als Indikator für die Ausführung des Programms.
- Es ermöglicht den Zugriff auf das Kontextmenü und auf das Programmhauptfenster.

Für das Programmsymbol gibt es die folgenden Statusvarianten, die Informationen über die Programmnutzung visualisieren:

- Das Symbol bedeutet, dass alle kritischen Schutzkomponenten des Programms aktiviert sind. Kaspersky Endpoint Security zeigt eine Warnung an, wenn der Benutzer eine Aktion ausführen muss, z. B. den Computer nach der Aktualisierung des Programms neu starten.
- Das Symbol bedeutet, dass die Funktion der Schutzkomponenten des Programms deaktiviert oder gestört ist. Die Funktion der Schutzkomponenten kann beispielsweise gestört sein, wenn die Lizenz abgelaufen ist oder im Programm eine Störung aufgetreten ist. Kaspersky Endpoint Security zeigt die Warnung und eine Beschreibung des Problems im Computerschutz an.

Das Kontextmenü des Programmsymbols enthält die folgenden Punkte:

- **Kaspersky Endpoint Security für Windows**. Öffnet das Programmhauptfenster. In diesem Fenster können Sie die Funktion der Komponenten und Aufgaben des Programms anpassen sowie eine Statistik zu verarbeiteten Dateien und gefundenen Bedrohungen einsehen.
- **Schutz anhalten** / **Schutz fortsetzen**. Anhalten aller Schutz- und Kontrollkomponenten, die in der Richtlinie kein Vorhängeschloss () haben. Bevor dieser Vorgang ausgeführt wird, sollte die Richtlinie für Kaspersky Security Center deaktiviert werden.

  Bevor die Schutz- und Kontrollkomponenten angehalten werden, fragt das Programm nach dem Kennwort für den Zugriff auf Kaspersky Endpoint Security (Kennwort des Benutzerkontos oder temporäres Kennwort). Dann können Sie auswählen, wie lange die Pause dauern soll: für einen bestimmten Zeitraum, bis zum Neustart, oder Fortsetzung auf Befehl des Benutzers.

  Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist. Um den Betrieb der Schutz- und Kontrollkomponenten fortzusetzen, klicken Sie im Kontextmenü des Programms auf **Schutz fortsetzen**.

Das Anhalten der Schutz- und Kontrollkomponenten beeinflusst die Ausführung von Update-Aufgaben und Aufgaben zur Virensuche nicht. Das Programm setzt auch die Verwendung von Kaspersky Security Network fort.

- **Richtlinie deaktivieren** / **Richtlinie aktivieren**. Richtlinie für Kaspersky Security Center auf dem Computer deaktivieren. Alle Einstellungen für Kaspersky Endpoint Security können angepasst werden, einschließlich jener Einstellungen, die in der Richtlinie ein geschlossenen Schloss (🔒) haben. Beim Deaktivieren der Richtlinie fragt das Programm nach dem Kennwort für den Zugriff auf Kaspersky Endpoint Security (Kennwort des Benutzerkontos oder temporäres Kennwort). Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist. Um die Richtlinie zu aktivieren, wählen Sie im Programm-Kontextmenü den Punkt **Richtlinie aktivieren** aus.

- **Einstellungen**. Öffnet das Fenster mit den Programmeinstellungen.

- **Support**. Öffnet ein Fenster, das Informationen zur Kontaktaufnahme mit dem Technischen Support von Kaspersky enthält.

- **Über das Programm**. Öffnet ein Informationsfenster mit Angaben zum Programm.

- **Beenden**. Beendet Kaspersky Endpoint Security. Wenn Sie diese Option im Kontextmenü gewählt haben, wird das Programm aus dem Arbeitsspeicher des Computers entfernt.



Kontextmenü des Programmsymbols

Einfache Programmoberfläche

Wenn der Client-Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie von Kaspersky Security Center unterliegt und in dieser Richtlinie die Anzeige der einfachen Programmoberfläche festgelegt ist, so ist das Programmhauptfenster auf diesem Client-Computer nicht verfügbar. Der Benutzer kann durch Rechtsklick das Kontextmenü des Symbols von Kaspersky Endpoint Security öffnen (siehe folgende Abb.), das folgende Punkte enthält:

- **Richtlinie deaktivieren** / **Richtlinie aktivieren**. Richtlinie für Kaspersky Security Center auf dem Computer deaktivieren. Alle Einstellungen für Kaspersky Endpoint Security können angepasst werden, einschließlich jener Einstellungen, die in der Richtlinie ein geschlossenen Schloss (🔒) haben. Beim Deaktivieren der Richtlinie fragt das Programm nach dem Kennwort für den Zugriff auf Kaspersky Endpoint Security (Kennwort des Benutzerkontos oder temporäres Kennwort). Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist. Um die Richtlinie zu aktivieren, wählen Sie im Programm-Kontextmenü den Punkt **Richtlinie aktivieren** aus.

- **Aufgaben**. Dropdown-Liste mit folgenden Elementen:

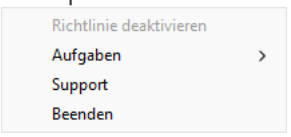
  - **Prüfung der Anwendungsintegrität**.

  - **Rollback der Datenbanken auf die vorherige Version**.

  - **Vollständige Untersuchung**.

- **Benutzerdefinierte Untersuchung**.
- **Untersuchung wichtiger Bereiche**.
- **Update**.

- **Support**. Öffnet ein Fenster, das Informationen zur Kontaktaufnahme mit dem Technischen Support von Kaspersky enthält.
- **Beenden**. Beendet Kaspersky Endpoint Security. Wenn Sie diese Option im Kontextmenü gewählt haben, wird das Programm aus dem Arbeitsspeicher des Computers entfernt.



Kontextmenü des Programmsymbols bei der Anzeige der einfachen Programmoberfläche

Darstellung der Programmoberfläche anpassen

Sie können die Anzeige der Programmoberfläche für den Computerbenutzer anpassen. Der Benutzer kann wie folgt mit dem Programm interagieren:

- **Vereinfacht**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Außerdem zeigt Kaspersky Endpoint Security über dem Anwendungssymbol nur Benachrichtigungen an, die das Eingreifen des Benutzers erfordern.
- **Vollständig**. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.
- **Benutzeroberfläche nicht anzeigen**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Endpoint Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.

So konfigurieren Sie den Anzeigemodus der Programmoberfläche in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Benutzeroberfläche** aus.

4. Passen Sie im Block **Interaktion mit dem Benutzer** an, wie die Benutzeroberfläche angezeigt werden soll:

   - **Benutzeroberfläche anzeigen**. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an. Bei Bedarf können Sie die Funktion **Abschnitt „Aktivitätsmonitor für Programme“ ausblenden** aktivieren. Dadurch werden Daten über die Anwendungsaktivität auf dem Computer ausgeblendet und der Benutzerzugriff auf den Aktivitätsmonitor für Programme wird eingeschränkt.

   - **Vereinfachte Programmoberfläche anzeigen**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Außerdem zeigt Kaspersky Endpoint Security über dem Anwendungssymbol nur Benachrichtigungen an, die das Eingreifen des Benutzers erfordern.

   - **Benutzeroberfläche nicht anzeigen**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Endpoint Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.

5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Anzeigemodus der Programmoberfläche in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.

5. Passen Sie im Block **Sichtbarkeit für Benutzer** an, wie die Benutzeroberfläche angezeigt werden soll:

   - **Benutzeroberfläche anzeigen**. Wenn diese Funktion deaktiviert ist, sind auf dem Client-Computer keine Anzeichen für den Betrieb von Kaspersky Endpoint Security zu sehen. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.

   - **Vereinfacht**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Außerdem zeigt Kaspersky Endpoint Security über dem Anwendungssymbol nur Benachrichtigungen an, die das Eingreifen des Benutzers erfordern.

   - **Vollständig**. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an.

   - **Abschnitt „Aktivitätsmonitor für Programme“ ausblenden**. Wenn Sie Informationen zur Programmaktivität auf einem Benutzercomputer ausblenden möchten, können Sie den Benutzerzugriff auf das Tool „Aktivitätsmonitor für Programme“ einschränken.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Vorbereitung des Programms

Nachdem das Programm auf den Client-Computern verteilt wurde, müssen Sie wie folgt vorgehen, um Kaspersky Endpoint Security aus Kaspersky Security Center zu verwenden:

- Richtlinie erstellen und anpassen.

  Mithilfe von Richtlinien können Sie identische Funktionseinstellungen von Kaspersky Endpoint Security für alle Client-Computer festlegen, die zu einer Administrationsgruppe gehören. Der Schnellstartassistent für Kaspersky Security Center erstellt automatisch eine Richtlinie für Kaspersky Endpoint Security.

- Die Aufgaben *Update der Datenbanken und Programm-Module* und *Schadsoftware-Untersuchung* erstellen.

  Die Aufgabe *Update der Datenbanken und Programm-Module* ist erforderlich, um den Computerschutz auf dem neuesten Stand zu halten. Bei der Aufgabenausführung aktualisiert Kaspersky Endpoint Security die Antiviren-Datenbanken und die Programm-Module. Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

  Die *Schadsoftware-Untersuchung* ist erforderlich, um Viren und andere bedrohliche Programme rechtzeitig zu erkennen. Die Aufgabe *Schadsoftware-Untersuchung* muss manuell erstellt werden.

  So erstellen Sie die Aufgabe Schadsoftware-Untersuchung über die Verwaltungskonsole (MMC)

  1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

     Die Aufgabenliste wird geöffnet.

  2. Klicken Sie auf **Neue Aufgabe**.

  Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Schadsoftware-Untersuchung** aus.

Schritt 2. Untersuchungsbereich

Erstellen Sie eine Liste der Objekte, die Kaspersky Endpoint Security im Rahmen der Untersuchungsaufgabe untersuchen soll.

Schritt 3. Aktion von Kaspersky Endpoint Security

Wählen Sie die Aktion beim Fund einer Bedrohung aus:

- **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 – Informieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Wenn die Desinfektion fehlschlägt, fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.

- **Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.

- **Aktive Desinfektion sofort ausführen**. Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Endpoint Security bei der Untersuchung die Technologie zur aktiven Desinfektion.

  Die *Technologie zur Desinfektion aktiver Infektionen* dient dazu, schädliche Programme aus dem Betriebssystem zu entfernen, falls diese ihre Prozesse bereits im Arbeitsspeicher gestartet haben und Kaspersky Endpoint Security daran hindern, sie auf reguläre Weise zu neutralisieren. Dadurch wird die Bedrohung neutralisiert. Es wird davon abgeraten, während der aktiven Desinfektion neue Prozesse zu starten oder die Registrierung des Betriebssystems zu ändern. Die Technologie zur Desinfektion aktiver Infektionen beansprucht erhebliche Betriebssystemressourcen, wodurch die Ausführung anderer Programme verlangsamt werden kann. Nach Abschluss der aktiven Desinfektion startet Kaspersky Endpoint Security den Computer neu, ohne nach einer Bestätigung des Benutzers zu fragen.

- **Nur ausführen, wenn der Computer inaktiv ist**. Schiebt den Start der Aufgabe auf, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde. Mit dieser Zeitplanoption können Sie die Computerressourcen schonen, während der Computer verwendet wird.

Schritt 4. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.

- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 5: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie eine Benutzerkonto für den Start der Aufgabe *Schadsoftware-Untersuchung* aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos. Wenn zum Untersuchungsbereich Netzlaufwerke oder andere Objekte gehören, auf die der Zugriff beschränkt ist, wählen Sie ein Benutzerkonto mit den erforderlichen Zugriffsrechten aus.

Schritt 6. Zeitplan des Aufgabenstarts anpassen

Passen Sie einen Zeitplan für den Aufgabenstart an, beispielsweise manuell oder nachdem die Antiviren-Datenbanken in den Speicher geladen wurden.

Schritt 7. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen an, beispielsweise *Vollständige Untersuchung täglich*.

Schritt 8. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch wird auf den Benutzercomputern eine Schadsoftware-Untersuchung gemäß dem festgelegten Zeitplan ausgeführt.

So erstellen Sie die Aufgabe Schadsoftware-Untersuchung über die Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Schadsoftware-Untersuchung**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Wöchentliche Untersuchung*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Wechseln Sie zu den Aufgabeneigenschaften, um den Zeitplan für die Aufgabenausführung anzupassen.

   Die Ausführung der Aufgabe sollte mindestens einmal wöchentlich festgelegt werden.

8. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

9. Klicken Sie auf **Starten**.

   Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen.

Dadurch wird auf den Benutzercomputern eine Schadsoftware-Untersuchung gemäß dem festgelegten Zeitplan ausgeführt.

- Leistung von Kaspersky Endpoint Security optimieren.

Richtlinienverwaltung

Eine *Richtlinie* ist eine Auswahl von Programmeinstellungen, die für eine bestimmte Administrationsgruppe gilt. Für ein Programm können mehrere Richtlinien mit unterschiedlichen Werten angepasst werden. Die Programmeinstellungen können sich für bestimmte Administrationsgruppen unterscheiden. In jeder Administrationsgruppe kann eine eigene Richtlinie für das Programm erstellt werden.

Jede Richtlinieneinstellung hat das Attribut („Vorhängeschloss"). Der Status dieses Attributs bestimmt, ob die Einstellung auf die verwalteten Geräte in der Administrationsgruppe übertragen wird:

- Wenn das „Vorhängeschloss" offen ist ( ), wird der Wert dieser Einstellung nicht auf die verwalteten Geräte übertragen. Die Einstellung kann in der lokalen Programmoberfläche geändert werden. Solche Einstellungen werden *entsperrt* genannt.

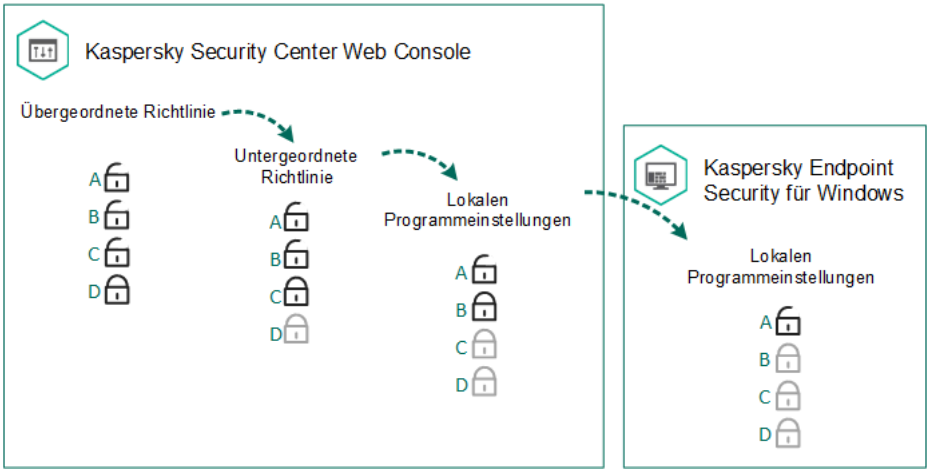
- Wenn das „Vorhängeschloss" geschlossen ist ( ), wird der Wert dieser Einstellung auf die verwalteten Geräte übertragen und auf diese angewandt. Solche Einstellungen werden *gesperrt* genannt. Gesperrte Einstellungen können in der lokalen Programmoberfläche nicht geändert werden.

Die Einstellungen der Richtlinie werden bei der *Synchronisierung* mithilfe des Administrationsagenten an die Client-Computer übertragen. Standardmäßig führt der Administrationsserver die Synchronisierung sofort aus, nachdem die Einstellungen der Richtlinie geändert wurden. Die Synchronisierung erfolgt über den UDP-Port 15000 auf dem Client-Computer. Der Administrationsserver führt standardmäßig alle 15 Minuten eine Synchronisierung durch. Wenn eine Synchronisierung nach der Änderung der Richtlinieneinstellungen fehlgeschlagen ist, wird der nächste Synchronisierungsversuch nach dem vorgegebenen Zeitplan ausgeführt.

Vererbung von Einstellungen

Richtlinien und Administrationsgruppen sind hierarchisch organisiert. Eine *untergeordnete Richtlinie* ist die Richtlinie einer untergeordneten Hierarchie-Ebene, d. h. eine Richtlinie für untergeordnete Administrationsgruppen und sekundäre Administrationsserver.

Eine untergeordnete Richtlinie erbt standardmäßig die Einstellungen der übergeordneten Richtlinie. Hat die Einstellung in der übergeordneten Richtlinie das Attribut (geschlossenes „Vorhängeschloss"), wird der Wert dieser Einstellung in untergeordneten Richtlinien und in den lokalen Programmeinstellungengemäß der übergeordneten Richtlinie überschrieben und die Einstellung wird gesperrt. Erforderlichenfalls können Sie die Vererbung von Einstellungen aus der übergeordneten Richtlinie deaktivieren. Mobile Richtlinien unterliegen nicht der Hierarchie von Administrationsgruppen für andere Richtlinien.



Vererbung von Einstellungen

Die Rechte für den Zugriff auf Richtlinieneinstellungen (Lesen, Ändern, Ausführen) werden für jeden Benutzer festgelegt, der Zugriff auf den Administrationsserver für Kaspersky Security Center besitzt, und zudem separat für jeden Funktionsbereich von Kaspersky Endpoint Security. Um die Rechte für den Zugriff auf Richtlinieneinstellungen anzupassen, gehen Sie zum Abschnitt **Sicherheit** des Eigenschaftenfensters für den Kaspersky Security Center-Administrationsserver (dieser Abschnitt ist in der Konsolenoberfläche standardmäßig ausgeblendet).

Revision von Richtlinien

Kaspersky Security Center verfolgt Richtlinienänderungen und erstellt Revisionen. Eine *Revision* ist eine Auswahl geänderter Parameter, die vom Benutzer gespeichert wurden. Anhand von Revisionen können Sie Änderungen an Richtlinienparametern vergleichen und rückgängig machen. Die Revision enthält neben den geänderten Parametern auch Informationen über den Benutzer, der die Änderungen vorgenommen hat, sowie Uhrzeit, IP-Adresse, Benutzerkommentare und andere relevante Daten.

So zeigen Sie das Revisionsprotokoll an: Öffnen Sie die Richtlinieneigenschaften und gehen Sie zum Abschnitt **Revisionsverlauf**. Weitere Informationen über die Arbeit mit Revisionen finden Sie in der Hilfe zu Kaspersky Security Center.

Richtlinie erstellen

Beim Erstellen einer Richtlinie schlägt der Assistent Einstellungen vor, die zum ausgewählten Modus passen. Für den Light Agent-Modus müssen Sie beispielsweise einen Schutzserver (SVM) hinzufügen. Wenn Sie die App zum Schutz eines SQL-Servers verwenden, müssen Sie vordefinierte Untersuchungsausnahmen hinzufügen, damit der Betrieb des Servers nicht beeinträchtigt wird. Nachdem ein Modus ausgewählt wurde, schlägt der Assistent entsprechende Richtlinieneinstellungen vor. Dann können Sie diese Einstellungen in den Richtlinieneigenschaften bearbeiten.

Erstellen einer Richtlinie In der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe aus, zu der die entsprechenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Klicken Sie auf **Neue Richtlinie**.

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

Schritt 1.

Wählen Sie das Programm **Kaspersky Endpoint Security für Windows (14.2)** aus.

Schritt 2.

Geben Sie einen Namen für die Gruppenrichtlinie ein, z. B. *Büro-Richtlinie*.

Sie können neue Richtlinien auch auf der Grundlage der vorhandenen mithilfe des Assistenten für das Erstellen einer Richtlinie erstellen. Aktivieren Sie dazu bei der Angabe des Namens der Gruppenrichtlinie das Kontrollkästchen **Richtlinieneinstellungen für eine frühere Version der Anwendung verwenden**. Der Assistent ermöglicht es auch, eine Richtlinie für Kaspersky Endpoint Security (KES) zu erstellen, die auf der Richtlinie einer anderen Lösung basiert, z. B. Kaspersky Security für Windows Server (KSWS) oder Kaspersky Security for Virtualization Light Agent für Windows.

Schritt 3. Text der Erklärung zu Kaspersky Security Network anzeigen

Bitte lesen und akzeptieren Sie die Erklärung zu Kaspersky Security Network (KSN).

Schritt 4.

Je nachdem, wie Sie Kaspersky Endpoint Security verwenden möchten, können Sie eine Richtlinie für die folgenden Programmmodi konfigurieren:

- Standardmodus für den Schutz von Hosts

  In diesem Modus können Sie auswählen, wie Sie die Richtlinie konfigurieren möchten:

  - **Eine Richtlinie mit Standardeinstellungen erstellen**. Die Standardeinstellungen gelten als optimal. Diese Einstellungen werden von den Kaspersky-Experten empfohlen. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung.

  - **Richtlinieneinstellungen im Assistenten ändern**. Mit dieser Methode können Sie die Richtlinieneinstellungen mithilfe eines Assistenten schrittweise anpassen. Sie können die Richtlinieneinstellungen auch mithilfe einer Konfigurationsdatei des Programms verwalten (mehr dazu im folgenden Schritt).

- Endpoint Detection and Response Agent für den Schutz vor komplexen Bedrohungen und gezielten Angriffen.

  Die App *Endpoint Detection and Response Agent* wird in der IT-Infrastruktur des Unternehmens auf einzelnen Workstations und Servern installiert und unterstützt die Detection and Response-Lösungen von Kaspersky. Beim nächsten Schritt müssen Sie eine Lösung für die EDR Agent-Integration auswählen.

- Light Agent für den Schutz virtueller Umgebungen.

  Um das Programm im Light Agent-Modus zu verwenden, müssen Sie eine Verbindung mit einer virtuellen SVM-Maschine konfigurieren. Diese Einstellungen sind erforderlich, damit das Programm im Light Agent-Modus funktioniert.

Kaspersky Endpoint Security bietet eine gemeinsame Richtlinie für alle Programm-Modi und Betriebssystemtypen. Das bedeutet, dass die Richtlinie alle Einstellungsvarianten abdeckt. Es kann jedoch vorkommen, dass das Programm einige der Richtlinieneinstellungen ignoriert, da Kaspersky Endpoint Security in einem Modus bereitgestellt wird, in dem einige Funktionen nicht verfügbar sind. Wenn das Programm beispielsweise im Endpoint Detection and Response Agent-Modus verwendet wird, sind nur die Einstellungen verfügbar, die für die Integration mit den Kaspersky Detection and Response-Lösungen und für die KUMA-Integration relevant sind.

Es wird empfohlen, für die einzelnen Modi und Betriebssystemtypen unterschiedliche Richtlinien zu verwenden.

Schritt 5. Einstellungen importieren

Dieser Schritt ist verfügbar, wenn Sie bei Schritt 4 die manuelle Richtlinienkonfiguration ausgewählt haben.

Sie können eine Richtlinie auf Basis von Einstellungen für Kaspersky Endpoint Security aus einer CFG-Konfigurationsdatei erstellen. Der Assistent für neue Richtlinien unterstützt keine verschlüsselten Konfigurationsdateien. Überspringen Sie beim Exportieren der Konfigurationsdatei den Schritt zur Dateiverschlüsselung.

Beim Importieren einer CFG-Konfigurationsdatei des Programms stehen im Assistenten nicht alle Richtlinieneinstellungen zur Verfügung. In den Programmeinstellungen fehlen beispielsweise Richtlinienprofile. Wenn Sie alle Einstellungen und Profile in die Richtlinie übertragen möchten, können Sie eine andere Richtlinie aus einer KLP-Datei importieren.

Wenn eine Konfigurationsdatei importiert wird, überträgt Kaspersky Endpoint Security keine Kennwörter für Krypto-Container. Wenn Sie für die Verbindung mit Servern die Zwei-Wege-Authentifizierung verwenden, müssen Sie die Kennwörter für Krypto-Container völlig neu angeben.

Schritt 6 bis 10. Richtlinieneinstellungen konfigurieren

Dieser Schritt ist verfügbar, wenn Sie bei Schritt 4 die manuelle Richtlinienkonfiguration ausgewählt haben.

Folgen Sie den Schritten, um die Richtlinieneinstellungen zu anzupassen.

Schritt 11. Vertrauenswürdige Zone konfigurieren

Vertrauenswürdige Zone konfigurieren Sie können vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme hinzufügen. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme sind auch praktisch, um Kaspersky Endpoint Security im Light Agent-Modus in virtuellen Citrix- und VMware-Umgebungen schnell zu konfigurieren.

Schritt 12. Status der Richtlinie auswählen

- **Aktiv**. Die Richtlinie wird auf diesem Computer nach der nächsten Synchronisierung als aktive Richtlinie verwendet.

  Die Einstellungen einer aktiven Richtlinie werden bei der Synchronisierung auf den Client-Computern gespeichert. Für einen Computer dürfen nicht mehrere Richtlinien gleichzeitig gelten, deshalb kann in jeder Gruppe nur eine Richtlinie aktiv sein.

- **Inaktiv**. Ersatzrichtlinie. Eine inaktive Richtlinie kann erforderlichenfalls aktiviert werden.

  Sie können unbeschränkt viele inaktive Richtlinien erstellen. Eine inaktive Richtlinie beeinflusst die Programmeinstellungen auf den Computern im Netzwerk nicht. Inaktive Richtlinien erlauben eine schnelle Reaktion auf Extremsituationen wie beispielsweise Virenangriffe. Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. Dabei wird die aktive Richtlinie automatisch inaktiv.

- **Mobil**. Die Richtlinie wird nur wirksam, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.

Schließen Sie den Assistenten ab.

So erstellen Sie eine Richtlinie in „Web Console“ und „Cloud Console”

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Richtlinien wird gestartet.
3. Wählen Sie Kaspersky Endpoint Security aus und klicken Sie auf **Weiter**.
4. Lesen und akzeptieren Sie die Erklärung zu Kaspersky Security Network (KSN) und klicken Sie auf **Weiter**.
5. Wählen Sie einen Programm-Modus aus:

   - Standard-Modus für den Schutz von Workstations und Servern
   - Endpoint Detection and Response Agent für den Schutz vor komplexen Bedrohungen und gezielten Angriffen.

     Wenn Sie diesen Modus auswählen, können Sie eine Richtlinie erstellen, um den Computer in die Lösungen von Kaspersky Detection and Response zu integrieren. Der Assistent fordert Sie auf, die Integration in Kaspersky Managed Detection and Response und anschließend in Kaspersky Anti Targeted Attack Platform (EDR) zu konfigurieren.
   - Light Agent für den Schutz virtueller Umgebungen.

     Wenn Sie diesen Modus auswählen, müssen Sie beim nächsten Schritt die Verbindung zum Schutzserver (SVM) konfigurieren. Diese Einstellungen sind erforderlich, damit das Programm im Light Agent-Modus funktioniert.

   Kaspersky Endpoint Security bietet eine gemeinsame Richtlinie für alle Programm-Modi und Betriebssystemtypen. Das bedeutet, dass die Richtlinie alle Einstellungsvarianten abdeckt. Es kann jedoch vorkommen, dass das Programm einige der Richtlinieneinstellungen ignoriert, da Kaspersky Endpoint Security in einem Modus bereitgestellt wird, in dem einige Funktionen nicht verfügbar sind. Wenn das Programm beispielsweise im Endpoint Detection and Response Agent-Modus verwendet wird, sind nur die Einstellungen verfügbar, die für die Integration mit den Kaspersky Detection and Response-Lösungen und für die KUMA-Integration relevant sind.

   > Es wird empfohlen, für die einzelnen Modi und Betriebssystemtypen unterschiedliche Richtlinien zu verwenden.
6. Vertrauenswürdige Zone konfigurieren Sie können vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme hinzufügen. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme sind auch praktisch, um Kaspersky Endpoint Security im Light Agent-Modus in virtuellen Citrix- und VMware-Umgebungen schnell zu konfigurieren.

7. Auf der Registerkarte **Allgemein** können Sie folgende Aktionen ausführen:

   - Name der Richtlinie ändern
   - Status der Richtlinie auswählen:
     - **Aktiv**. Die Richtlinie wird auf diesem Computer nach der nächsten Synchronisierung als aktive Richtlinie verwendet.

       Die Einstellungen einer aktiven Richtlinie werden bei der Synchronisierung auf den Client-Computern gespeichert. Für einen Computer dürfen nicht mehrere Richtlinien gleichzeitig gelten, deshalb kann in jeder Gruppe nur eine Richtlinie aktiv sein.

     - **Inaktiv**. Ersatzrichtlinie. Eine inaktive Richtlinie kann erforderlichenfalls aktiviert werden.

       Sie können unbeschränkt viele inaktive Richtlinien erstellen. Eine inaktive Richtlinie beeinflusst die Programmeinstellungen auf den Computern im Netzwerk nicht. Inaktive Richtlinien erlauben eine schnelle Reaktion auf Extremsituationen wie beispielsweise Virenangriffe. Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. Dabei wird die aktive Richtlinie automatisch inaktiv.

     - **Mobil**. Die Richtlinie wird nur wirksam, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.
   - Vererbung von Einstellungen anpassen:
     - **Einstellungen aus übergeordneter Richtlinie erben**. Ist dieser Schalter aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Stufe übernommen. Die Einstellungen der Richtlinie können nicht geändert werden, wenn in der übergeordneten Richtlinie das Attribut gilt.

     - **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen**. Ist der Schalter aktiviert, so werden die Werte der Richtlinieneinstellungen an die untergeordnete Richtlinien vererbt. 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 aus der übergeordneten Richtlinie übernommen, unter Ausnahme von Einstellungen mit dem Attribut . Die Einstellungen von untergeordneten Richtlinien können nicht geändert werden, wenn in der übergeordneten Richtlinie das Attribut gilt.

8. Auf der Registerkarte **Anwendungseinstellungen** können Sie die Einstellungen der Richtlinie für Kaspersky Endpoint Security anpassen.

9. Schließen Sie den Assistenten ab.

Dadurch wird festgelegt, dass die Einstellungen von Kaspersky Endpoint Security auf den Client-Computern bei der nächsten Synchronisierung angepasst werden. Informationen über die Richtlinie, die für den Computer gilt, finden Sie auf der Benutzeroberfläche von Kaspersky Endpoint Security. Klicken Sie dazu im Hauptfenster auf die Schaltfläche (z. B. Name der Richtlinie). Dafür muss in den Richtlinieneinstellungen des Administrationsagenten der Empfang erweiterter Richtliniendaten aktiviert sein. Weitere Informationen über die Richtlinie des Administrationsagenten finden Sie in der Hilfe zu Kaspersky Security Center.

Eine Richtlinie exportieren und importieren

Mit Kaspersky Endpoint Security können Sie eine Richtlinie mit Einstellungen und Profilen in eine KLP-Datei exportieren. Anschließend können Sie die Export/Import-Funktion für Richtlinien verwenden, um ein Backup von Richtlinien anzulegen, Richtlinien auf einen anderen Server zu migrieren oder Richtlinien beispielsweise von Kaspersky Security Center Windows nach Kaspersky Security Center Linux zu migrieren. Details zur Verwaltung von Richtlinien finden Sie in der Hilfe zu Kaspersky Security Center.

So exportieren und importieren Sie eine Richtlinie (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. So exportieren Sie eine Richtlinie:
   a. Klicken Sie auf die Richtlinie, die Sie exportieren möchten.
   b. Klicken Sie auf den Link **Richtlinie in Datei exportieren**, der sich rechts im Fenster befindet.
   c. Geben Sie im folgenden Fenster den Namen der KLP-Datei an, in die Sie die Richtlinie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll.
   d. Speichern Sie die Datei.
5. So importieren Sie eine Richtlinie:
   a. Klicken Sie auf **Richtlinie aus Datei importieren**.
   b. Wählen Sie im angezeigten Fenster die KLP-Richtliniendatei aus, die Sie importieren möchten.
   c. Öffnen Sie die Datei.

   Dadurch wird eine neue Richtlinie mit dem Status *Inaktive Richtlinie* hinzugefügt.

So exportieren und importieren Sie die Richtlinie in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. So exportieren Sie eine Richtlinie:
   a. Aktivieren Sie das Kontrollkästchen der Richtlinie, die Sie exportieren möchten.
   b. Klicken Sie auf die Schaltfläche **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der KLP-Datei an, in die Sie die Richtlinie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll.
   d. Speichern Sie die Datei.

3. So importieren Sie eine Richtlinie:

    a. Klicken Sie auf **Importieren**.

    b. Wählen Sie die KLP-Richtliniendatei aus, die Sie importieren möchten.

    c. Nachdem die Richtlinie erfolgreich verarbeitet wurde, wählen Sie die Administrationsgruppe aus, auf die Sie die Richtlinie anwenden möchten.

    d. Klicken Sie auf **Abgeschlossen**, um den Import der Richtlinie abzuschließen.

    Dadurch wird eine neue Richtlinie mit dem Status *Inaktiv* hinzugefügt.

Indikator des Schutzniveaus

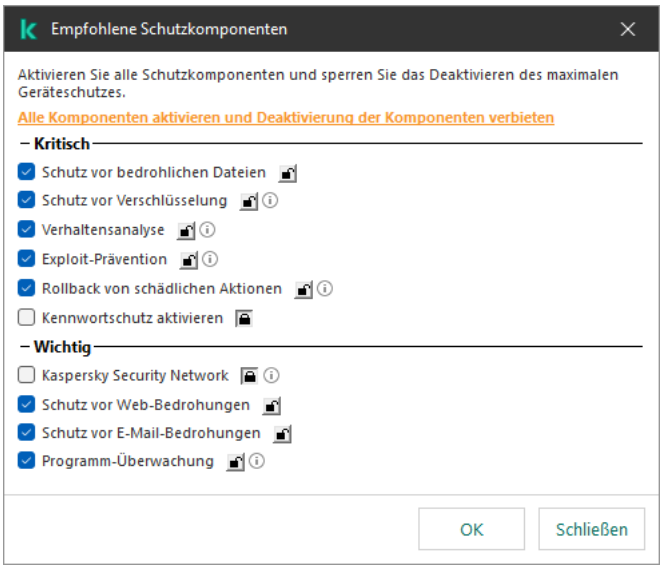
Der Sicherheitsstufen-Indikator befindet sich am oberen Rand des Fensters mit den Richtlinieneigenschaften. Der Indikator kann einen der folgenden Werte annehmen:

- **Hohes Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Grün, wenn alle Komponenten, die zu den folgenden Kategorien gehören, aktiviert sind:
    - **Kritisch**. Diese Kategorie umfasst die folgenden Komponenten:
        - Schutz vor bedrohlichen Dateien.
        - Verhaltensanalyse.
        - Exploit-Prävention.
        - Rollback von schädlichen Aktionen.
        - Schutz der App-Dienste vor externer Steuerung.
    - **Wichtig**. Diese Kategorie umfasst die folgenden Komponenten:
        - Kaspersky Security Network.
        - Schutz vor Web-Bedrohungen.
        - Schutz vor E-Mail-Bedrohungen.
        - Programm-Überwachung.
        - Kennwortschutz.
- **Mittleres Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Gelb, wenn eine wichtige Komponente deaktiviert ist.

- **Niedriges Schutzniveau**. Der Indikator nimmt diesen Wert an und wird Rot, wenn einer der folgenden Fälle eintritt:
  - Eine oder mehrere kritische Komponenten sind deaktiviert.
  - Eine oder mehrere wichtige Komponenten sind deaktiviert.

Wenn der Indikator mit dem Wert **Mittleres Schutzniveau** oder **Niedriges Schutzniveau** angezeigt wird, befindet sich rechts vom Indikator ein Link, der ins Fenster **Empfohlene Schutzkomponenten** führt. In diesem Fenster können Sie die empfohlenen Schutzkomponenten aktivieren.

Nach dem Programm-Upgrade wird möglicherweise eine niedrigere Schutzstufe angezeigt als vor dem Upgrade. Der Grund: Mit der neueren Programmversion werden neue Komponenten oder Funktionen eingeführt, die für die Sicherheit des Computers wichtig sind. Nach dem Programm-Upgrade müssen Sie die neuen Einstellungen anpassen, um eine hohe Schutzstufe sicherzustellen.



Indikator für die Sicherheitsstufe der Richtlinie

Aufgabenverwaltung

Für die Arbeit mit Kaspersky Endpoint Security über Kaspersky Security Center können Sie folgende Aufgabentypen erstellen:

- lokale Aufgaben für einen einzelnen Client-Computer
- Gruppenaufgaben für Client-Computer, die zu Administrationsgruppen gehören
- Aufgabe für bestimmte Computer.

Sie können beliebig viele Gruppenaufgabe, Aufgaben für bestimmte Computer und lokale Aufgaben erstellen. Weitere Informationen über die Verwendung von Administrationsgruppen und bestimmten Computern finden Sie in der Hilfe für Kaspersky Security Center.

Kaspersky Endpoint Security unterstützt die Ausführung der folgenden Aufgaben:

- **Schadsoftware-Untersuchung**. Kaspersky Endpoint Security untersucht die Computerbereiche, die in den Aufgabeneinstellungen angegeben sind, auf Viren und andere bedrohliche Programme. Die Aufgabe *Schadsoftware-Untersuchung* ist für Kaspersky Endpoint Security obligatorisch und wird im Rahmen des Schnellstartassistenten erstellt. Die Ausführung der Aufgabe sollte mindestens einmal wöchentlich festgelegt werden.

- **Schlüssel hinzufügen**. Kaspersky Endpoint Security fügt einen Schlüssel für die Aktivierung des Programms hinzu. Dies kann auch ein Reserveschlüssel sein. Vergewissern Sie sich vor der Aufgabenausführung, dass die Anzahl der Computer, auf denen die Aufgabe ausgeführt werden soll, nicht über der Anzahl der Computer liegt, für welche die Lizenz gilt.

- **Auswahl der Programmkomponenten ändern**. Kaspersky Endpoint Security installiert oder löscht Komponenten auf den Client-Computern. Dabei wird nach der Komponentenliste verfahren, die in den Aufgabeneinstellungen angegeben ist. Die Komponente „Schutz vor bedrohlichen Dateien“ kann nicht gelöscht werden. Durch eine optimale Auswahl der Komponenten von Kaspersky Endpoint Security können die Ressourcen des Computers geschont werden.

- **Inventarisierung**. Kaspersky Endpoint Security erhält Informationen über alle ausführbaren Programmdateien, die auf dem Computer gespeichert sind. Die Aufgabe *Inventarisierung* wird von der Komponente „Programmkontrolle“ ausgeführt. Wenn die Komponente „Programmkontrolle“ nicht installiert ist, wird die Aufgabe mit einem Fehler beendet.

- **Update der Datenbanken und Programm-Module**. Kaspersky Endpoint Security aktualisiert die Datenbanken und Programm-Module. Die Aufgabe *Update der Datenbanken und Programm-Module* ist für Kaspersky Endpoint Security obligatorisch und wird im Rahmen des Schnellstartassistenten erstellt. Die Ausführung der Aufgabe sollte mindestens einmal täglich eingeplant werden.

- **Daten zurücksetzen**. Kaspersky Endpoint Security löscht die Dateien und Ordner vom Benutzercomputer entweder sofort oder wenn längere Zeit keine Verbindung zu Kaspersky Security Center besteht.

- **Update-Rollback**. Kaspersky Endpoint Security macht das letzte Update der Datenbanken und Programm-Module rückgängig. Dies kann beispielsweise erforderlich sein, wenn die neuen Datenbanken fehlerhafte Daten enthalten, was dazu führen kann, dass Kaspersky Endpoint Security ein sicheres Programm blockiert.

- **Prüfung der Anwendungsintegrität**. Kaspersky Endpoint Security analysiert die Programmdateien, untersucht die Dateien auf Beschädigungen und Veränderungen, und überprüft die digitalen Signaturen der Programmdateien.

- **Authentifizierungsagenten-Konten verwalten**. Kaspersky Endpoint Security passt die Einstellungen der Benutzerkonten für den Authentifizierungsagenten an. Der Authentifizierungsagent ist für die Arbeit mit verschlüsselten Datenträgern erforderlich. Der Benutzer muss vor dem Start des Betriebssystems die Authentifizierung mithilfe des Agenten durchlaufen.

Wenn die App als Teil der Kaspersky-Lösung Endpoint Detection and Response eingesetzt wird, können Sie zusätzliche Aufgaben als Aktionen zur Erkennungsreaktion (responses) ausführen. Sie können beispielsweise Prozesse mithilfe der Aufgabe *Prozess beenden* per Fernzugriff beenden.

Die Aufgaben werden nur dann auf dem Computer gestartet, wenn das Programm Kaspersky Endpoint Security läuft.

Eine Aufgabe erstellen

In der Verwaltungskonsole (MMC) eine Aufgabe erstellen

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Aufgaben**.
3. Klicken Sie auf **Neue Aufgabe**.

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

So erstellen Sie eine Aufgabe in der Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.
3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Aufgabe aus, die Sie auf den Benutzercomputern ausführen möchten.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.
4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt
5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.
6. Schließen Sie den Assistenten ab.

Die neue Aufgabe wird in der Aufgabenliste angezeigt. Die Aufgabe besitzt Standardeinstellungen. Um die Aufgabeneinstellungen anzupassen, müssen Sie zu den Aufgabeneigenschaften wechseln. Um die Aufgabe auszuführen, müssen Sie das Kontrollkästchen neben der Aufgabe aktivieren und auf **Starten** klicken. Nach dem Aufgabenstart können Sie die Aufgabe anhalten und später fortsetzen.

In der Aufgabenliste können Sie das Ausführungsergebnis der Aufgaben kontrollieren: Aufgabenstatus und Statistik über die Aufgabenausführung auf den Computern. Sie können auch eine Auswahl mit bestimmten Ereignissen erstellen, um die Aufgabenausführung zu überwachen (**Überwachung → Ereignisauswahlen**). Weitere Informationen über die Ereignisauswahl finden Sie in der Hilfe zu Kaspersky Security Center. Die Ergebnisse der Aufgabenausführung werden auch lokal auf dem Computer im Ereignisprotokoll von Windows und in den Berichten von Kaspersky Endpoint Security gespeichert.

Zugriff auf Aufgaben verwalten

Die Rechte für den Zugriff auf die Aufgaben von Kaspersky Endpoint Security (Lesen, Ändern, Ausführen) werden für jeden Benutzer festgelegt, der Zugriff auf den Kaspersky Security Center Administrationsserver besitzt. Die Rechte werden über die Zugriffseinstellungen für die Funktionsbereiche von Kaspersky Endpoint Security zugeteilt. Um den Zugriff auf die Funktionsbereiche von Kaspersky Endpoint Security anzupassen, gehen Sie im Eigenschaftenfenster des Kaspersky Security Center-Administrationsservers zum Abschnitt **Sicherheit**. Weitere Informationen zur Aufgabenverwaltung über Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Sie können die Zugriffsrechte der Benutzer für Aufgaben mithilfe einer Richtlinie konfigurieren (*Modus der Aufgabenverwaltung*). Sie können beispielsweise Gruppenaufgaben auf der Benutzeroberfläche von Kaspersky Endpoint Security ausblenden.

So konfigurieren Sie den Aufgabenverwaltungsmodus in der Benutzeroberfläche von Kaspersky Endpoint Security über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Lokale Aufgaben** → **Aufgabenverwaltung** aus.
4. Passen Sie den Modus für die Arbeit mit Aufgaben an (s. folgende Tabelle).
5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Aufgabenverwaltungsmodus in der Benutzeroberfläche von Kaspersky Endpoint Security über die Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.
5. Konfigurieren Sie unter **Erlaubte Aktionen** den Modus der Aufgabenverwaltung (siehe folgende Tabelle).
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Einstellung	Beschreibung
Auf lokale Aufgaben zugreifen	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. Wenn dieses Kontrollkästchen deaktiviert ist, werden lokale Aufgaben in der Programmoberfläche ausgeblendet. 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	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	Wenn das Kontrollkästchen aktiviert ist, können Benutzer die in der Kaspersky Security Center-Konsole angegebenen 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: Entweder startet Kaspersky Endpoint Security die geplanten Aufgaben automatisch oder der Administrator startet die Aufgaben manuell über die Kaspersky Security Center-Konsole.

Lokale Programmeinstellungen anpassen

Im Kaspersky Security Center können Sie die Einstellungen von Kaspersky Endpoint Security auf einem bestimmten Computer konfigurieren. Sie sind die *lokalen Programmeinstellungen*. Es kann sein, dass bestimmte Einstellungen nicht geändert werden können. Diese Einstellungen sind durch das Attribut in den Eigenschaften der Richtlinie blockiert.

So konfigurieren Sie die lokalen Programmeinstellungen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.
6. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Endpoint Security für Windows (14.2)** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.
7. Passen Sie im Abschnitt **Allgemeine Einstellungen** Kaspersky Endpoint Security sowie die Einstellungen für Berichte und Speicher an.

   Die übrigen Abschnitte im Fenster mit den Programmeigenschaften sind für Kaspersky Security Center standardmäßig. Eine Beschreibung dieser Abschnitte finden Sie in der Hilfe zu Kaspersky Security Center.

Gilt für das Programm eine Richtlinie, durch die eine Änderung bestimmter Einstellungen untersagt ist, so können diese Einstellungen nicht geändert werden, während die Programmeinstellungen im Abschnitt **Allgemeine Einstellungen** angepasst werden.

8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die lokalen Programmeinstellungen in der Web Console und der Cloud-Konsole

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.

   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Klicken Sie auf **Kaspersky Endpoint Security für Windows 14.2**.

   Die lokalen Programmeinstellungen werden geöffnet.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Passen Sie die lokalen Programmeinstellungen an.
7. Speichern Sie die vorgenommenen Änderungen.

Die lokalen Programmeinstellungen entsprechen den Einstellungen der Richtlinie, unter Ausnahme der Verschlüsselungseinstellungen.

Kaspersky Endpoint Security starten und beenden

Nach der Installation von Kaspersky Endpoint Security auf dem Benutzercomputer wird das Programm automatisch gestartet. Künftig wird Kaspersky Endpoint Security standardmäßig sofort nach dem Betriebssystem gestartet. Der automatische Programmstart kann in den Einstellungen des Betriebssystems nicht angepasst werden.

Nach dem Start des Betriebssystems kann es bis zu zwei Minuten dauern, bis die Antiviren-Datenbanken für Kaspersky Endpoint Security geladen sind. Die Dauer ist von der Leistung (den technischen Möglichkeiten) des Computers abhängig. In diesem Zeitraum ist das Schutzniveau des Computers reduziert. Werden die Antiviren-Datenbanken beim Start des Programms Kaspersky Endpoint Security geladen, wenn das Betriebssystem bereits gestartet wurde, so wird das Schutzniveau des Computers dadurch nicht negativ beeinflusst.

So konfigurieren Sie den Start von Kaspersky Endpoint Security in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.

4. Passen Sie mithilfe des Kontrollkästchens **Programm beim Hochfahren des Computers starten (empfohlen)** den Programmstart an.

5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Start von Kaspersky Endpoint Security in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Interaktion mit dem Benutzer**.

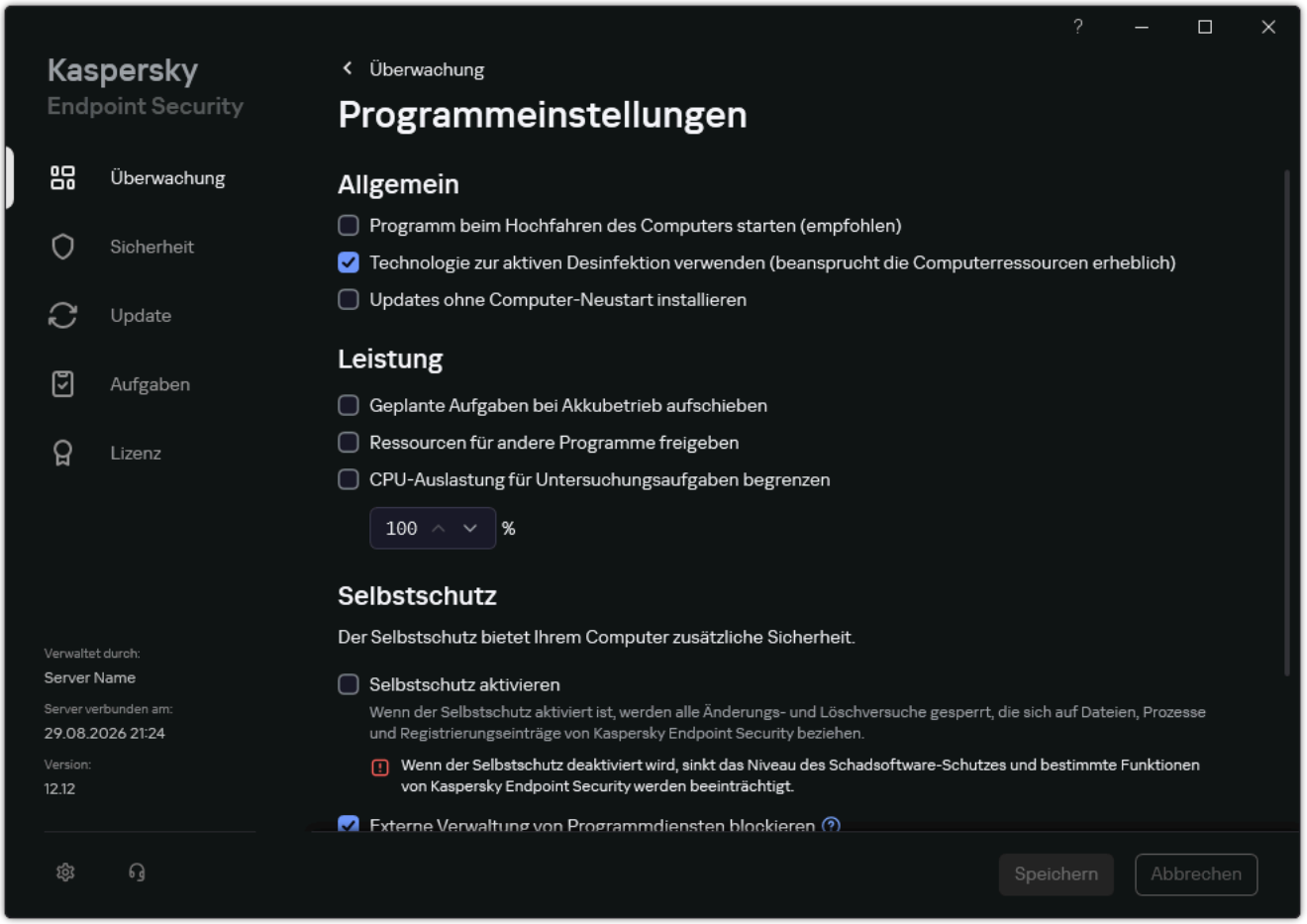
5. Passen Sie mithilfe des Kontrollkästchens **Kaspersky Endpoint Security beim Hochfahren des Computers starten (empfohlen)** den Programmstart an.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Start von Kaspersky Endpoint Security in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows"

3. Passen Sie mithilfe des Kontrollkästchens **Programm beim Hochfahren des Computers starten (empfohlen)** den Programmstart an.

4. Speichern Sie die vorgenommenen Änderungen.

Die Kaspersky-Experten warnen davor, Kaspersky Endpoint Security zu beenden, da Ihr Computer und Ihre Daten dann bedroht sind. Bei Bedarf können Sie den Computerschutz für einen bestimmten Zeitraum anhalten, ohne das Programm zu beenden.

Den Programmstatus können Sie über das Widget **Schutzstatus** überwachen.

So starten oder stoppen Sie Kaspersky Endpoint Security in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.

4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.

5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.

6. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Endpoint Security für Windows (14.2)** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.

7. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie das Programm starten möchten, klicken Sie rechts von der Liste der Kaspersky-Programme auf die Schaltfläche .
   - Wenn Sie das Programm beenden möchten, klicken Sie rechts von der Liste der Kaspersky-Programme auf die Schaltfläche .

So starten oder stoppen Sie Kaspersky Endpoint Security in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Klicken Sie auf den Namen des Computers, auf dem Sie Kaspersky Endpoint Security starten oder beenden möchten.

   Das Eigenschaftenfenster des Computers wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungen** aus.

4. Aktivieren Sie das Kontrollkästchen neben **Kaspersky Endpoint Security für Windows**.

5. Klicken Sie auf **Starten** oder **Beenden**.

So starten oder stoppen Sie Kaspersky Endpoint Security von der Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.

2. Gehen Sie in den Ordner, in dem sich die ausführbare Datei klpsm.exe befindet.

3. Um das Programm zu starten, geben Sie in der Befehlszeile ein: `klpsm.exe start_avp_service`.

4. Um das Programm zu beenden, geben Sie in der Befehlszeile ein: `klpsm.exe stop_avp_service`.

Um das Programm aus der Befehlszeile zu beenden, muss die externe Steuerung von Systemdiensten aktiviert werden.



Die App über die Befehlszeile starten und beenden

Anhalten und Fortsetzen von Computerschutz und -kontrolle

Werden der Schutz und die Kontrolle des Computers angehalten, so werden alle Schutzkomponenten und alle Kontrollkomponenten von Kaspersky Endpoint Security vorübergehend deaktiviert.

Der Programmstatus wird mit dem Programmsymbol im Infobereich der Taskleiste visualisiert:

- Das Symbol bedeutet, dass Schutz und Kontrolle des Computers angehalten sind.
- Das Symbol bedeutet, dass Schutz und Kontrolle des Computers aktiviert sind.

Wenn der Schutz und die Kontrolle des Computers angehalten oder fortgesetzt werden, hat dies keinen Einfluss auf die Ausführung von Untersuchungs- und Update-Aufgaben.

Wenn zum Zeitpunkt, zu dem der Schutz und die Kontrolle des Computers angehalten oder fortgesetzt werden, Netzwerkverbindungen bestehen, informiert eine Bildschirmmeldung darüber, dass diese Verbindungen getrennt werden.

Um den Schutz und die Kontrolle des Computers fortzusetzen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.

2. Wählen Sie im Kontextmenü **Schutz anhalten** (siehe Abbildung unten).

   Dieser Punkt des Kontextmenüs ist verfügbar, wenn der Kennwortschutz aktiviert ist.

3. Wählen Sie eine der vorgeschlagenen Varianten aus:

   - **Anhalten für <Zeitraum>** – Der Schutz und die Kontrolle des Computers werden nach Ablauf des Zeitraums aktiviert, der in der Dropdown-Liste festgelegt wird.
   - **Anhalten bis zum Neustart der App** – Der Schutz und die Kontrolle des Computers werden nach einem Neustart des Programms oder des Betriebssystems aktiviert. Um diese Option zu verwenden, muss der automatische Programmstart aktiviert sein.
   - **Anhalten** – Der Schutz und die Kontrolle des Computers werden aktiviert, wenn Sie sie fortsetzen.

4. Klicken Sie auf **Schutz anhalten**.

Kaspersky Endpoint Security hält alle Schutz- und Kontrollkomponenten an, die in der Richtlinie kein Vorhängeschloss () haben. Bevor dieser Vorgang ausgeführt wird, sollte die Richtlinie für Kaspersky Security Center deaktiviert werden.



Kontextmenü des Programmsymbols

Gehen Sie folgendermaßen vor, um den Schutz und die Kontrolle des Computers fortzusetzen:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Wählen Sie im Kontextmenü den Punkt **Schutz fortsetzen**.

Sie können den Schutz und die Kontrolle des Computers jederzeit fortsetzen, unabhängig davon, auf welche Weise der Schutz und die Kontrolle des Computers zuvor angehalten wurden.

Konfigurationsdatei erstellen und verwenden

Mithilfe der Konfigurationsdatei für die Einstellungen von Kaspersky Endpoint Security lassen sich folgende Aufgaben lösen:

- Ausführen einer lokalen Installation von Kaspersky Endpoint Security über die Befehlszeile mit zuvor festgelegten Einstellungen.
- Ausführen einer Remote-Installation von Kaspersky Endpoint Security über Kaspersky Security Center mit zuvor festgelegten Einstellungen.
- Programmeinstellungen in eine Richtlinie übertragen.
- Migrieren Sie die Einstellungen für Kaspersky Endpoint Security von einem Computer auf einen anderen (siehe folgenden Anleitung).

Eine Konfigurationsdatei exportieren

Ab Kaspersky Endpoint Security Version 14.2 kann die exportierte Konfigurationsdatei verschlüsselt werden. Da die Konfigurationsdatei Anmeldeinformationen enthalten kann, empfehlen wir, die Konfigurationsdatei zu verschlüsseln. Sie können eine verschlüsselte Datei nicht bearbeiten. Jeder Versuch, eine Konfigurationsdatei zu ändern, führt zur Beschädigung der Datei.

Für die Verschlüsselung von Konfigurationsdateien gelten die folgenden Besonderheiten:

- Kaspersky Endpoint Security ermöglicht den Import verschlüsselter Dateien nur über die Benutzeroberfläche des Programms oder über die Befehlszeile. Sie können eine solche Datei nicht in einer Konsole von Kaspersky Security Center verwenden, um eine Richtlinie zu konfigurieren oder das Programm remote zu installieren. Wenn Sie die Datei zu einer Richtlinie oder einem Installationspaket hinzufügen möchten, überspringen Sie den Schritt zur Verschlüsselung der Datei.
- Das Kennwort einer verschlüsselten Datei kann nicht wiederhergestellt werden.
- Versionen von Kaspersky Endpoint Security vor Version 14.1 unterstützen den Import verschlüsselter Konfigurationsdateien nicht. Wenn Sie die Datei in eine frühere Version des Programms importieren möchten, überspringen Sie den Schritt zur Verschlüsselung der Datei.

Um eine Konfigurationsdatei zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Einstellungen verwalten** aus.
3. Klicken Sie auf **Export**.
4. Um die Konfigurationsdatei zu speichern, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Einstellungen exportieren** besitzen.
5. Geben Sie in dem sich öffnenden Fenster den Pfad zu dem Ort an, an dem Sie die Konfigurationsdatei speichern möchten, und geben Sie ihren Namen ein.

   Um die Konfigurationsdatei für die lokale Installation oder für die Remote-Installation von Kaspersky Endpoint Security zu verwenden, müssen Sie die Datei als install.cfg benennen.

6. Aktivieren Sie bei Bedarf den Schalter **Exportierte Datei verschlüsseln** und geben Sie das Verschlüsselungskennwort für die Konfigurationsdatei ein.

   Speichern Sie das Kennwort in einem sicheren Speicher. Dieses Kennwort kann nicht wiederhergestellt werden.

7. Speichern Sie die Datei.

Daraufhin erstellt das Programm eine Konfigurationsdatei.

Eine Konfigurationsdatei importieren

Wenn eine Konfigurationsdatei importiert wird, überträgt Kaspersky Endpoint Security keine Kennwörter für Krypto-Container. Wenn Sie für die Verbindung mit Servern die Zwei-Wege-Authentifizierung verwenden, müssen Sie die Kennwörter für Krypto-Container völlig neu angeben.

Um die Einstellungen für Kaspersky Endpoint Security aus einer Konfigurationsdatei zu importieren, gehen Sie wie folgt vor:

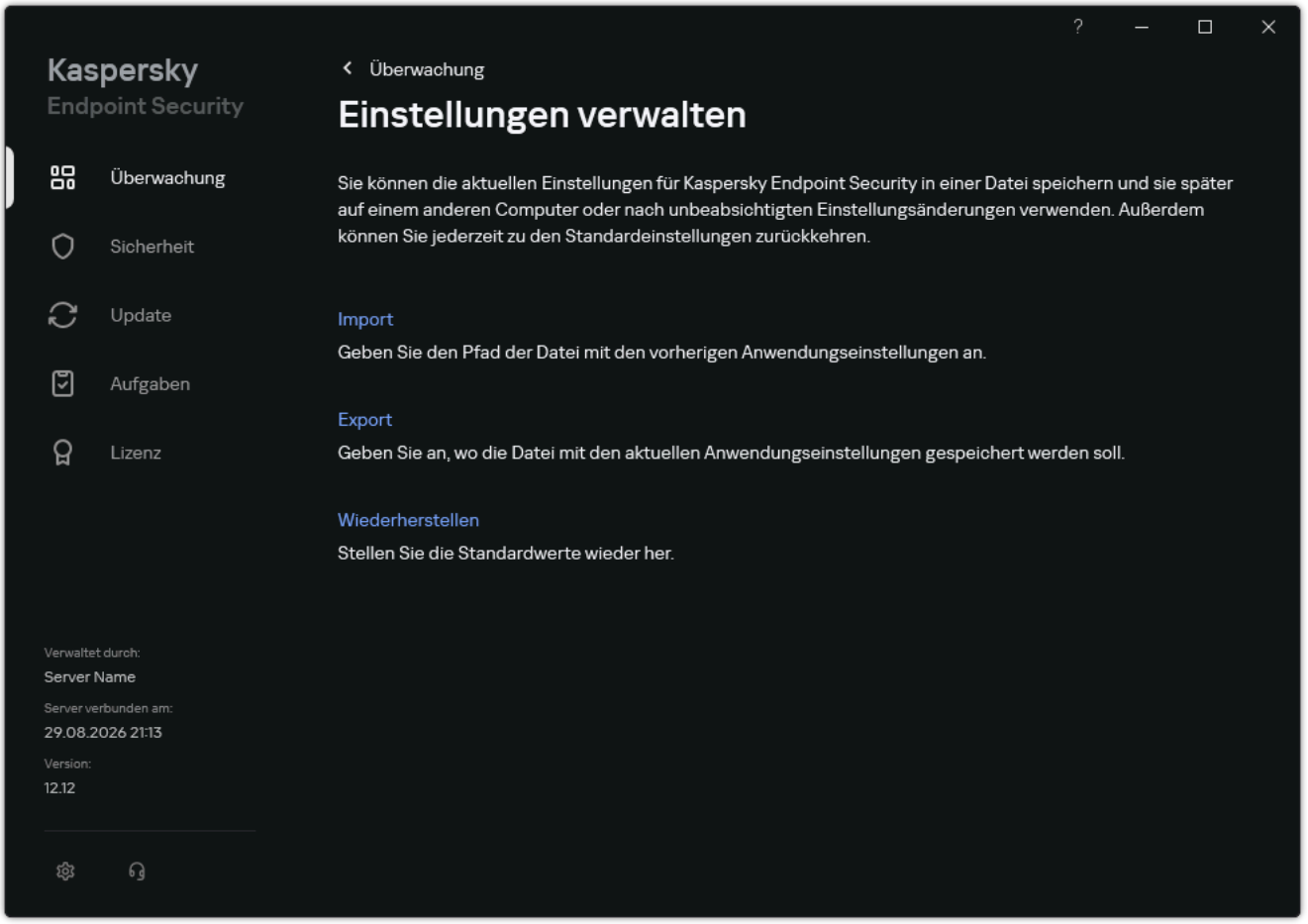
1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Einstellungen verwalten** aus.
3. Klicken Sie auf **Import**.
4. Geben Sie im folgenden Fenster den Pfad der Konfigurationsdatei an.

5. Wenn die Konfigurationsdatei verschlüsselt ist, geben Sie das beim Export festgelegte Kennwort ein.

> Wenn Sie das Verschlüsselungskennwort der Konfigurationsdatei vergessen haben, können Sie es nicht wiederherstellen. In diesem Fall müssen Sie die Schritte zum Exportieren der Konfigurationsdatei wiederholen.

6. Öffnen Sie die Datei.

Alle Werte für die Einstellungen von Kaspersky Endpoint Security werden gemäß der ausgewählten Konfigurationsdatei festgelegt.



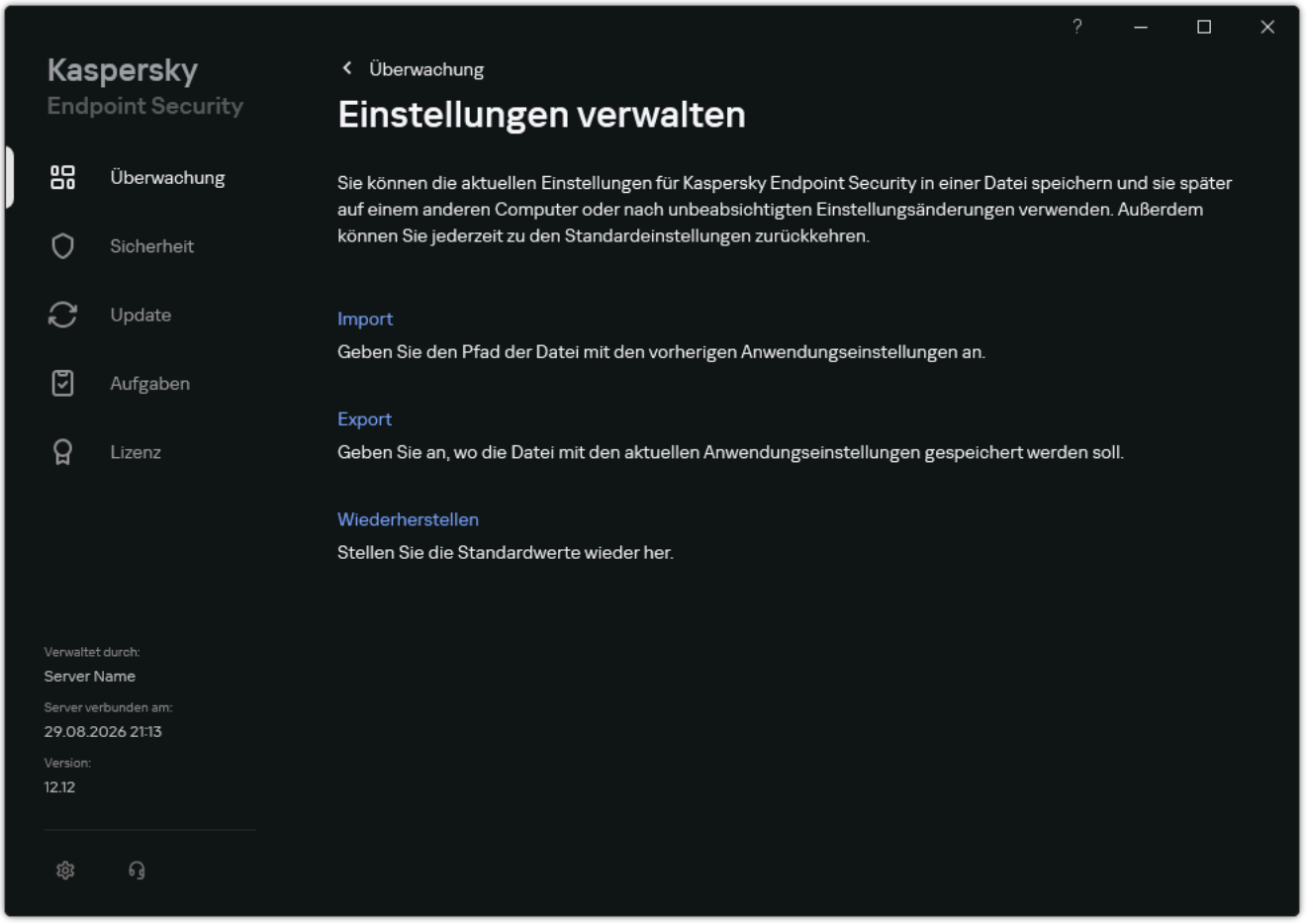
App-Einstellungen verwalten

Standardeinstellungen für das Programm wiederherstellen

Sie können jederzeit die von Kaspersky- empfohlenen Programmeinstellungen wiederherstellen. Wenn die Einstellungen wiederhergestellt werden, wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** festgelegt.

So stellen Sie die Standardeinstellungen für das Programm wieder her:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Einstellungen verwalten** aus.
3. Klicken Sie auf **Wiederherstellen**.
4. Speichern Sie die vorgenommenen Änderungen.



App-Einstellungen verwalten

Leistung von Kaspersky Endpoint Security und Kompatibilität mit anderen Programmen

Unter der Leistung von Kaspersky Endpoint Security sind die Anzahl der erkennbaren Objekttypen, die dem Computer Schaden zufügen können, sowie der Energieverbrauch und die benötigten Computerressourcen zu verstehen.

Erkennbare Objekttypen wählen

Kaspersky Endpoint Security erlaubt es, den Computerschutz flexibel anzupassen und die Objekttypen auszuwählen, die das Programm bei seiner Ausführung erkennen soll. Kaspersky Endpoint Security untersucht das Betriebssystem stets auf Viren, Würmer und trojanische Programme. Die Untersuchung dieser Objekttypen kann nicht deaktiviert werden. Diese Programme können dem Computer erheblichen Schaden zufügen. Um das Schutzniveau zu erhöhen, können Sie die Liste der erkennbaren Objekttypen erweitern. Aktivieren Sie dazu die Kontrolle der Aktionen legaler Programme, die von Angreifern zur Beschädigung des Computers und der Benutzerdaten genutzt werden können.

Energiesparmodus nutzen

Bei mobilen Computern ist der Energieverbrauch, der von Programmen verursacht wird, ein wichtiges Thema. Häufig beanspruchen die von Kaspersky Endpoint Security nach Zeitplan ausgeführten Aufgaben erhebliche Ressourcen. Läuft der Computer im Akkubetrieb, können Sie zur Gewährleistung einer längeren Akkulaufzeit den Energiesparmodus nutzen.

Der Energiesparmodus ermöglicht eine automatische Verschiebung von Aufgaben, für die ein Start nach Zeitplan festgelegt ist:

- Aufgabe zur vollständigen Untersuchung;
- Aufgabe zur Untersuchung wichtiger Bereiche;
- Aufgabe zur benutzerdefinierten Untersuchung;
- Aufgabe zur Integritätsprüfung.

Unabhängig davon, ob der Energiesparmodus aktiviert ist oder nicht, hält Kaspersky Endpoint Security laufende Verschlüsselungsaufgaben an, wenn ein Laptop in den Batteriebetrieb wechselt. Wenn der Laptop aus dem Batteriebetrieb in den Netzbetrieb wechselt, setzt das Programm die Verschlüsselungsaufgaben fort.

Computerressourcen für andere Programme freigeben

Während der Untersuchung eines Computers werden die Computerressourcen beansprucht. Dadurch erhöht sich möglicherweise die Auslastung des Prozessors und der Laufwerksubsysteme. Um Probleme zu vermeiden, die bei gleichzeitiger Verwendung mit anderen Anwendungen aufgrund erhöhter Belastung des Prozessors und der Laufwerksubsysteme auftreten können, kann Kaspersky Endpoint Security Ressourcen für andere Anwendungen freigeben.

Technologie zur Desinfektion aktiver Infektionen nutzen

Moderne schädliche Programme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Bei Erkennen einer schädlichen Aktivität im Betriebssystem nimmt Kaspersky Endpoint Security eine erweiterte Desinfektion vor, wobei eine spezielle Technologie zur Desinfektion aktiver Infektionen zum Einsatz kommt. Die *Technologie zur Desinfektion aktiver Infektionen* dient dazu, schädliche Programme aus dem Betriebssystem zu entfernen, falls diese ihre Prozesse bereits im Arbeitsspeicher gestartet haben und Kaspersky Endpoint Security daran hindern, sie auf reguläre Weise zu neutralisieren. Dadurch wird die Bedrohung neutralisiert. Es wird davon abgeraten, während der aktiven Desinfektion neue Prozesse zu starten oder die Registrierung des Betriebssystems zu ändern. Die Technologie zur Desinfektion aktiver Infektionen beansprucht erhebliche Betriebssystemressourcen, wodurch die Ausführung anderer Programme verlangsamt werden kann.

Nachdem die aktive Desinfektion auf einem Computer mit Microsoft Windows Workstation abgeschlossen wurde, fragt Kaspersky Endpoint Security den Benutzer um Erlaubnis für einen Neustart des Computers. Nach dem Neustart des Computers löscht Kaspersky Endpoint Security die Schadsoftware-Dateien und startet eine vereinfachte vollständige Untersuchung des Computers.

Auf einem Computer mit Microsoft Windows für Server ist eine Abfrage für den Neustart des Computers nicht möglich. Dies ist durch Besonderheiten des Programms Kaspersky Endpoint Security bedingt. Ein ungeplanter Neustart des Dateiservers kann zu Problemen führen. Es kann zu einer vorübergehenden Nichtverfügbarkeit der Dateiserverdaten oder zum Verlust von nicht gespeicherten Daten kommen. Es wird empfohlen, den Neustart eines Dateiservers streng nach Zeitplan auszuführen. Aus diesem Grund ist die Technologie zur aktiven Desinfektion für Dateiserver standardmäßig deaktiviert.

Wird auf einem Dateiserver eine aktive Infektion erkannt, so wird ein Ereignis an Kaspersky Security Center gesendet, das über die Notwendigkeit einer „Aktiven Desinfektion“ informiert. Für die aktive Desinfektion einer Infektion auf einem Server, müssen Sie die Technologie zur „Aktiven Desinfektion“ für Server aktivieren und die Gruppenaufgabe *Schadsoftware-Untersuchung* starten. Dafür sollte ein Zeitpunkt gewählt werden, der für die Benutzer des Servers günstig ist.

Energiesparmodus aktivieren und deaktivieren

Der *Energiesparmodus* entlastet die Laptop-Ressourcen und verlängert die Akkulaufzeit, ohne die Sicherheitsstufe wesentlich zu beeinträchtigen. Im Energiesparmodus beschränkt die Anwendung den Start von geplanten Aufgaben. Dadurch sorgt der Energiesparmodus für ein ausgewogenes Verhältnis zwischen der Sicherheitsstufe und der Akkulaufzeit des Laptops.

Wenn der Energiesparmodus aktiviert ist und der Computer im Akkubetrieb läuft, werden die folgende Aufgaben auch dann nicht gestartet, wenn ein Startzeitplan vorhanden ist:

- *Vollständige Untersuchung*.
- *Untersuchung wichtiger Bereiche*.
- *Benutzerdefinierte Untersuchung*.
- *Prüfung der Anwendungsintegrität*.

- *IOC-Untersuchung*.
- *Update der Datenbanken und Programm-Module* (nur Patches)

Die Anwendung überspringt geplante Datenbanken-Updates nur dann, wenn der Laptop im Akkubetrieb läuft und der Akkuladestand unter 30 % liegt (Standardwert). Sie können den Mindestakkuladestand, ab dem die Anwendung geplante Updates der Antiviren-Datenbanken überspringt, durch Bearbeiten der Registrierung ändern (siehe Anleitung unten). In allen anderen Fällen aktualisiert Kaspersky Endpoint Security die Datenbanken nach Zeitplan, unabhängig davon, ob sich der Laptop im Netz- oder Akkubetrieb befindet oder ob die Anwendung im Energiesparmodus läuft.

So aktivieren oder deaktivieren Sie den Energiesparmodus (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
5. Verwenden Sie im Block **Leistung** das Kontrollkästchen **Geplante Aufgaben bei Akkubetrieb aufschieben**, um den Stromsparmodus zu aktivieren oder zu deaktivieren.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Energiesparmodus (in der Web Console)

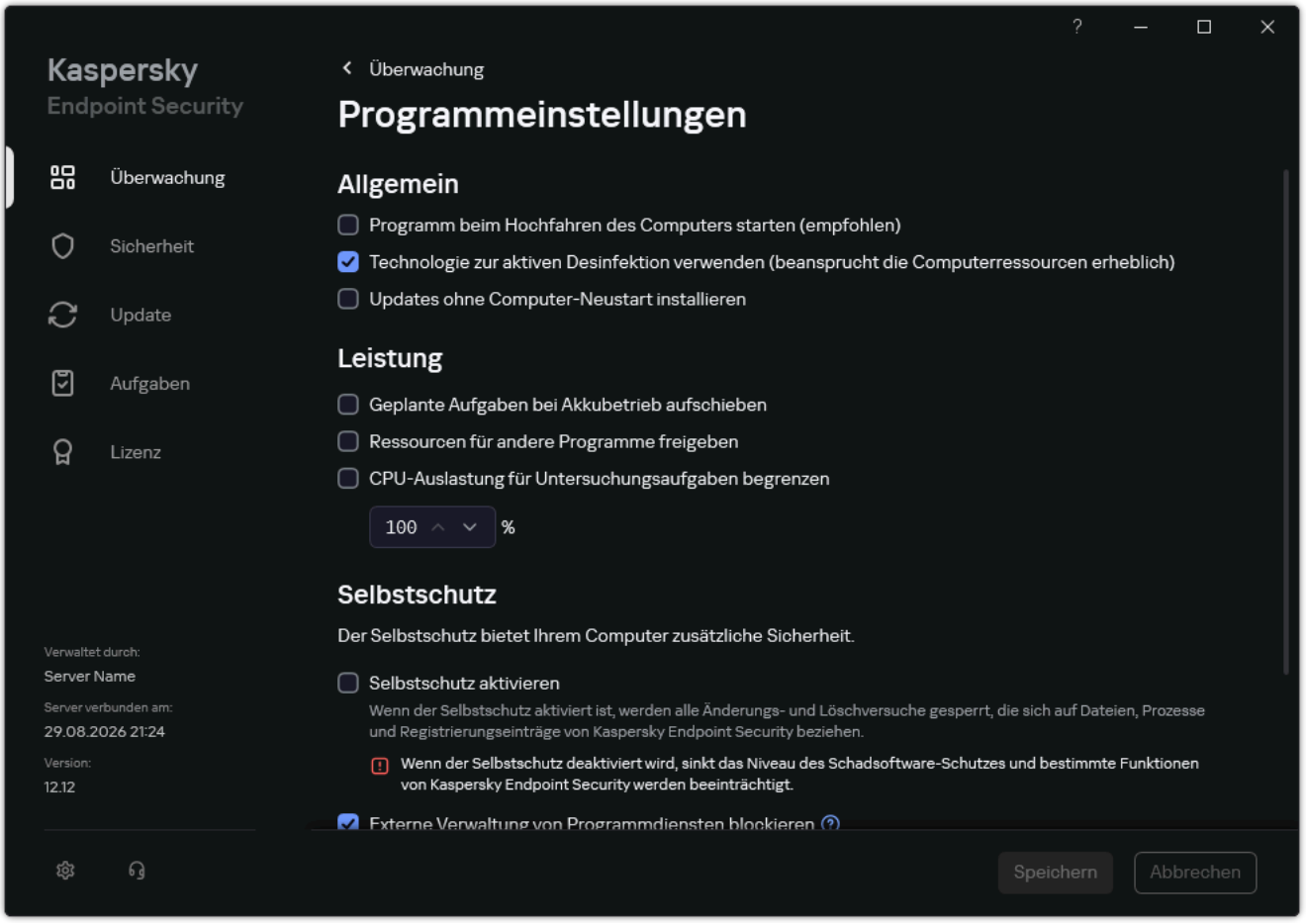
1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Leistung**.
5. Verwenden Sie im Block **Geplante Aufgaben bei Akkubetrieb aufschieben oder überspringen** das Kontrollkästchen **Geplante Aufgaben bei Akkubetrieb aufschieben oder überspringen (je nach Betriebssystem)**, um den Stromsparmodus zu aktivieren oder zu deaktivieren.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Energiesparmodus (in der Anwendungsoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Verwenden Sie im Block **Leistung** das Kontrollkästchen **Geplante Aufgaben bei Akkubetrieb aufschieben**, um den Stromsparmodus zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie den Mindestakkuladestand, ab dem die Anwendung geplante Updates der Antiviren-Datenbanken überspringt

1. Öffnen Sie den Registrierungseditor auf dem Computer.

2. Gehen Sie im Registrierungseditor zum folgenden Abschnitt:

   - Für 64-Bit-Betriebssysteme:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - Für 32-Bit-Betriebssysteme:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. Öffnen Sie `UpdaterAccumulatorThreshold` zur Bearbeitung.

4. Geben Sie den Mindestakkuladestand an, ab dem die Anwendung geplante Updates der Antiviren-Datenbanken überspringt.

Freigabe von Ressourcen für andere Programme aktivieren und deaktivieren

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.

So aktivieren oder deaktivieren Sie über die Verwaltungskonsole (MMC) die Zuweisung von Ressourcen an andere Programme

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
4. Verwenden Sie im Block **Leistung** das Kontrollkästchen **Ressourcen für andere Programme freigeben**, um die Zuweisung von Ressourcen an andere Programme zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie über die Web Console und Cloud Console die Zuweisung von Ressourcen an andere Programme

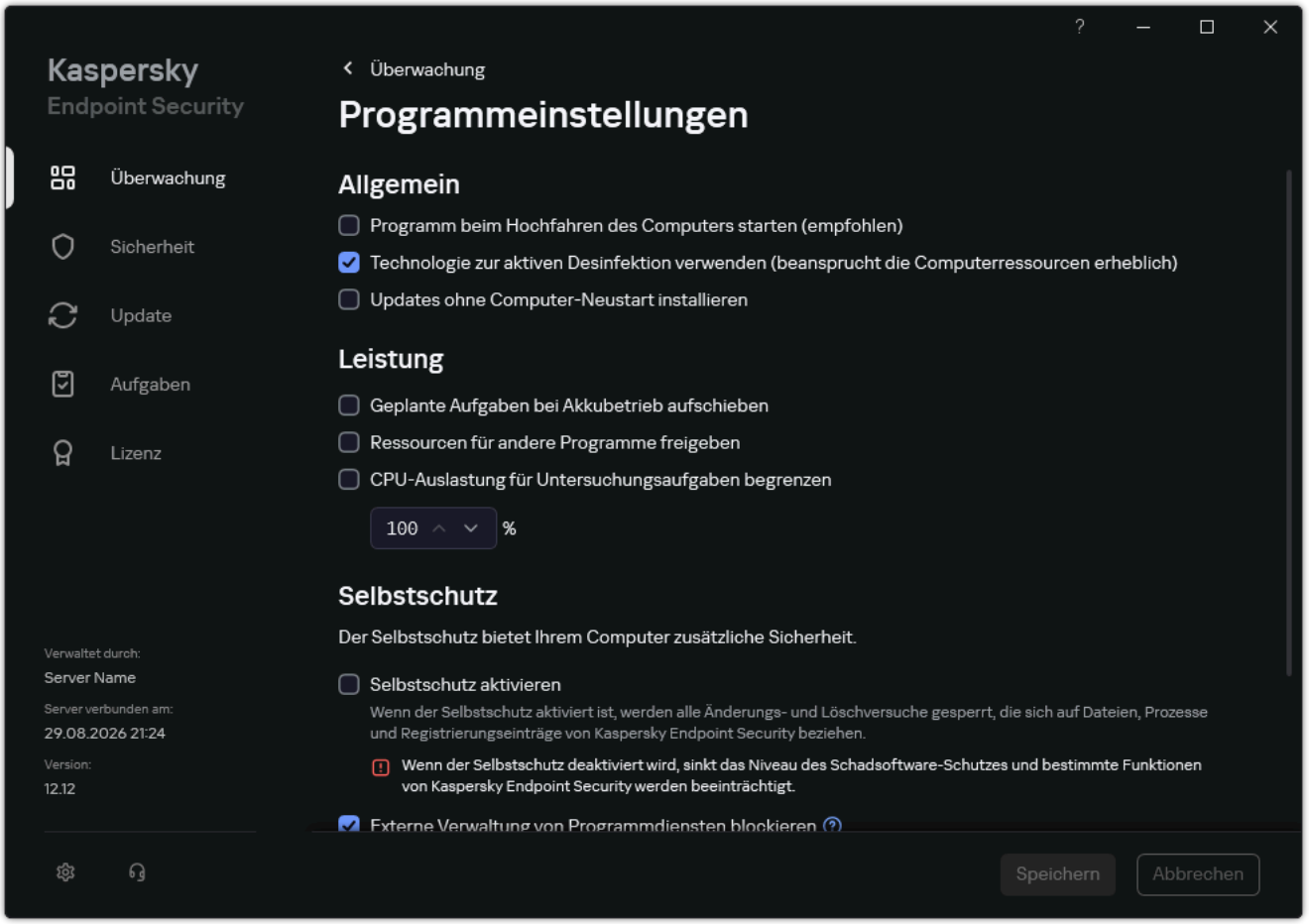
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Leistung**.
5. Verwenden Sie im Block **Ressourcen für andere Programme freigeben** den Schalter **Ressourcen für andere Programme freigeben**, um die Zuweisung von Ressourcen an andere Programme zu aktivieren bzw. zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren bzw. deaktivieren Sie über die App-Benutzeroberfläche die Zuweisung von Ressourcen an andere Programme

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Verwenden Sie im Block **Leistung** das Kontrollkästchen **Ressourcen für andere Programme freigeben**, um die Zuweisung von Ressourcen an andere Programme zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Bewährte Methoden zur Leistungsoptimierung von Kaspersky Endpoint Security

Hier finden Sie einige Tipps, mit denen Sie bei der Bereitstellung von Kaspersky Endpoint Security für Windows den Computerschutz anpassen und die Leistung optimieren können. Weitere Informationen zum Umfang mit Problemen bei der Computerleistung finden Sie in der Wissensdatenbank des Technischen Supports.

Allgemein

Konfigurieren Sie die allgemeinen Programmeinstellungen anhand der folgenden Tipps:

1. Aktualisieren Sie Kaspersky Endpoint Security auf die neueste Version.

   In neueren Versionen des Programms wurden Fehler behoben, die Stabilität verbessert und die Leistung optimiert.

2. Aktivieren Sie die Schutzkomponenten mit den Standardeinstellungen.

   Die Standardeinstellungen gelten als optimal. Diese Einstellungen werden von den Kaspersky-Experten empfohlen. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung. Bei Bedarf können Sie die standardmäßigen Programmeinstellungen wiederherstellen.

3. Aktivieren Sie die Funktionen zur Optimierung der Programmleistung.

   Das Programm bietet Funktionen zur Leistungsoptimierung: Energiesparmodus und Freigabe von Ressourcen für andere Programme. Stellen Sie sicher, dass diese Optionen aktiviert sind.

Schadsoftware-Untersuchung auf Workstations

Für eine Schadsoftware-Untersuchung auf Workstations sollte die Untersuchung im Hintergrund aktiviert werden. Die *Untersuchung im Hintergrund* ist ein Untersuchungsmodus 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. Die Einstellungen für die Untersuchung im Hintergrund gelten als optimal. Diese Einstellungen werden von den Kaspersky-Experten empfohlen. Um den Computer auf Schadsoftware zu untersuchen, können Sie also einfach die Untersuchung im Hintergrund verwenden, ohne andere Untersuchungsaufgaben auszuführen.

Wenn die Untersuchung im Hintergrund Ihren Anforderungen nicht entspricht, passen Sie die Aufgabe *Schadsoftware-Untersuchung* anhand der folgenden Tipps an:

1. Legen Sie ein Limit für die CPU-Ressourcen fest, die während der Untersuchung des Computers verbraucht werden dürfen.

   Sie können die CPU-Auslastung aufgrund der Aufgabe *Schadsoftware-Untersuchung* beschränken. Geben Sie dazu in den App-Einstellungen an, wie viel Prozent der CPU-Leistung für alle Kerne während der Untersuchung des Computers genutzt werden dürfen. Dadurch kann die Untersuchung Ihres Computers länger dauern.

2. Konfigurieren Sie einen optimalen Zeitplan für die Untersuchung des Computers.

   Sie können festlegen, dass die Aufgabe ausgeführt wird, wenn der Computer minimal ausgelastet ist. Sie können die Aufgabe beispielsweise so anpassen, dass sie nachts oder am Wochenende ausgeführt wird.

   Wenn Benutzer den Computer außerhalb der Geschäftszeiten ausschalten, können Sie die Wake-on-LAN-Funktion aktivieren. Mithilfe der Wake-on-LAN-Funktion kann der Computer aus der Ferne durch das Senden eines speziellen Signals über das lokale Netzwerk eingeschaltet werden. Um diese Funktion zu verwenden, müssen Sie Wake-on-LAN in den BIOS-Einstellungen aktivieren. Sie können auch festlegen, dass der Computer nach der Untersuchung automatisch ausschaltet.

Falls Sie keinen optimalen Untersuchungszeitplan erstellt haben, legen Sie fest, dass Aufgaben nur ausgeführt werden, wenn der Computer inaktiv ist. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde.

3. Legen Sie einen Untersuchungsbereich fest.

   Wählen Sie die folgenden Objekte für die Untersuchung aus (minimale Auswahl von Untersuchungsbereichen):

   - Kernel-Speicher
   - Laufende Prozesse und Autostart-Objekte
   - Bootsektoren
   - %systemroot% (ohne Unterordner)
   - %systemroot%\System (ohne Unterordner)
   - %systemroot%\System32 (ohne Unterordner)
   - %systemroot%\System32\drivers (ohne Unterordner)
   - %systemroot%\SysWOW64 (ohne Unterordner)
   - %systemroot%\SysWOW64\drivers (ohne Unterordner)

4. Aktivieren Sie die Technologien iSwift und iChecker.

   - iSwift-Technologie.

     Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

   - iChecker-Technologie.

     Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Sie können die Technologien iSwift und iChecker nur in der Verwaltungskonsole (MMC) und der Benutzeroberfläche von Kaspersky Endpoint Security aktivieren. Sie können diese Technologien nicht in der „Kaspersky Security Center Web Console“ aktivieren.

5. Deaktivieren Sie die Untersuchung von kennwortgeschützten Archiven.

   Wenn die Untersuchung von kennwortgeschützten Archiven aktiviert ist, wird vor der Archivuntersuchung das Kennwort abgefragt. Da empfohlen wird, die Aufgabe außerhalb der aktiven Nutzungszeiten auszuführen, kann der Benutzer das Kennwort nicht eingeben. Sie können kennwortgeschützte Archive manuell untersuchen.

6. Deaktivieren Sie den gleichzeitigen Start mehrerer Untersuchungsaufgaben.

   Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert.

Schadsoftware-Untersuchung auf den Servern

Konfigurieren Sie die Aufgabe *Schadsoftware-Untersuchung* anhand der folgenden Tipps:

1. Legen Sie ein Limit für die CPU-Ressourcen fest, die während der Untersuchung des Computers verbraucht werden dürfen.

   Sie können die CPU-Auslastung aufgrund der Aufgabe *Schadsoftware-Untersuchung* beschränken. Geben Sie dazu in den App-Einstellungen an, wie viel Prozent der CPU-Leistung für alle Kerne während der Untersuchung des Computers genutzt werden dürfen. Dadurch kann die Untersuchung Ihres Computers länger dauern.

2. Konfigurieren Sie einen optimalen Zeitplan für die Untersuchung des Computers.

   Sie können festlegen, dass die Aufgabe ausgeführt wird, wenn der Computer minimal ausgelastet ist. Sie können die Aufgabe beispielsweise so anpassen, dass sie nachts oder am Wochenende ausgeführt wird.

3. Aktivieren Sie die Technologien iSwift und iChecker.

   - iSwift-Technologie.

     Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

   - iChecker-Technologie.

     Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

   Sie können die Technologien iSwift und iChecker nur in der Verwaltungskonsole (MMC) und der Benutzeroberfläche von Kaspersky Endpoint Security aktivieren. Sie können diese Technologien nicht in der „Kaspersky Security Center Web Console“ aktivieren.

4. Deaktivieren Sie die Untersuchung von kennwortgeschützten Archiven.

   Wenn die Untersuchung von kennwortgeschützten Archiven aktiviert ist, wird vor der Archivuntersuchung das Kennwort abgefragt. Da empfohlen wird, die Aufgabe außerhalb der aktiven Nutzungszeiten auszuführen, kann der Benutzer das Kennwort nicht eingeben. Sie können kennwortgeschützte Archive manuell untersuchen.

5. Deaktivieren Sie den gleichzeitigen Start mehrerer Untersuchungsaufgaben.

   Kaspersky Endpoint Security reiht neue Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert.

Kaspersky Security Network

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Für den Empfang dieser Daten ist Kaspersky Security Network vorgesehen.

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. 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.

Ändern Sie die Einstellungen für Kaspersky Security Network anhand der folgenden Tipps:

1. Deaktivieren Sie den erweiterten KSN-Modus.

   Im *erweiterten KSN-Modus* überträgt Kaspersky Endpoint Security zusätzliche Daten an Kaspersky.

2. Konfigurieren Sie Kaspersky Private Security Network.

   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.

3. Aktivieren Sie den Cloud-Modus.

   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.

Schadsoftware-Untersuchung

Die Schadsoftware-Untersuchung ist ein wichtiger Faktor für die Gewährleistung der Computersicherheit. Schadsoftware-Untersuchungen sollten regelmäßig durchgeführt werden, um eine mögliche Ausbreitung von schädlichen Programmen auszuschließen, die von den Schutzkomponenten beispielsweise aufgrund einer zu niedrigen Schutzstufe nicht erkannt wurden.

Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, werden nicht durch Kaspersky Endpoint Security untersucht. Es werden aber Berichtseinträge darüber erstellt, dass diese Dateien nicht untersucht wurden.

Vollständige Untersuchung

Ausführliche Untersuchung des Systems. Kaspersky Endpoint Security untersucht folgende Objekte:

- Kernel-Speicher
- Objekte, die beim Hochfahren des Betriebssystems geladen werden
- Bootsektoren
- Backup des Betriebssystems
- alle Festplatten und Wechseldatenträger

Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgabe *Vollständige Untersuchung* zu ändern.

Um die Computerressourcen zu schonen, wird empfohlen, statt der Aufgabe zur vollständigen Untersuchung die Aufgabe zur Untersuchung im Hintergrund zu verwenden. Dabei bleibt das Niveau des Computerschutzes unverändert.

Untersuchung wichtiger Bereiche

Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden Prozesse und die Bootsektoren.

Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgabe *Untersuchung wichtiger Bereiche* zu ändern.

Benutzerdefinierte Untersuchung

Kaspersky Endpoint Security untersucht die vom Benutzer ausgewählten Objekte. Sie können ein beliebiges Objekt aus der folgenden Liste untersuchen:

- Systemspeicher
- Objekte, die beim Hochfahren des Betriebssystems geladen werden
- Backup des Betriebssystems
- Festplatten, Wechseldatenträger und Netzlaufwerke
- Eine beliebige ausgewählte Datei

Untersuchung im Hintergrund

Die *Untersuchung im Hintergrund* ist ein Untersuchungsmodus 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.

Prüfung der Anwendungsintegrität

Kaspersky Endpoint Security überprüft, ob die Programm-Module Beschädigungen oder Änderungen aufweisen.

Untersuchung des Computers

Die Untersuchung ist ein wichtiger Faktor für die Gewährleistung der Computersicherheit. Schadsoftware-Untersuchungen sollten regelmäßig durchgeführt werden, um eine mögliche Ausbreitung von schädlichen Programmen auszuschließen, die von den Schutzkomponenten beispielsweise aufgrund einer zu niedrigen Schutzstufe nicht erkannt wurden. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

In Kaspersky Endpoint Security gibt es die folgenden vordefinierten Standardaufgaben: *Vollständige Untersuchung*, *Untersuchung wichtiger Bereiche*, *Benutzerdefinierte Untersuchung*. Wenn in Ihrem Unternehmen das Administrationssystem von Kaspersky Security Center bereitgestellt wurde, können Sie eine *Schadsoftware-Untersuchung* erstellen und die Untersuchung anpassen.

So führen Sie eine Untersuchungsaufgabe in der Verwaltungskonsole (MMC) aus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Wählen Sie die Untersuchungsaufgabe aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.

   Erstellen Sie bei Bedarf die Aufgabe *Schadsoftware-Untersuchung*.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
5. Passen Sie die Untersuchungsaufgabe an (siehe Tabelle unten).

   Passen Sie erforderlichenfalls den Zeitplan für die Untersuchungsaufgabe an.
6. Speichern Sie die vorgenommenen Änderungen.
7. Starten Sie die Untersuchungsaufgabe.

Kaspersky Endpoint Security beginnt mit der Untersuchung des Computers. Wenn der Benutzer die Aufgabenausführung unterbrochen hat, z. B. durch das Ausschalten des Computers, führt Kaspersky Endpoint Security die Untersuchung automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde.

So führen Sie eine Untersuchungsaufgabe in der Web Console aus

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Passen Sie die Untersuchungsaufgabe an (siehe Tabelle unten).

   Passen Sie erforderlichenfalls den Zeitplan für die Untersuchungsaufgabe an.
5. Speichern Sie die vorgenommenen Änderungen.
6. Starten Sie die Untersuchungsaufgabe.

Kaspersky Endpoint Security beginnt mit der Untersuchung des Computers. Wenn der Benutzer die Aufgabenausführung unterbrochen hat, z. B. durch das Ausschalten des Computers, führt Kaspersky Endpoint Security die Untersuchung automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde.

So führen Sie eine Untersuchungsaufgabe in der Programmoberfläche aus

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.
2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.

Wird die Untersuchungsaufgabe nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

In der Programmoberfläche können Sie nur lokale Untersuchungsaufgaben konfigurieren: *Vollständige Untersuchung*, *Untersuchung wichtiger Bereiche*, *Benutzerdefinierte Untersuchung*. Gruppenaufgaben, die über die Konsole von Kaspersky Security Center hinzugefügt wurden, können nicht in der Programmoberfläche konfiguriert werden. Die Schaltfläche ⚙ wird für Gruppenaufgaben nicht angezeigt.

3. Passen Sie die Untersuchungsaufgabe an (siehe Tabelle unten).

   Passen Sie erforderlichenfalls den Zeitplan für die Untersuchungsaufgabe an.

4. Speichern Sie die vorgenommenen Änderungen.

5. Starten Sie die Untersuchungsaufgabe.

   Kaspersky Endpoint Security beginnt mit der Untersuchung des Computers. Das Programm zeigt den Untersuchungsfortschritt, die Anzahl der untersuchten Dateien und die verbleibende Untersuchungszeit an. Sie können die Aufgabe jederzeit beenden, indem Sie auf die Schaltfläche **Abbrechen** klicken.

Um die Leistung von Kaspersky Endpoint Security für die Computeruntersuchung zu optimieren, können Sie die erweiterten Einstellungen der Aufgabe *Vollständige Untersuchung* anpassen und die Auslastung der CPU-Ressourcen begrenzen.

In Kaspersky Security Center können Sie auch die Aufgabe *Untersuchung im Hintergrund* verwenden (anstelle der Aufgabe *Vollständige Untersuchung*), um die Leistung des Programms zu optimieren. Dabei bleibt das Niveau des Computerschutzes unverändert. Die Untersuchung im Hintergrund kann nicht angepasst werden.

Als Ergebnis untersucht Kaspersky Endpoint Security den Computer und führt bei Erkennung einer Bedrohung die in den App-Einstellungen festgelegte Aktion aus. Normalerweise versucht die App, infizierte Dateien zu desinfizieren. Infizierte Dateien können dabei die folgenden Status erhalten:

- **Zurückgestellt**. Die infizierte Datei konnte nicht desinfiziert werden. Die App löscht die infizierte Datei nach dem Neustart des Computers.
- **Protokolliert**. Die infizierte Datei konnte nicht desinfiziert werden. Die App fügt Informationen über erkannte infizierte Dateien zur Liste der aktiven Bedrohungen hinzu.
- **Schreiben wird nicht unterstützt** oder **Schreibfehler**. Die infizierte Datei konnte nicht desinfiziert werden. Die App hat keinen Schreibzugriff.
- **Bereits verarbeitet**. Die App hat zuvor eine infizierte Datei erkannt. Die App desinfiziert oder löscht die infizierte Datei nach dem Neustart des Computers.

Einstellung	Beschreibung
Sicherheitsstufe	Kaspersky Endpoint Security kann verschiedene Gruppen von Einstellungen für die Ausführung einer Untersuchung verwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Kaspersky Endpoint Security untersucht alle Dateitypen. Bei der Untersuchung zusammengesetzter Dateien untersucht das Programm Archive, Programmpakete und Dateien in Office-Formaten. Kennwortgeschützte Archive werden jedoch nicht untersucht. Wenn diese Sicherheitsstufe festgelegt ist, verwendet das Programm die heuristische Analyse mit der Genauigkeitsstufe **Tief**. • **Empfohlen**. Kaspersky Endpoint Security untersucht alle Dateitypen. Bei der Untersuchung zusammengesetzter Dateien untersucht das Programm Archive, Programmpakete und Dateien in Office-Formaten. Kennwortgeschützte Archive werden jedoch nicht untersucht. Wenn diese Sicherheitsstufe festgelegt ist, verwendet das Programm die heuristische Analyse mit der Genauigkeitsstufe **Mittel**. • **Niedrig**. Kaspersky Endpoint Security untersucht nur die angegebenen Dateiformate. Bei der Untersuchung zusammengesetzter Dateien untersucht das Programm Archive, Programmpakete und Dateien in Office-Formaten. Kennwortgeschützte Archive werden jedoch nicht untersucht. Wenn diese Sicherheitsstufe festgelegt ist, verwendet das Programm die heuristische Analyse mit der Genauigkeitsstufe **Oberflächlich**. Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.
Aktion beim Fund einer Bedrohung	**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 – Informieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Wenn die Desinfektion fehlschlägt, fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu. **Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu. Bevor versucht wird, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann. Beim Fund infizierter Dateien, die Teile einer App aus dem Windows Store sind, versucht Kaspersky Endpoint Security, die Datei zu löschen.
Aktive Desinfektion sofort ausführen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Wenn auf dem Computer eine Untersuchungsaufgabe ausgeführt wird, erfolgt nur dann eine aktive Desinfektion, wenn in den Eigenschaften der Richtlinie, die für diesen Computer gilt, die Aktive Desinfektion aktiviert ist. Wenn das Kontrollkästchen aktiviert ist, desinfiziert Kaspersky Endpoint Security die aktive Infektion sofort, nachdem diese während einer Untersuchungsaufgabe erkannt wurde. Nachdem die aktive Infektion desinfiziert wurde, startet Kaspersky Endpoint Security den Computer neu, ohne den Benutzer zuvor zu benachrichtigen. Wenn das Kontrollkästchen deaktiviert ist, desinfiziert Kaspersky Endpoint Security die aktive Infektion nicht sofort, nachdem diese während einer Untersuchungsaufgabe erkannt wurde. Kaspersky Endpoint Security generiert Ereignisse über aktive Infektionen in lokalen Programmberichten und in Kaspersky Security Center. In diesem Fall kann die aktive Infektion desinfiziert werden, wenn die Untersuchungsaufgabe erneut ausgeführt wird und dabei die Funktion „Aktive Desinfektion“ aktiviert ist. Auf diese Weise kann der Systemadministrator einen geeigneten Zeitpunkt für die „Aktive Desinfektion“ und den anschließenden automatischen Neustart des Computers wählen.

Einstellung	Beschreibung
Untersuchungsbereich	Liste der Objekte, die im Rahmen einer Untersuchungsaufgabe von Kaspersky Endpoint Security untersucht werden. Zu den Objekten innerhalb des Untersuchungsbereichs können der Kernel-Speicher, laufende Prozesse, Bootsektoren, System-Backup-Speicher, Festplatte, Wechseldatenträger oder Netzlaufwerk, Ordner oder Datei gehören. In Kaspersky Endpoint Security für Windows 12.12 sind E-Mail-Nachrichten aus dem Untersuchungsbereich des Programms ausgeschlossen. Die Untersuchung ein- und ausgehender E-Mail-Nachrichten wird von der Komponente „Schutz vor E-Mail-Bedrohungen“ ausgeführt. Wenn Sie eine ältere Version des Verwaltungs-Plug-ins verwenden, schließt das Programm E-Mail-Nachrichten aus dem Untersuchungsbereich aus, selbst wenn diese durch die Richtlinie eingeschlossen werden.
Untersuchungszeitplan	**Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. **Nach Zeitplan**. In diesem Startmodus für die Untersuchungsaufgabe führt das Programm die Untersuchungsaufgabe nach dem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Untersuchungsaufgabe können Sie die Untersuchungsaufgabe auch manuell starten.
Ausführung nach Programmstart aufschieben für n Minuten	Der Start der Untersuchungsaufgabe wird nach dem Programmstart aufgeschoben. Da beim Start des Betriebssystems viele Prozesse ausgeführt werden, ist es vorteilhaft, die Untersuchungsaufgabe aufzuschieben, anstatt sie sofort nach dem Start von Kaspersky Endpoint Security auszuführen.
Übersprungene Aufgaben ausführen	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security die übersprungene Aufgabe, sobald dies möglich ist. Die Aufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Aufgabe ausgeschaltet war. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen. Wenn dieses Kontrollkästchen deaktiviert ist, führt Kaspersky Endpoint Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Nur ausführen, wenn der Computer inaktiv ist	Schiebt den Start der Aufgabe auf, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde. Mit dieser Zeitplanoption können Sie die Computerressourcen schonen, während der Computer verwendet wird.
Untersuchung ausführen als	Standardmäßig wird die Untersuchungsaufgabe im Namen des Benutzers ausgeführt, mit dessen Rechten Sie im Betriebssystem registriert sind. Der Schutzbereich kann Netzlaufwerke und andere Objekte enthalten, die besondere Zugriffsrechte erfordern. Sie können in den Programmeinstellungen einen Benutzer angeben, der über die erforderlichen Rechte verfügt, und die Untersuchungsaufgabe unter dem Konto dieses Benutzers ausführen.
Dateitypen	Dateien ohne Erweiterung werden von Kaspersky Endpoint Security als ausführbar betrachtet. Ausführbare Dateien werden vom Programm immer untersucht, unabhängig davon, welchen Dateityp Sie für die Untersuchung ausgewählt haben. **Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). **Dateien nach Format untersuchen**. 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. **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt. Kaspersky Endpoint Security untersucht Dateien standardmäßig aufgrund ihres Formats. Eine Untersuchung von Dateien nach deren Erweiterung ist weniger sicher, denn eine bösartige Datei kann auch eine Erweiterung haben, die nicht als potenziell infizierbar gelistet ist (z. B. `.123`).
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.
Datei überspringen, wenn Untersuchung länger dauert als n Sekunde(n)	Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

Einstellung	Beschreibung
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Sie haben beispielsweise die Ausführung von Untersuchungsaufgaben für 18:00 und 20:00 Uhr geplant. Kaspersky Endpoint Security verschiebt die für 20:00 Uhr geplante Untersuchungsaufgabe, wenn die für 18:00 Uhr geplante Untersuchungsaufgabe noch ausgeführt wird. Das Programm führt die verschobene Untersuchung durch, sobald die um 18:00 Uhr gestartete Aufgabe abgeschlossen ist. Eine Untersuchungsaufgabe wird aber sofort gestartet, auch wenn eine der folgenden Untersuchungsaufgaben bereits ausgeführt wird: • Wechseldatenträger beim Anschließen untersuchen. • Untersuchung aus dem Kontextmenü. • Untersuchung wichtiger Bereiche, die aufgrund der Erkennung eines Kompromittierungsindikators (IoC) gestartet wurde. Wenn dieses Kontrollkästchen deaktiviert ist, erlaubt Kaspersky Endpoint Security den gleichzeitigen Start mehrere Untersuchungsaufgaben. Die Ausführung mehrere Untersuchungsaufgaben erfordert mehr Computerressourcen.
Archive untersuchen	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Programmpakete untersuchen	Verteilungspakete für Drittanbieter-Programme untersuchen.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Dateien in E-Mail-Formaten untersuchen	Untersuchung von Dateien E-Mail-Formaten und E-Mail-Datenbanken. Die App untersucht PST- und OST-Dateien, die von den Mail-Clients MS Outlook und Windows Mail verwendet werden, sowie auch EML-Dateien. Kaspersky Endpoint Security unterstützt die 64-Bit-Version des E-Mail-Clients Microsoft Outlook nicht. Das bedeutet: Kaspersky Endpoint Security untersucht Microsoft Outlook-Dateien (PST- und OST-Dateien) nicht, wenn eine 64-Bit-Version von Microsoft Outlook auf dem Computer installiert ist. Dies gilt auch, wenn E-Mails zum Untersuchungsbereich gehören. Ist dieses Kontrollkästchen aktiviert, zerlegt Kaspersky Endpoint Security die Mailformat-Datei und untersucht die einzelnen Komponenten (Kopfzeile, Text, Anhänge) auf Bedrohungen. Ist dieses Kontrollkästchen deaktiviert, untersucht Kaspersky Endpoint Security die Mailformat-Datei wie eine einzelne Datei. Beim Fund eines schädlichen Objekts in pst- oder ost-Dateien führt Kaspersky Endpoint Security die ausgewählte Aktion damit aus (z. B. Datei desinfizieren oder löschen). Wenn in Dateien anderer E-Mail-Clients (z. B. Mozilla Thunderbird) schädliche Objekte erkannt werden, desinfiziert oder löscht Kaspersky Endpoint Security diese Dateien nicht, um zu verhindern, dass Ihre E-Mail-Nachrichten unbeabsichtigt gelöscht werden. Kaspersky Endpoint Security fügt nur Informationen über erkannte Objekte zur Liste der aktiven Bedrohungen hinzu. Sie müssen in der Benutzeroberfläche Ihres E-Mail-Clients Maßnahmen ergreifen, um E-Mails mit schädlichen Dateien in Anhängen zu löschen. Wenn das Löschen von Nachrichten mit schädlichen Objekten derzeit aus irgendeinem Grund nicht möglich ist, können Sie solche Bedrohungen in der Benutzeroberfläche von Kaspersky Endpoint Security verarbeiten, indem Sie die erkannten Objekte zur Liste der Untersuchungsausnahmen hinzufügen.
Kennwortgeschützte Archive untersuchen	Ist dieses Kontrollkästchen aktiviert, werden kennwortgeschützte Archive vom Programm untersucht. Dabei erfolgt eine Kennwortabfrage, bevor Dateien untersucht werden, die in einem Archiv enthalten sind. Ist dieses Kontrollkästchen deaktiviert, werden kennwortgeschützte Archive bei der Untersuchung vom Programm übersprungen.
Große zusammengesetzte Dateien nicht entpacken	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.

Einstellung	Beschreibung
Machine Learning und Signaturanalyse	Bei der Untersuchungsmethode Maschinelles Lernen und Signaturanalyse werden die Datenbanken von Kaspersky Endpoint Security verwendet, die Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Die Verwendung dieser Untersuchungsmethode gewährleistet die minimal zulässige Sicherheitsstufe. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.
Heuristische Analyse	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
iSwift-Technologie *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Wechseldatenträger beim Anschließen an den Computer untersuchen

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. Außerdem verwendet Kaspersky Endpoint Security zur Untersuchungsoptimierung die Technologien iSwift und iChecker. Diese Technologien sind immer aktiviert und können nicht deaktiviert werden.

So konfigurieren Sie die Ausführung der Untersuchung von Wechseldatenträgern über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Lokale Aufgaben → Untersuchung von Wechseldatenträgern** aus.
4. Wählen Sie in der Dropdown-Liste **Aktion bei Verbindung eines Wechseldatenträgers** die Variante **Genaue Untersuchung** oder **Schnelle Untersuchung**.

5. Konfigurieren Sie die erweiterten Optionen für die Untersuchung von Wechseldatenträgern (siehe Tabelle unten).

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Ausführung der Untersuchung von Wechseldatenträgern über die „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Untersuchung von Wechseldatenträgern**.

5. Verwenden Sie den Schalter **Untersuchung von Wechseldatenträgern AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Wählen Sie im Block **Untersuchungstyp** den Punkt **Genaue Untersuchung** oder **Schnelle Untersuchung** aus.

7. Konfigurieren Sie die erweiterten Optionen für die Untersuchung von Wechseldatenträgern (siehe Tabelle unten).

8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Ausführung der Untersuchung von Wechseldatenträgern über die Programmoberfläche

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.

2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.

3. Verwenden Sie den Schalter für die **Untersuchung von Wechseldatenträgern**, um die Untersuchung von Wechseldatenträgern beim Anschließen an den Computer zu aktivieren oder zu deaktivieren.

4. Konfigurieren Sie die erweiterten Optionen für die Untersuchung von Wechseldatenträgern (siehe Tabelle unten).

5. Speichern Sie die vorgenommenen Änderungen.

Künftig führt Kaspersky Endpoint Security eine Untersuchung von Wechseldatenträgern für jene Wechseldatenträger durch, die die angegebene maximale Größe nicht überschreiten. Wird die Aufgabe *Untersuchung von Wechseldatenträgern* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Einstellungen für die Aufgabe „Untersuchung von Wechseldatenträgern"

Einstellung	Beschreibung
Untersuchungstyp	**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. **Schnelle Untersuchung**. Wenn diese Option ausgewählt ist, 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.
Maximale Datenträgergröße (MB)	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.
Untersuchungsfortschritt ausblenden	Ist dieses Kontrollkästchen aktiviert, so zeigt Kaspersky Endpoint Security den Fortschritt der Untersuchung von Wechseldatenträgern in einem separaten Fenster sowie im Abschnitt **Aufgaben** an. Ist das Kontrollkästchen deaktiviert, so führt Kaspersky Endpoint Security die Untersuchung von Wechseldatenträgern im Hintergrundmodus aus.
Benutzern das Anhalten der Untersuchung verbieten	Ist dieses Kontrollkästchen aktiviert, so sind für die Aufgabe zur Wechseldatenträger-Untersuchung auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security die **Abbrechen**-Schaltfläche im Abschnitt **Aufgaben** und die **Abbrechen**-Schaltfläche im Fenster für die Wechseldatenträger-Untersuchung nicht verfügbar.

Untersuchung im Hintergrund

Die *Untersuchung im Hintergrund* ist ein Untersuchungsmodus 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.

Um die Computerressourcen zu schonen, wird empfohlen, statt der Aufgabe zur vollständigen Untersuchung die Aufgabe zur Untersuchung im Hintergrund zu verwenden. Dabei bleibt das Niveau des Computerschutzes unverändert. Diese Aufgaben haben den gleichen Untersuchungsbereich. Um die Auslastung des Computers zu optimieren, führt das Programm die Aufgaben „Vollständige Untersuchung" und „Untersuchung im Hintergrund" nicht gleichzeitig aus. Wenn Sie bereits eine Aufgabe zur vollständigen Untersuchung ausgeführt haben, führt Kaspersky Endpoint Security nach deren Abschluss sieben Tage lang keine Untersuchungsaufgabe im Hintergrund mehr aus.

Die Untersuchung im Hintergrund wird in folgenden Fällen gestartet:

- nach dem Update der Antiviren-Datenbanken
- 30 Minuten nach dem Start von Kaspersky Endpoint Security
- alle sechs Stunden
- Wenn der Computer für fünf Minuten oder länger im Leerlauf ist (der Computer ist gesperrt oder der Bildschirmschoner ist eingeschaltet).

Die Hintergrunduntersuchung bei Inaktivität des Computers wird unterbrochen, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Computer hat in den aktiven Modus gewechselt.

  Wenn die Untersuchung im Hintergrund seit über zehn Tagen nicht mehr ausgeführt wurde, wird die Untersuchung nicht unterbrochen.

- Der Computer (das Notebook) hat in den Batteriebetrieb gewechselt.

Wenn die Aufgabe „Hintergrunduntersuchung“ ausgeführt wird, werden Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, nicht von Kaspersky Endpoint Security untersucht.

So aktivieren Sie die Untersuchung im Hintergrund über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Lokale Aufgaben** → **Untersuchung im Hintergrund** aus.
4. Verwenden Sie das Kontrollkästchen **Untersuchung im Hintergrund aktivieren**, um die Untersuchung im Hintergrund zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Untersuchung im Hintergrund über die „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Verwenden Sie unter **Untersuchung im Hintergrund** den Schalter **Untersuchung im Hintergrund AKTIVIERT**, um die Untersuchung im Hintergrund zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Untersuchung im Hintergrund über der Programmoberfläche

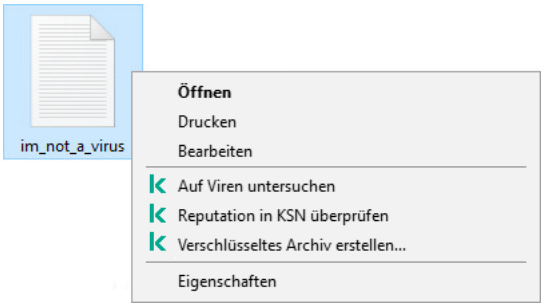
1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.
2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.
3. Verwenden Sie den Schalter **Untersuchung im Hintergrund**, um die Untersuchung im Hintergrund zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wird die *Untersuchung im Hintergrund* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Untersuchung aus dem Kontextmenü

Kaspersky Endpoint Security bietet die Möglichkeit, aus dem Kontextmenü bestimmte Dateien auf Viren und andere bedrohliche Programme zu untersuchen (s. folgende Abb.).

Wenn eine Untersuchung aus dem Kontextmenü ausgeführt wird, werden Dateien, deren Inhalt sich im Cloud-Speicher OneDrive befindet, nicht von Kaspersky Endpoint Security untersucht.



Untersuchung aus dem Kontextmenü

So konfigurieren Sie die Untersuchung aus dem Kontextmenü über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Lokale Aufgaben** → **Untersuchung aus dem Kontextmenü** aus.
4. Passen Sie die Untersuchung aus dem Kontextmenü an (siehe Tabelle unten).
5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung aus dem Kontextmenü über die „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Konfigurieren Sie unter **Untersuchung aus dem Kontextmenü** die Untersuchung aus dem Kontextmenü (siehe folgende Tabelle).
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung aus dem Kontextmenü über die Programmoberfläche

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.
2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.
3. Passen Sie die Untersuchung aus dem Kontextmenü an (siehe Tabelle unten).
4. Speichern Sie die vorgenommenen Änderungen.

Wird die Aufgabe *Untersuchung aus dem Kontextmenü* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Einstellungen für die Aufgabe „Untersuchung aus dem Kontextmenü"

Einstellung	Beschreibung
Sicherheitsstufe	Kaspersky Endpoint Security kann verschiedene Gruppen von Einstellungen für die Ausführung einer Untersuchung verwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Kaspersky Endpoint Security untersucht alle Dateitypen. Bei der Untersuchung zusammengesetzter Dateien untersucht das Programm Archive, Programmpakete und Dateien in Office-Formaten. Kennwortgeschützte Archive werden jedoch nicht untersucht. Wenn diese Sicherheitsstufe festgelegt ist, verwendet das Programm die heuristische Analyse mit der Genauigkeitsstufe **Tief**. • **Empfohlen**. Kaspersky Endpoint Security untersucht alle Dateitypen. Bei der Untersuchung zusammengesetzter Dateien untersucht das Programm Archive, Programmpakete und Dateien in Office-Formaten. Kennwortgeschützte Archive werden jedoch nicht untersucht. Wenn diese Sicherheitsstufe festgelegt ist, verwendet das Programm die heuristische Analyse mit der Genauigkeitsstufe **Mittel**. • **Niedrig**. Kaspersky Endpoint Security untersucht nur die angegebenen Dateiformate. Bei der Untersuchung zusammengesetzter Dateien untersucht das Programm Archive, Programmpakete und Dateien in Office-Formaten. Kennwortgeschützte Archive werden jedoch nicht untersucht. Wenn diese Sicherheitsstufe festgelegt ist, verwendet das Programm die heuristische Analyse mit der Genauigkeitsstufe **Oberflächlich**.
Aktion beim Fund einer Bedrohung	**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 – Informieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Wenn die Desinfektion fehlschlägt, fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu. **Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.
Dateitypen	Dateien ohne Erweiterung werden von Kaspersky Endpoint Security als ausführbar betrachtet. Ausführbare Dateien werden vom Programm immer untersucht, unabhängig davon, welchen Dateityp Sie für die Untersuchung ausgewählt haben. **Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). **Dateien nach Format untersuchen**. 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. **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt. Kaspersky Endpoint Security untersucht Dateien standardmäßig aufgrund ihres Formats. Eine Untersuchung von Dateien nach deren Erweiterung ist weniger sicher, denn eine bösartige Datei kann auch eine Erweiterung haben, die nicht als potenziell infizierbar gelistet ist (z. B. `.123`).
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.
Datei überspringen, wenn Untersuchung länger dauert als n Sekunde(n)	Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

Einstellung	Beschreibung
Archive untersuchen	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Programmpakete untersuchen	Dieses Kontrollkästchen aktiviert/deaktiviert die Untersuchung von Programmpaketen.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Dateien in E-Mail-Formaten untersuchen	Untersuchung von Dateien E-Mail-Formaten und E-Mail-Datenbanken. Die App untersucht PST- und OST-Dateien, die von den Mail-Clients MS Outlook und Windows Mail verwendet werden, sowie auch EML-Dateien. Kaspersky Endpoint Security unterstützt die 64-Bit-Version des E-Mail-Clients Microsoft Outlook nicht. Das bedeutet: Kaspersky Endpoint Security untersucht Microsoft Outlook-Dateien (PST- und OST-Dateien) nicht, wenn eine 64-Bit-Version von Microsoft Outlook auf dem Computer installiert ist. Dies gilt auch, wenn E-Mails zum Untersuchungsbereich gehören. Ist dieses Kontrollkästchen aktiviert, zerlegt Kaspersky Endpoint Security die Mailformat-Datei und untersucht die einzelnen Komponenten (Kopfzeile, Text, Anhänge) auf Bedrohungen. Ist dieses Kontrollkästchen deaktiviert, untersucht Kaspersky Endpoint Security die Mailformat-Datei wie eine einzelne Datei. Beim Fund eines schädlichen Objekts in pst- oder ost-Dateien führt Kaspersky Endpoint Security die ausgewählte Aktion damit aus (z. B. Datei desinfizieren oder löschen). Wenn in Dateien anderer E-Mail-Clients (z. B. Mozilla Thunderbird) schädliche Objekte erkannt werden, desinfiziert oder löscht Kaspersky Endpoint Security diese Dateien nicht, um zu verhindern, dass Ihre E-Mail-Nachrichten unbeabsichtigt gelöscht werden. Kaspersky Endpoint Security fügt nur Informationen über erkannte Objekte zur Liste der aktiven Bedrohungen hinzu. Sie müssen in der Benutzeroberfläche Ihres E-Mail-Clients Maßnahmen ergreifen, um E-Mails mit schädlichen Dateien in Anhängen zu löschen. Wenn das Löschen von Nachrichten mit schädlichen Objekten derzeit aus irgendeinem Grund nicht möglich ist, können Sie solche Bedrohungen in der Benutzeroberfläche von Kaspersky Endpoint Security verarbeiten, indem Sie die erkannten Objekte zur Liste der Untersuchungsausnahmen hinzufügen.
Kennwortgeschützte Archive untersuchen	Ist dieses Kontrollkästchen aktiviert, werden kennwortgeschützte Archive vom Programm untersucht. Dabei erfolgt eine Kennwortabfrage, bevor Dateien untersucht werden, die in einem Archiv enthalten sind. Ist dieses Kontrollkästchen deaktiviert, werden kennwortgeschützte Archive bei der Untersuchung vom Programm übersprungen.
Große zusammengesetzte Dateien nicht entpacken	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.
Machine Learning und Signaturanalyse	Bei der Untersuchungsmethode Maschinelles Lernen und Signaturanalyse werden die Datenbanken von Kaspersky Endpoint Security verwendet, die Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Die Verwendung dieser Untersuchungsmethode gewährleistet die minimal zulässige Sicherheitsstufe. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.
Heuristische Analyse	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.

Einstellung	Beschreibung
iSwift-Technologie	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Integritätsprüfung für Anwendungen

Kaspersky Endpoint Security überprüft, ob die Programm-Module Beschädigungen oder Änderungen aufweisen. Beispiel: Besitzt eine Programmbibliothek eine inkorrekte digitale Signatur, so gilt diese Bibliothek als beschädigt. Zur Untersuchung von Programmdateien dient die Aufgabe *Prüfung der Anwendungsintegrität*. Starten Sie die Aufgabe *Prüfung der Anwendungsintegrität*, wenn Kaspersky Endpoint Security ein schädliches Objekt gefunden hat, dieses aber nicht neutralisiert wurde.

Die Aufgabe *Prüfung der Anwendungsintegrität* können Sie in der Kaspersky Security Center Web Console und über die Verwaltungskonsole erstellen. Diese Aufgabe kann nicht im Programm Kaspersky Security Center Cloud Console erstellt werden.

Verletzungen der Programm-Integrität können beispielsweise in den folgenden Fällen auftreten:

- Ein schädliches Objekt hat die Dateien von Kaspersky Endpoint Security verändert. In diesem Fall führen Sie den Vorgang zur Wiederherstellung von Kaspersky Endpoint Security mit Betriebssystemmitteln aus. Starten Sie nach der Wiederherstellung eine vollständige Untersuchung des Computers und wiederholen Sie die Integritätsprüfung.
- Die digitale Signatur ist abgelaufen. In diesem Fall aktualisieren Sie Kaspersky Endpoint Security.

So führen Sie eine Integritätsprüfung des Programms über die Verwaltungskonsole (MMC) durch

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

   Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Prüfung der Anwendungsintegrität** aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Zeitplan des Aufgabenstarts anpassen

Passen Sie den Zeitplan des Aufgabenstarts an, z. B. manuell oder beim Erkennen eines Virenangriffs.

Schritt 4. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen an, beispielsweise *Integritätsprüfung für das Programm nach einer Computerinfektion*.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch führt Kaspersky Endpoint Security eine Integritätsprüfung des Programms aus. Außerdem können Sie in den Aufgabeneigenschaften einen Zeitplan für die Integritätsprüfung von Programmen einrichten (siehe Tabelle unten).

So führen Sie eine Integritätsprüfung eines Programms über die Web Console durch

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Prüfung der Anwendungsintegrität**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *App-Integritätsprüfung nach Computerinfektion*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

Dadurch führt Kaspersky Endpoint Security eine Integritätsprüfung des Programms aus. Außerdem können Sie in den Aufgabeneigenschaften einen Zeitplan für die Integritätsprüfung von Programmen einrichten (siehe Tabelle unten).

So führen Sie eine Integritätsprüfung über die Programmoberfläche aus

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Prüfung der Anwendungsintegrität* aus und klicken Sie auf **Starten**.

Dadurch führt Kaspersky Endpoint Security eine Integritätsprüfung des Programms aus. Außerdem können Sie in den Aufgabeneigenschaften einen Zeitplan für die Integritätsprüfung von Programmen einrichten (siehe Tabelle unten). Wird die Aufgabe *Prüfung der Anwendungsintegrität* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Einstellungen für Integritätsprüfungsaufgaben

Einstellung	Beschreibung
Untersuchungszeitplan	**Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. **Nach Zeitplan**. In diesem Startmodus für die Untersuchungsaufgabe führt das Programm die Untersuchungsaufgabe nach dem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Untersuchungsaufgabe können Sie die Untersuchungsaufgabe auch manuell starten.
Übersprungene Aufgaben ausführen	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security die übersprungene Aufgabe, sobald dies möglich ist. Die Aufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Aufgabe ausgeschaltet war. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen. Wenn dieses Kontrollkästchen deaktiviert ist, führt Kaspersky Endpoint Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Nur ausführen, wenn der Computer inaktiv ist	Schiebt den Start der Aufgabe auf, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde. Mit dieser Zeitplanoption können Sie die Computerressourcen schonen, während der Computer verwendet wird.

Untersuchungsbereich bearbeiten

Der *Untersuchungsbereich* ist eine Liste mit Ordnerpfaden und Pfaden, die Kaspersky Endpoint Security bei der Ausführung der Aufgabe untersucht. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

Um den Untersuchungsbereich zu bearbeiten, empfehlen wir die Verwendung der Aufgabe *Benutzerdefinierte Untersuchung*. Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgaben *Vollständige Untersuchung* und *Untersuchung wichtiger Bereiche* zu ändern.

Kaspersky Endpoint Security bietet die folgenden vordefinierten Objekte als Teil des Untersuchungsbereichs:

- **Systemspeicher**.
- **Aktive Prozesse und Autostart-Objekte**.

  Speicherplatz, der belegt ist durch Prozesse bzw. ausführbare Programmdateien, die beim Systemstart ausgeführt werden.
- **Laufwerks-Bootsektoren**.

  Bootsektoren von Festplatten und Wechseldatenträgern.
- **System-Backup**.

  Inhalt des Ordners „System Volume Information“.
- **Alle externen Geräte**.
- **Alle Festplatten**.
- **Alle Netzlaufwerke**.

In Kaspersky Endpoint Security für Windows 12.12 sind E-Mail-Nachrichten aus dem Untersuchungsbereich des Programms ausgeschlossen. Die Untersuchung ein- und ausgehender E-Mail-Nachrichten wird von der Komponente „Schutz vor E-Mail-Bedrohungen“ ausgeführt. Wenn Sie eine ältere Version des Verwaltungs-Plug-ins verwenden, schließt das Programm E-Mail-Nachrichten aus dem Untersuchungsbereich aus, selbst wenn diese durch die Richtlinie eingeschlossen werden.

Für Netzlaufwerke oder freigegebene Ordnern empfehlen wir, eine separate Untersuchungsaufgabe zu erstellen. Geben Sie in den Einstellungen der Aufgabe *Schadsoftware-Untersuchung* einen Benutzer an, der Schreibzugriff auf dieses Laufwerk hat. Dies ist notwendig, um erkannte Bedrohungen zu neutralisieren. Wenn der Server, auf dem sich das Netzlaufwerk befindet, über eigene Sicherheitstools verfügt, führen Sie die Untersuchungsaufgabe für dieses Laufwerk nicht aus. Dadurch können Sie eine doppelte Untersuchung von Objekten vermeiden und die Leistung des Servers verbessern.

Um Ordner oder Dateien aus dem Untersuchungsbereich auszuschließen, fügen Sie den Ordner oder die Datei zur vertrauenswürdigen Zone hinzu.

So bearbeiten Sie einen Untersuchungsbereich über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Wählen Sie die Untersuchungsaufgabe aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.

   Erstellen Sie bei Bedarf die Aufgabe *Schadsoftware-Untersuchung*.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
5. Klicken Sie im Abschnitt **Untersuchungsbereich** auf **Einstellungen**.
6. Wählen Sie im folgenden Fenster die Objekte aus, die Sie dem Untersuchungsbereich hinzufügen oder davon ausschließen möchten.
7. Um ein neues Objekt zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie im Feld **Objekt** den Ordner- oder Dateipfad ein.

   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` funktioniert nicht.
   - 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.

   Sie können Masken überall in einem Datei- oder Ordnerpfad verwenden. Wenn Sie beispielsweise möchten, dass der Untersuchungsbereich den Ordner „Downloads“ für alle Benutzerkonten auf dem Computer umfasst, geben Sie folgende Maske ein: `C:\Users\*\Downloads\`.

   Das Objekt **Dieser PC** in der Liste der Dateiressourcen des Computers enthält die folgenden Objekte: **Alle Festplatten**, **Alle Netzlaufwerke** und **Alle Wechseldatenträger**.

   Sie können ein Objekt von Untersuchungen ausschließen, ohne es aus der Liste der Objekte im Untersuchungsbereich zu löschen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So bearbeiten Sie einen Untersuchungsbereich über die „Web Console“ oder „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Erstellen Sie bei Bedarf die Aufgabe *Schadsoftware-Untersuchung*.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Legen Sie im Abschnitt **Untersuchungsbereich** fest, welche Objekte Sie dem Untersuchungsbereich hinzufügen oder daraus ausschließen möchten.

5. Um ein neues Objekt zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie den Ordner- oder Dateipfad ein.

      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` funktioniert nicht.

      - 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.

      Sie können Masken überall in einem Datei- oder Ordnerpfad verwenden. Wenn Sie beispielsweise möchten, dass der Untersuchungsbereich den Ordner „Downloads“ für alle Benutzerkonten auf dem Computer umfasst, geben Sie folgende Maske ein: `C:\Users\*\Downloads\`.

   Sie können ein Objekt von Untersuchungen ausschließen, ohne es aus der Liste der Objekte im Untersuchungsbereich zu löschen. Setzen Sie dazu den Umschalter neben dem Objekt auf „Aus“.

6. Speichern Sie die vorgenommenen Änderungen.

So bearbeiten Sie einen Untersuchungsbereich über die Programmoberfläche

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.
2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Benutzerdefinierte Untersuchung* aus und klicken Sie auf **Auswählen**.

   Sie können den Untersuchungsbereich auch für andere Aufgaben bearbeiten. Die Kaspersky-Experten raten davon ab, den Untersuchungsbereich der Aufgaben *Vollständige Untersuchung* und *Untersuchung wichtiger Bereiche* zu ändern.
3. Wählen Sie im folgenden Fenster die Objekte aus, die Sie dem Untersuchungsbereich hinzufügen möchten.
4. Speichern Sie die vorgenommenen Änderungen.

Wird die Untersuchungsaufgabe nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Untersuchung nach Zeitplan ausführen

Die Aufgabe *Schadsoftware-Untersuchung* kann zeitaufwendig sein und die Nutzung der Computerressourcen durch Kaspersky Endpoint Security erhöhen. Daher sollte die Aufgabe zu einem optimalen Zeitpunkt ausgeführt werden, um die Auswirkungen auf die Leistung anderer Programme zu minimieren.

Wenn die Mitarbeiter in Ihrem Unternehmen beispielsweise feste Arbeitszeiten haben, können Sie die Computeruntersuchung so konfigurieren, dass sie nachts oder am Wochenende stattfindet. Ist der Start der Aufgabe nicht möglich (beispielsweise wenn der Computer im betreffenden Moment ausgeschaltet ist), können Sie festlegen, dass eine übersprungene Untersuchungsaufgabe automatisch zum nächstmöglichen Zeitpunkt ausgeführt wird. Mit dieser Funktion sollten Sie vorsichtig sein: Sie kann die Programme auf dem Benutzercomputer verlangsamen, wenn der Computer morgens eingeschaltet wird.

Falls es keinen optimalen Untersuchungszeitplan für Ihre Situation gibt, können Sie die Untersuchung so konfigurieren, dass sie unter einer der folgenden Bedingungen ausgeführt wird:

- Nach einem Datenbanken-Update.

  Kaspersky Endpoint Security führt die Untersuchung des Computers mit den aktualisierten Signatur-Datenbanken durch.
- Nach dem Programmstart.

  Nachdem das Programm gestartet wurde, wartet Kaspersky Endpoint Security für einen festgelegten Zeitraum und führt dann die Computeruntersuchung aus. Da beim Start des Betriebssystems viele Prozesse ausgeführt werden, ist es vorteilhaft, die Untersuchungsaufgabe aufzuschieben, anstatt sie sofort nach dem Start von Kaspersky Endpoint Security auszuführen.
- Funktion Wake-on-LAN.

  Kaspersky Endpoint Security führt eine Computeruntersuchung gemäß dem Zeitplan durch, selbst wenn der Computer ausgeschaltet ist. Dazu verwendet das Programm die Funktion Wake-on-LAN des Betriebssystems. Mithilfe der Wake-on-LAN-Funktion kann der Computer aus der Ferne durch das Senden eines speziellen Signals über das lokale Netzwerk eingeschaltet werden. Um diese Funktion zu verwenden, müssen Sie Wake-on-LAN in den BIOS-Einstellungen aktivieren.

  Sie können die Untersuchung unter Verwendung von Wake-on-LAN nur für die Aufgabe *Schadsoftware-Untersuchung* in Kaspersky Security Center konfigurieren. Sie können Wake-on-LAN nicht aktivieren, um den Computer über die Programmoberfläche zu untersuchen.

- Wenn der Computer inaktiv ist.

  Kaspersky Endpoint Security führt eine Untersuchung des Computers gemäß dem Zeitplan durch, wenn der Bildschirmschoner aktiv oder der Bildschirm gesperrt ist. Wenn der Benutzer den Computer entsperrt, hält Kaspersky Endpoint Security die Untersuchung an. In diesem Fall kann die vollständige Untersuchung mehrere Tage dauern.

- Wenn die Aufgabe übersprungen wurde.

  Kaspersky Endpoint Security führt die übersprungene Aufgabe aus, sobald dies möglich ist. Die Aufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Aufgabe ausgeschaltet war. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen.

So konfigurieren Sie den Untersuchungszeitplan über die „Web Console“ und „Cloud Console“

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

4. Passen Sie den Zeitplan für die Untersuchungsaufgabe an.

5. Passen Sie je nach gewählter Frequenz die erweiterten Einstellungen des Zeitplans für den Aufgabenstart an (siehe Tabelle unten).

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Untersuchungszeitplan über die Programmoberfläche

Sie können den Untersuchungszeitplan nur konfigurieren, wenn für den Computer keine Richtlinie gilt. Für Computer, die einer Richtlinie unterliegen, können Sie den Aufgabenzeitplan für die *Schadsoftware-Untersuchung* in Kaspersky Security Center konfigurieren.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.

2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.

   Sie können einen Zeitplan für die Ausführung einer vollständigen Untersuchung, einer Untersuchung wichtiger Bereiche oder einer Integritätsprüfung konfigurieren. Eine benutzerdefinierte Untersuchung kann nur manuell ausgeführt werden.

3. Klicken Sie auf **Untersuchungszeitplan**.

4. Konfigurieren Sie im angezeigten Fenster den Zeitplan der Untersuchungsaufgabe.

5. Passen Sie je nach gewählter Frequenz die erweiterten Einstellungen des Zeitplans für den Aufgabenstart an (siehe Tabelle unten).

6. Speichern Sie die vorgenommenen Änderungen.

Einstellungen für den Untersuchungszeitplan

Einstellung	Beschreibung
Untersuchungszeitplan	**Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. **Nach Zeitplan**. In diesem Startmodus für die Untersuchungsaufgabe führt das Programm die Untersuchungsaufgabe nach dem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Untersuchungsaufgabe können Sie die Untersuchungsaufgabe auch manuell starten.
Ausführung nach Programmstart aufschieben für n Minuten	Der Start der Untersuchungsaufgabe wird nach dem Programmstart aufgeschoben. Da beim Start des Betriebssystems viele Prozesse ausgeführt werden, ist es vorteilhaft, die Untersuchungsaufgabe aufzuschieben, anstatt sie sofort nach dem Start von Kaspersky Endpoint Security auszuführen.
Übersprungene Aufgaben ausführen	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security die übersprungene Aufgabe, sobald dies möglich ist. Die Aufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Aufgabe ausgeschaltet war. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen. Wenn dieses Kontrollkästchen deaktiviert ist, führt Kaspersky Endpoint Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Nur ausführen, wenn der Computer inaktiv ist	Schiebt den Start der Aufgabe auf, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde. Mit dieser Zeitplanoption können Sie die Computerressourcen schonen, während der Computer verwendet wird.
Automatische zufällige Verzögerung für Aufgabenstarts verwenden *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe nicht streng nach Zeitplan ausgeführt, sondern zufällig in einem bestimmten Intervall, d. h. die Aufgabenstarts werden zeitlich verteilt. Zufällige Startzeiten verhindern, dass viele Computer gleichzeitig auf den Administrationsserver zugreifen, wenn die Aufgabe nach Zeitplan ausgeführt wird. Der Bereich der zufälligen Startzeiten wird beim Erstellen der Aufgabe automatisch berechnet. Dabei wird die Anzahl der Computer berücksichtigt, denen die Aufgabe zugewiesen ist. Anschließend wird die Aufgabe immer zur berechneten Startzeit ausgeführt. Die berechnete Startzeit ändert sich aber, wenn die Aufgabeneinstellungen geändert werden oder die Aufgabe manuell ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe exakt zum geplanten Zeitpunkt ausgeführt.
Zufällige Verzögerung für den Aufgabenstart innerhalb von (Min.)	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe auf Computern innerhalb eines bestimmten Zeitraums zu einem zufälligen Zeitpunkt ausgeführt. Zufällige Startzeiten verhindern, dass viele Computer gleichzeitig auf den Administrationsserver zugreifen, wenn die Aufgabe nach Zeitplan ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe exakt zum geplanten Zeitpunkt ausgeführt.
Aufgabe anhalten, wenn sie länger ausgeführt wird als (Min.) *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt. Um die Ausführungsdauer einer Aufgabe zu reduzieren, können Sie z. B. den Untersuchungsbereich anpassen oder die Untersuchung optimieren.
Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren (Min.) *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Wenn dieses Kontrollkästchen aktiviert ist, erhält das Betriebssystem des Computers eine bestimmte Vorlaufzeit für seinen Start, bevor die Aufgabe ausgeführt wird. Standardmäßig beträgt die Vorlaufzeit 5 Minuten. Aktivieren Sie das Kontrollkästchen, wenn Sie die Aufgabe auf allen Computern ausführen möchten, auch auf ausgeschalteten Computern.
Geräte nach Abschluss der Aufgabe herunterfahren *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Wenn dieses Kontrollkästchen aktiviert ist, wird der Computer nach Abschluss der Aufgabe heruntergefahren. Sie können diese Funktion beispielsweise aktivieren, um den Computer freitags nach Feierabend untersuchen zu lassen. Nach Abschluss der Aufgabe schaltet das Programm den Computer für das Wochenende aus.
Aufgabe anhalten	Sie können einen Zeitraum festlegen, in dem die Ausführung einer zuvor geplanten Aufgabe angehalten wird. Nach Ablauf des angegebenen Zeitraums wird die Aufgabe fortgesetzt. Dies kann beispielsweise erforderlich sein, um die Auswirkungen von Kaspersky Endpoint Security auf die Leistung Ihres Computers bei hoher Auslastung zu minimieren.
Zeitplan deaktivieren ab	Wenn das Kontrollkästchen aktiviert ist, beendet Kaspersky Endpoint Security ab dem angegebenen Datum die Ausführung der geplanten Aufgabe. Die Aufgabe wird in den Modus **Manuell** versetzt.

Untersuchung als anderer Benutzer ausführen

Standardmäßig wird die Untersuchungsaufgabe im Namen des Benutzers ausgeführt, mit dessen Rechten Sie im Betriebssystem registriert sind. Der Schutzbereich kann Netzlaufwerke und andere Objekte enthalten, die besondere Zugriffsrechte erfordern. Sie können in den Programmeinstellungen einen Benutzer angeben, der über die erforderlichen Rechte verfügt, und die Untersuchungsaufgabe unter dem Konto dieses Benutzers ausführen.

Die folgenden Untersuchungen können im Namen eines anderen Benutzers ausgeführt werden:

- Untersuchung wichtiger Bereiche
- Vollständige Untersuchung.
- Benutzerdefinierte Untersuchung
- Untersuchung aus dem Kontextmenü.

Die Benutzerrechte zum Ausführen der Untersuchung von Wechseldatenträgern, der Untersuchung im Hintergrund oder der Integritätsprüfung können nicht konfiguriert werden.

So führen Sie eine Untersuchung als ein anderer Benutzer über die Verwaltungskonsole (MMC) aus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Aufgaben** aus.
4. Wählen Sie die Untersuchungsaufgabe aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.
5. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Benutzerkonto** aus.
6. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechte Sie eine Untersuchungsaufgabe ausführen möchten.
7. Speichern Sie die vorgenommenen Änderungen.

So führen Sie eine Untersuchung als ein anderer Benutzer über die „Web Console“ oder „Cloud Console“ aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Einstellungen** aus.
4. Klicken Sie im Block **Benutzerkonto** auf **Einstellungen**.

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechte Sie eine Untersuchungsaufgabe ausführen möchten.

6. Speichern Sie die vorgenommenen Änderungen.

So führen Sie eine Untersuchung als ein anderer Benutzer über die Programmoberfläche aus

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.

2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.

3. Wählen Sie in den Aufgabeneigenschaften **Erweiterte Einstellungen → Untersuchung ausführen als**.

4. Geben Sie im angezeigten Fenster die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechte Sie eine Untersuchungsaufgabe ausführen möchten.

5. Speichern Sie die vorgenommenen Änderungen.

Wird die Untersuchungsaufgabe nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Untersuchung optimieren

Beschränken der CPU-Auslastung während der Untersuchung des Computers

Sie können die CPU-Auslastung aufgrund der Aufgabe *Schadsoftware-Untersuchung* beschränken. Dadurch kann die Untersuchung Ihres Computers länger dauern.

So begrenzen Sie über die Verwaltungskonsole (MMC) die CPU-Auslastung bei der Untersuchung des Computers

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.

4. Aktivieren Sie unter **Leistung** das Kontrollkästchen **CPU-Auslastung für Untersuchungsaufgaben begrenzen** und geben Sie den Durchschnittswert für die CPU-Auslastung in Prozent ein.

5. Speichern Sie die vorgenommenen Änderungen.

So begrenzen Sie die CPU-Auslastung bei der Untersuchung des Computers in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Leistung**.

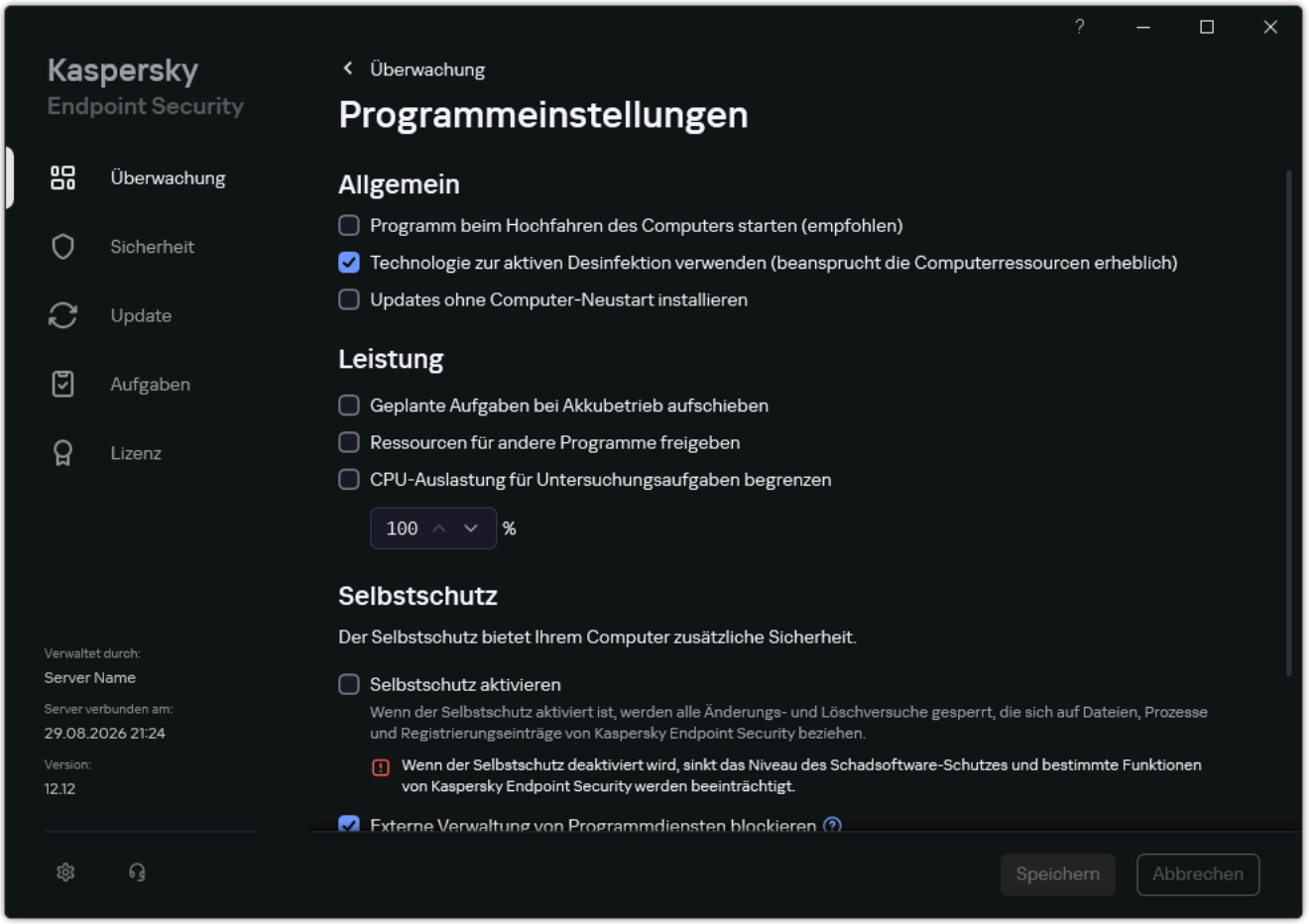
5. Setzen Sie unter **CPU-Auslastung für Untersuchungsaufgaben begrenzen** den Schalter auf **CPU-Auslastung für Untersuchungsaufgaben begrenzen** und geben Sie den Durchschnittswert für die CPU-Auslastung in Prozent ein.

6. Speichern Sie die vorgenommenen Änderungen.

So begrenzen Sie über App-Benutzeroberfläche die CPU-Auslastung bei der Untersuchung des Computers

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Aktivieren Sie unter **Leistung** das Kontrollkästchen **CPU-Auslastung für Untersuchungsaufgaben begrenzen** und geben Sie den Durchschnittswert für die CPU-Auslastung in Prozent ein.

4. Speichern Sie die vorgenommenen Änderungen.

Konfigurieren von erweiterten Einstellungen der Aufgabe Schadsoftware-Untersuchung.

Die Dateiuntersuchung lässt sich in folgender Hinsicht optimieren: Untersuchungsdauer verkürzen und Arbeitsgeschwindigkeit von Kaspersky Endpoint Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien. Außerdem können Sie die Untersuchungsdauer für eine einzelne Datei beschränken. Nach Ablauf des vorgegebenen Zeitraums schließt Kaspersky Endpoint Security eine Datei aus der laufenden Untersuchung aus (außer Archiven und Objekten, die aus mehreren Dateien bestehen).

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. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

Außerdem können Sie die Technologien iChecker und iSwift aktivieren. Mit den Technologien iChecker und iSwift lässt sich die Dateiuntersuchung beschleunigen. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

So optimieren Sie die Untersuchung über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Wählen Sie die Untersuchungsaufgabe aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.

   Erstellen Sie bei Bedarf die Aufgabe *Schadsoftware-Untersuchung*.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
5. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.

   Dadurch wird das Fenster mit den Einstellungen der Untersuchungsaufgabe geöffnet.
6. Konfigurieren Sie im Block **Optimierung** die Untersuchungseinstellungen:

   - **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.

     Sie können auch festlegen, dass bei der Untersuchung neuer Dateien der Typ berücksichtigt werden soll. Sie können beispielsweise angeben, dass alle Verteilungspakete untersucht werden, aber nur neue Archive und Dateien im Office-Format.

- **Dateien überspringen, wenn Untersuchung länger dauert als n Sek**. Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

- **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**. Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Sie haben beispielsweise die Ausführung von Untersuchungsaufgaben für 18:00 und 20:00 Uhr geplant. Kaspersky Endpoint Security verschiebt die für 20:00 Uhr geplante Untersuchungsaufgabe, wenn die für 18:00 Uhr geplante Untersuchungsaufgabe noch ausgeführt wird. Das Programm führt die verschobene Untersuchung durch, sobald die um 18:00 Uhr gestartete Aufgabe abgeschlossen ist.

7. Klicken Sie auf **Erweitert**.

   Dadurch wird das Fenster mit den Untersuchungseinstellungen für zusammengesetzte Dateien geöffnet.

8. Aktivieren Sie im Block **Größenbeschränkung** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**. Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

   Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

9. Klicken Sie auf **OK**.

10. Gehen Sie zur Registerkarte **Erweitert**.

11. Aktivieren Sie im Abschnitt **Untersuchungstechnologien** die Kontrollkästchen für die Technologien, die bei der Untersuchung verwendet werden sollen.

    - **iSwift-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

    - **iChecker-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

12. Speichern Sie die vorgenommenen Änderungen.

So optimieren Sie die Untersuchung in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Untersuchungsaufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Erstellen Sie bei Bedarf die Aufgabe *Schadsoftware-Untersuchung*.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Aktivieren Sie im Block **Aktion beim Fund einer Bedrohung** das Kontrollkästchen **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.

   Sie können auch festlegen, dass bei der Untersuchung neuer Dateien der Typ berücksichtigt werden soll. Sie können beispielsweise angeben, dass alle Verteilungspakete untersucht werden, aber nur neue Archive und Dateien im Office-Format.

5. Aktivieren Sie im Block **Untersuchung optimieren** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**. Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

   > Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

6. Aktivieren Sie das Kontrollkästchen **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**. Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Sie haben beispielsweise die Ausführung von Untersuchungsaufgaben für 18:00 und 20:00 Uhr geplant. Kaspersky Endpoint Security verschiebt die für 20:00 Uhr geplante Untersuchungsaufgabe, wenn die für 18:00 Uhr geplante Untersuchungsaufgabe noch ausgeführt wird. Das Programm führt die verschobene Untersuchung durch, sobald die um 18:00 Uhr gestartete Aufgabe abgeschlossen ist.

7. Aktivieren Sie im Block **Erweiterte Einstellungen** das Kontrollkästchen **Datei überspringen, wenn Untersuchung länger dauert als (Sek.)**. Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

8. Speichern Sie die vorgenommenen Änderungen.

So optimieren Sie die Untersuchung über die Programmoberfläche

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Aufgaben**.

2. Wählen Sie in der Aufgabenliste die Untersuchungsaufgabe und klicken Sie auf ⚙.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Konfigurieren Sie im Block **Optimierung** die Untersuchungseinstellungen:

   - **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.

     Sie können auch festlegen, dass bei der Untersuchung neuer Dateien der Typ berücksichtigt werden soll. Sie können beispielsweise angeben, dass alle Verteilungspakete untersucht werden, aber nur neue Archive und Dateien im Office-Format.

   - **Datei überspringen, wenn Untersuchung länger dauert als n Sekunde(n)**. Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

   - **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**. Geplante Untersuchungsaufgaben verzögern, wenn eine zuvor gestartete geplante Untersuchung noch ausgeführt wird. Kaspersky Endpoint Security reiht geplante Untersuchungsaufgaben in die Warteschlange ein, wenn die laufende Untersuchung fortgesetzt wird. Dadurch wird die Auslastung des Computers optimiert. Sie haben beispielsweise die Ausführung von Untersuchungsaufgaben für 18:00 und 20:00 Uhr geplant. Kaspersky Endpoint Security verschiebt die für 20:00 Uhr geplante Untersuchungsaufgabe, wenn die für 18:00 Uhr geplante Untersuchungsaufgabe noch ausgeführt wird. Das Programm führt die verschobene Untersuchung durch, sobald die um 18:00 Uhr gestartete Aufgabe abgeschlossen ist.

5. Aktivieren Sie im Block **Größenbeschränkung** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**. Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

   Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

6. Aktivieren Sie im Abschnitt **Untersuchungstechnologien** die Kontrollkästchen für die Technologien, die bei der Untersuchung verwendet werden sollen.

   - **iSwift-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

   - **iChecker-Technologie**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

7. Speichern Sie die vorgenommenen Änderungen.

Wird die Untersuchungsaufgabe nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) ist in der Software in den USA möglicherweise nicht verfügbar.

Für ein regelmäßiges Update ist eine aktuelle Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Der Computer muss mit dem Internet verbunden sein, um das Update-Paket erfolgreich von den Kaspersky-Update-Servern herunterzuladen. Standardmäßig wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, müssen Sie die Proxyserver-Einstellungen konfigurieren.

Updates werden mit dem HTTPS-Protokoll heruntergeladen. Falls ein Download mit dem HTTPS-Protokoll nicht möglich ist, erfolgt der Download mit dem HTTP-Protokoll.

Bei einer Aktualisierung werden folgende Objekte auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Endpoint Security. Der Computerschutz basiert auf Datenbanken, die Signaturen für Viren und andere bedrohliche Programme, sowie Informationen über entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese Informationen bei der Suche nach und der Desinfektion von infizierten Dateien auf dem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Endpoint Security werden auch die Netzwerktreiber aktualisiert, die gewährleisten, dass die Schutzkomponenten den Netzwerkverkehr abfangen können.

- Programm-Module. Neben den Datenbanken von Kaspersky Endpoint Security können auch die Programm-Module aktualisiert werden. Updates für Programm-Module beheben Schwachstellen von Kaspersky Endpoint Security, fügen neue Funktionen hinzu und optimieren vorhandene Funktionen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version verglichen, die in der Update-Quelle vorliegt. Sind die Datenbanken und Programm-Module nicht aktuell, werden fehlende Teile der Updates auf dem Computer installiert.

Sind die Datenbanken stark veraltet, kann das Update-Paket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Informationen über den aktuellen Status der Datenbanken von Kaspersky Endpoint Security werden im Programmhauptfenster oder in einem Tooltip angezeigt. Den Tooltip sehen Sie, wenn Sie den Mauszeiger über das Programmsymbol im Infobereich bewegen.

Informationen über die Aktualisierungsergebnisse und über alle Ereignisse, die bei der Ausführung einer Update-Aufgabe auftreten, werden im Bericht von Kaspersky Endpoint Security protokolliert.

Wenn das Programm im Light Agent-Modus ausgeführt wird, müssen beim Update der Programm-Datenbanken und Module einige Besonderheiten berücksichtigt werden.

Schemata für das Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Auf den Benutzercomputern werden die folgenden Objekte aktualisiert:

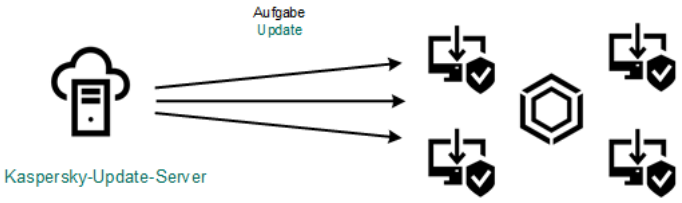
- Antiviren-Datenbanken. Die Antiviren-Datenbanken enthalten Datenbanken mit den Signaturen schädlicher Programme, Definitionen von Netzwerkangriffen, Datenbanken für bösartige Webadressen und Phishing-Webadressen, Datenbanken für Banner, Spam-Datenbanken sowie andere Daten.

- Programm-Module. Ein Update für Module dient dazu, Schwachstellen im Programm zu beheben und die Methoden des Computerschutzes zu verbessern. Bei Modul-Updates kann das Verhalten von Programmkomponenten geändert und neue Funktionen können hinzugefügt werden.

Kaspersky Endpoint Security unterstützt folgende Schemata für das Update der Datenbanken und Programm-Module:

- Update von den Kaspersky-Servern.

  Die Kaspersky-Update-Server befinden sich in unterschiedlichen Ländern. Dadurch wird die Zuverlässigkeit des Updates erhöht. Wenn das Update nicht vom einem Server ausgeführt werden kann, wechselt Kaspersky Endpoint Security zum nächsten Server.



Update von den Kaspersky-Servern

- Zentralisiertes Update.

  Das zentralisierte Update gewährleistet eine Reduzierung des externen Internet-Datenverkehrs und eine bequeme Kontrolle des Updates.

  Das zentralisierte Update umfasst die folgenden Schritte:

  1. Upload des Update-Pakets in eine Ablage innerhalb des Unternehmensnetzwerks.

     Das Update-Paket wird mithilfe der Administrationsserver-Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* in die Datenverwaltung heruntergeladen.

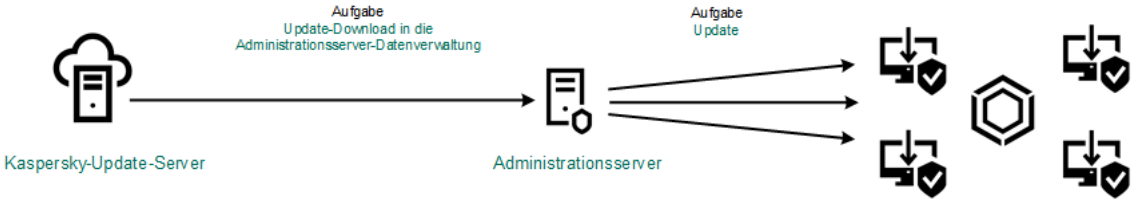
2. Upload des Update-Pakets in einen gemeinsamen Ordner (optional).

   Für den Upload des Update-Pakets in einen gemeinsamen Ordner bestehen die folgenden Möglichkeiten:

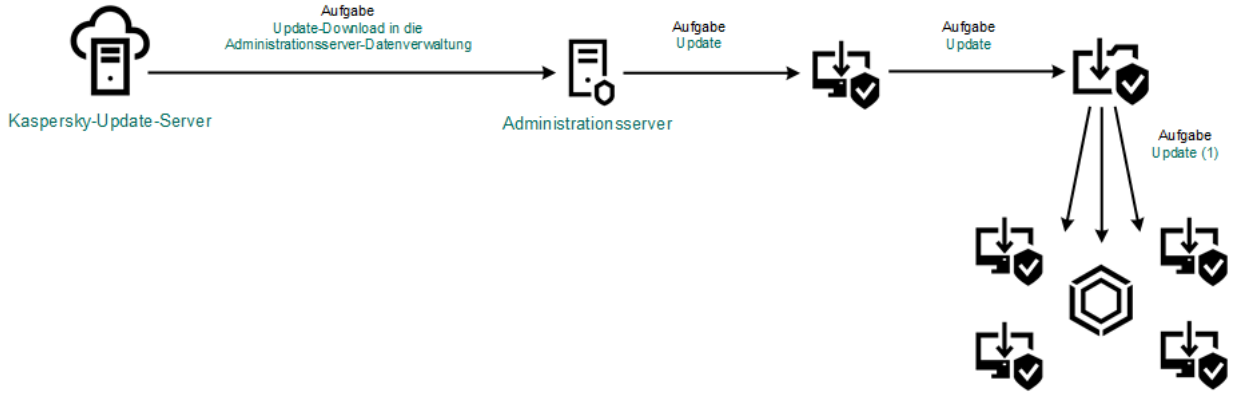
   - Mithilfe der *Update der Datenbanken und Programm-Module*-Aufgabe von Kaspersky Endpoint Security. Diese Aufgabe ist für einen der Computer des lokalen Unternehmensnetzwerks vorgesehen.
   - Mithilfe von Kaspersky Update Utility. Ausführliche Informationen über die Verwendung von Kaspersky Update Utility finden Sie in der Kaspersky-Wissensdatenbank.

3. Verteilung des Update-Pakets an die Client-Computer.

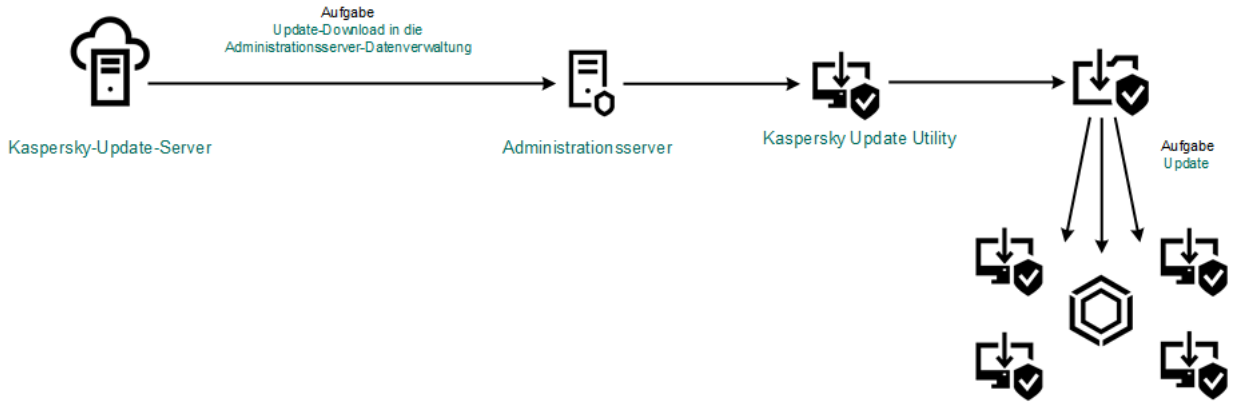
   Die Verteilung des Update-Pakets an die Client-Computer wird durch die Kaspersky Endpoint Security-Aufgabe *Update der Datenbanken und Programm-Module* gewährleistet. Sie können eine unbeschränkte Anzahl von Update-Aufgaben für jede der Administrationsgruppen erstellen.



Update aus dem Serverspeicher



Update aus dem gemeinsamen Ordner



Update mithilfe von Kaspersky Update Utility

Für Kaspersky Security Center enthält die Liste der Update-Quellen standardmäßig den Kaspersky Security Center-Administrationsserver und die Kaspersky-Update-Server. Für Kaspersky Security Center Cloud Console enthält die Liste der Update-Quellen standardmäßig die Verteilungspunkte und die Kaspersky-Update-Server. Details über die Verteilungspunkte finden Sie in der Hilfe zu Kaspersky Security Center Cloud Console. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden. Wenn das Update von einer Update-Quelle nicht ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten.

Updates werden mit den standardmäßigen Netzwerkprotokolle von den Kaspersky-Update-Servern oder von anderen FTP- oder HTTP-Servern heruntergeladen. Wenn für den Zugriff auf eine Update-Quelle die Verbindung mit einem Proxyserver erforderlich ist, geben Sie die Proxyserver-Einstellungen in den Eigenschaften der Richtlinie für Kaspersky Endpoint Security ein.

Update aus dem Serverspeicher

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update der Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus dem Serverspeicher erfolgen soll. Dabei lädt Kaspersky Security Center das Update-Paket von den Kaspersky-Update-Servern in einen Speicher (FTP-, HTTP-Server, Netzwerkordner oder lokaler Ordner) herunter. Die übrigen Computer des lokalen Unternehmensnetzwerks können das Update-Paket dann aus dem Serverspeicher abrufen.

Um das Update der Datenbanken und Programm-Module aus einem Serverspeicher einzurichten, sind folgende Schritte erforderlich:

1. Konfigurieren des Downloads eines Update-Pakets in die Datenverwaltung des Administrationsservers (Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*).

   Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird vom Schnellstartassistenten des Administrationsservers automatisch erstellt. Diese Aufgabe darf nur eine einzige Instanz haben. Standardmäßig kopiert Kaspersky Security Center das Update-Paket in den Ordner `\\<server name>\KLSHARE\Updates`. Weitere Informationen über den Download von Updates in die Datenverwaltung des Administrationsservers finden Sie in der Hilfe zu Kaspersky Security Center.

2. Anpassen des Updates für Datenbanken und Programm-Module aus dem festgelegten Serverspeicher für die Verteilung an die übrigen Computer des lokalen Unternehmensnetzwerks (Aufgabe *Update der Datenbanken und Programm-Module*).

   So konfigurieren Sie über die Verwaltungskonsole (MMC) das Update für Kaspersky Endpoint Security aus dem angegebenen Serverspeicher

   1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

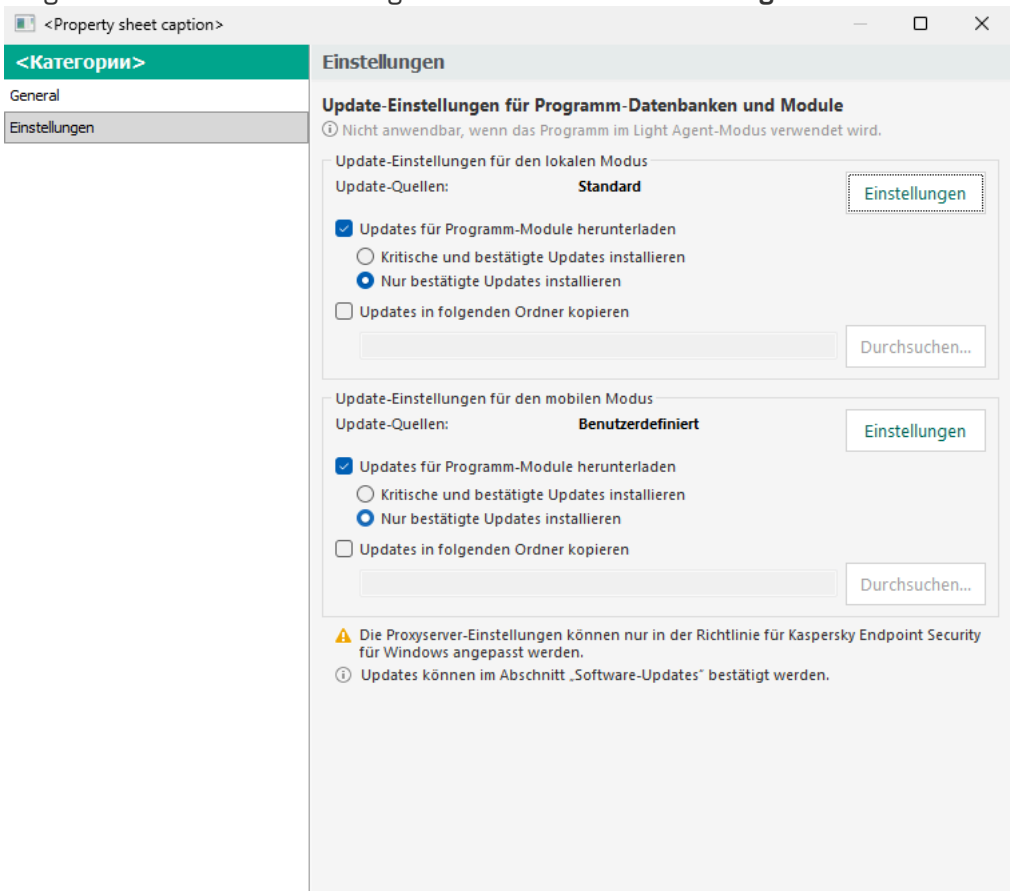
      Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.

   2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

      Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

      Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

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



Einstellungen der Aufgabe Update der Datenbanken und Programm-Module

4. Klicken Sie im Block **Update-Einstellungen für den lokalen Modus** auf **Einstellungen**.

5. Stellen Sie sicher, dass in der Liste der Update-Quellen das Update von der Quelle **Kaspersky Security Center** aktiviert ist. Außerdem muss die Quelle **Kaspersky Security Center** die höchste Priorität haben.

6. Fügen Sie bei Bedarf die Update-Quellen hinzu:

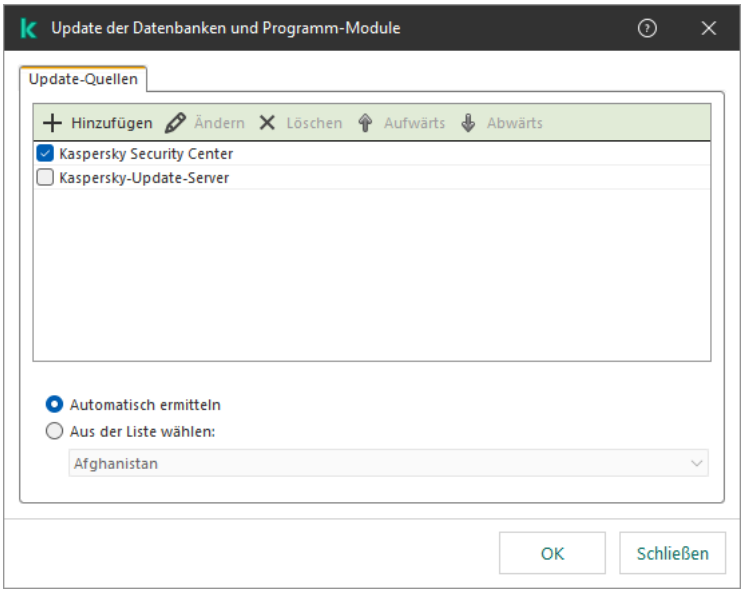
   a. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.

   b. Geben Sie im Feld **Update-Quellen** die Adresse des FTP- oder HTTP-Servers, Netzwerkordners oder lokalen Ordners an, in den Kaspersky Security Center ein Update-Paket kopieren soll, das von den Kaspersky-Servern heruntergeladen wurde.

   > Die Adresse der Update-Quelle muss mit der Adresse übereinstimmen, die im Feld **Ordner zum Speichern von Updates** angegeben wurde, als der Update-Download in den Serverspeicher konfiguriert wurde (Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*).

   c. Klicken Sie auf **OK**.

Sie können eine Update-Quelle ausschließen, ohne sie aus der Liste der Update-Quellen zu entfernen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.



Update-Quellen

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

8. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus und konfigurieren Sie den Ausführungsmodus der Aufgabe.

9. Standardmäßig führt Kaspersky Endpoint Security die Aufgabe im manuellen Modus aus.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die Web Console das Update für Kaspersky Endpoint Security aus dem angegebenen Serverspeicher

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Lokaler Modus** aus.

4. Stellen Sie sicher, dass in der Liste der Update-Quellen das Update von der Quelle **Kaspersky Security Center** aktiviert ist. Außerdem muss die Quelle **Kaspersky Security Center** die höchste Priorität haben.

5. Fügen Sie bei Bedarf die Update-Quellen hinzu:

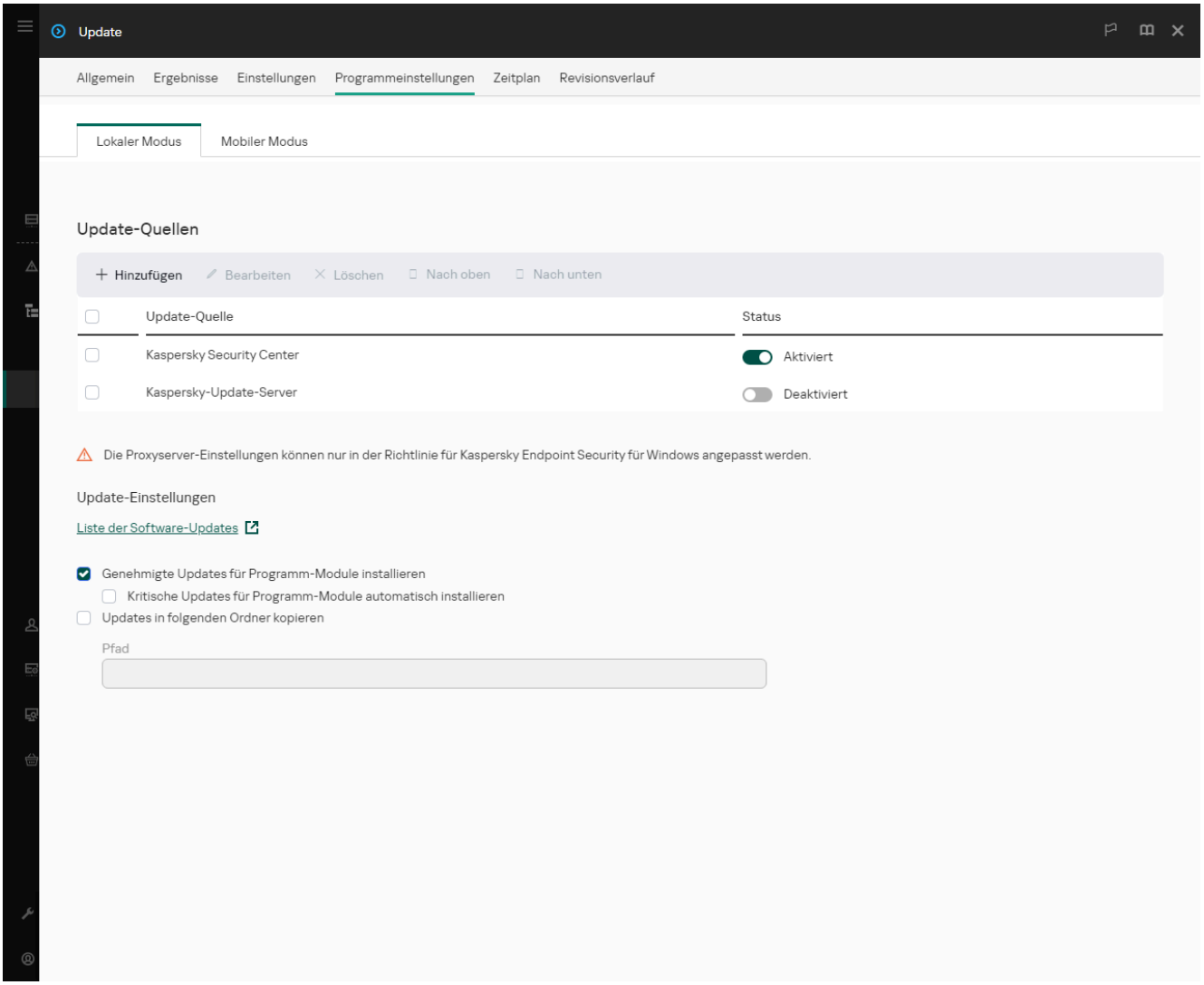
   a. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.

   b. Geben Sie im Feld **Update-Quellen** die Adresse des FTP- oder HTTP-Servers, Netzwerkordners oder lokalen Ordners an, in den Kaspersky Security Center ein Update-Paket kopieren soll, das von den Kaspersky-Servern heruntergeladen wurde.

      Die Adresse der Update-Quelle muss mit der Adresse übereinstimmen, die im Feld **Ordner zum Speichern von Updates** angegeben wurde, als der Update-Download in den Serverspeicher konfiguriert wurde (Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*).

   c. Klicken Sie auf **Speichern**.

Sie können eine Update-Quelle ausschließen, ohne sie aus der Liste der Update-Quellen zu entfernen. Setzen Sie dazu den Umschalter neben dem Objekt auf „Aus“.



Update-Quellen

6. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

7. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Zeitplan** aus und konfigurieren Sie den Ausführungsmodus der Aufgabe.

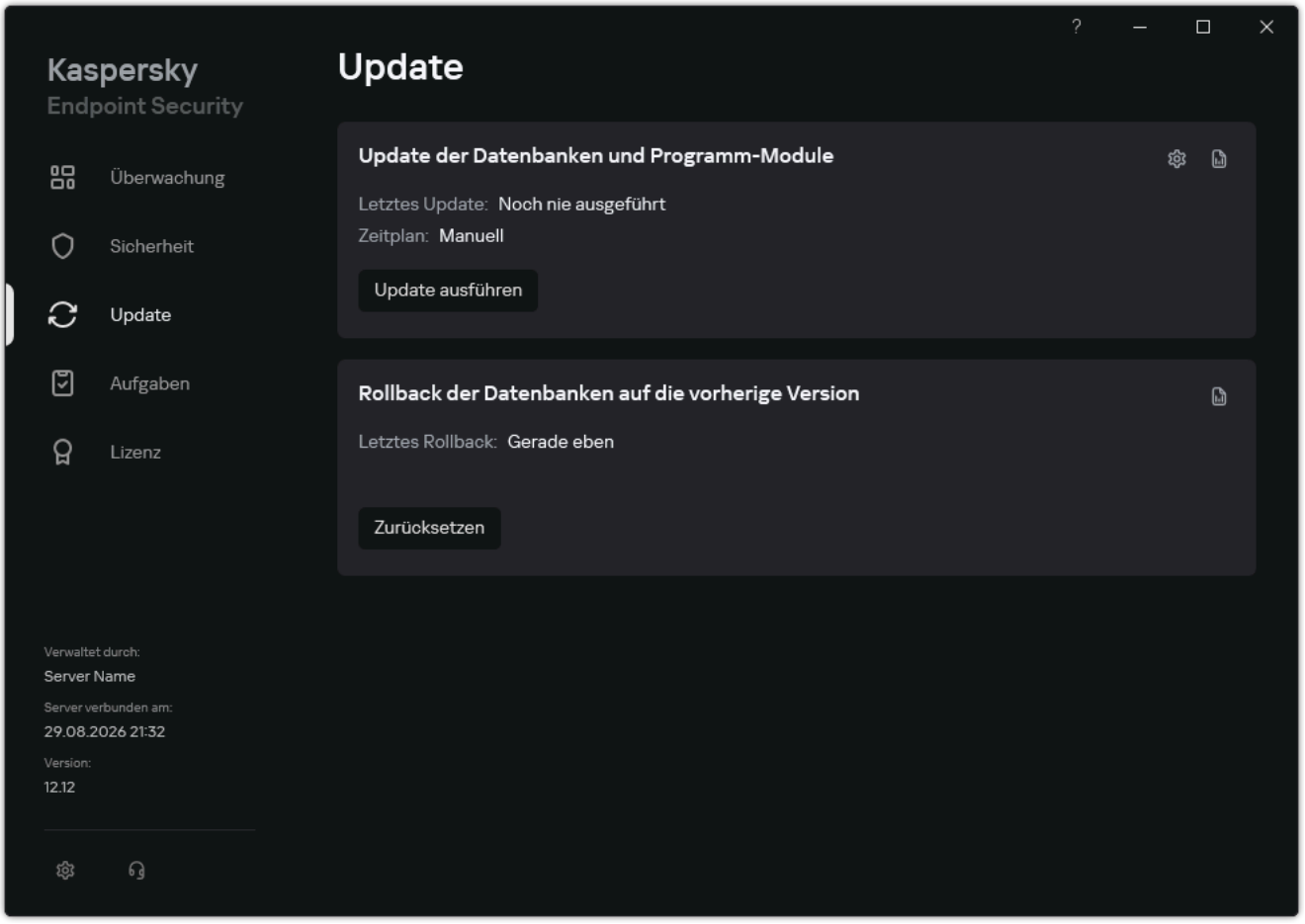
8. Standardmäßig führt Kaspersky Endpoint Security die Aufgabe im manuellen Modus aus.

9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die App-Oberfläche das Update für Kaspersky Endpoint Security aus dem angegebenen Serverspeicher

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

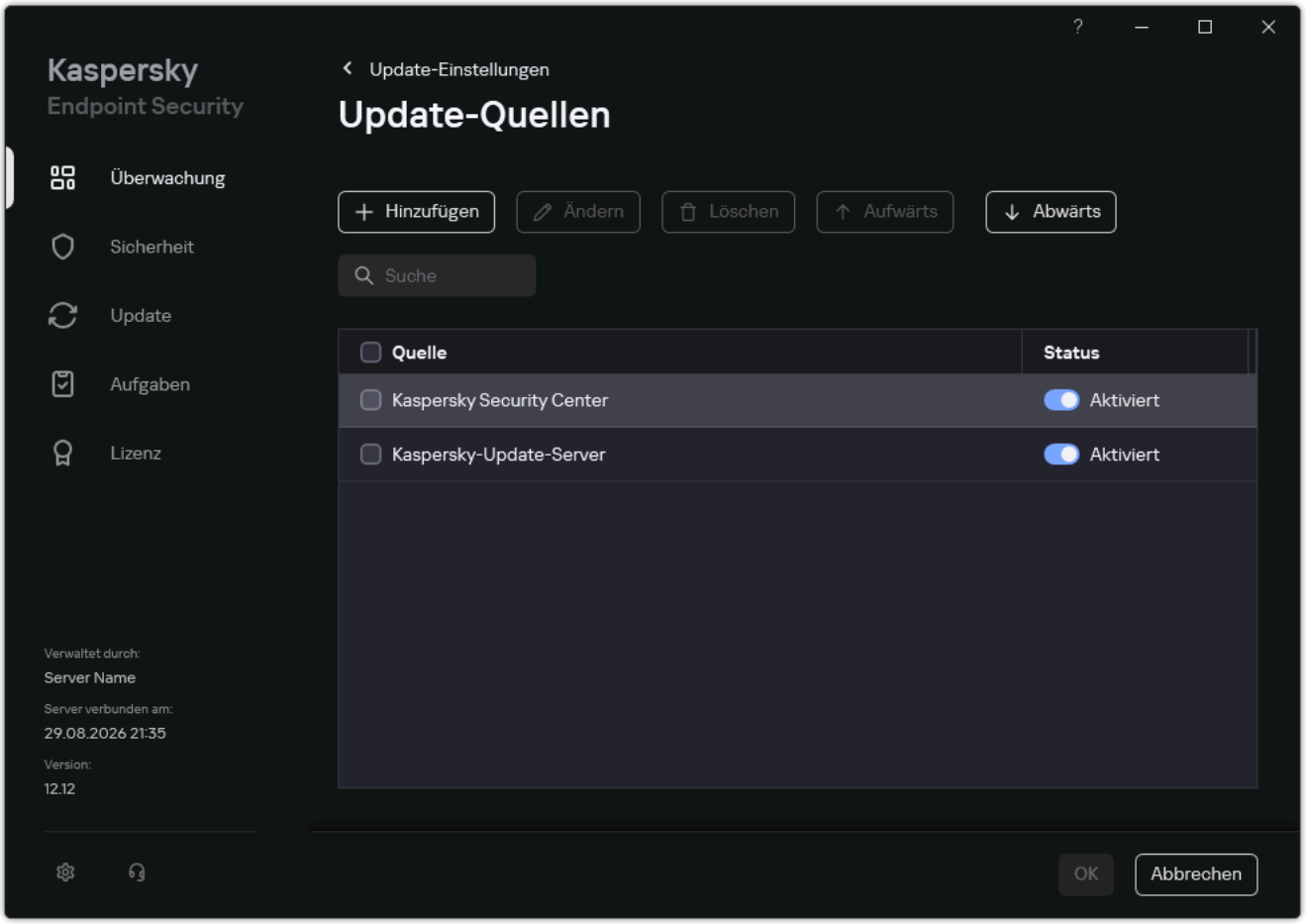
   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Klicken Sie im Eigenschaftenfenster auf **Update-Quellen anpassen**.

4. Stellen Sie sicher, dass in der Liste der Update-Quellen das Update von der Quelle **Kaspersky Security Center** aktiviert ist. Außerdem muss die Quelle **Kaspersky Security Center** die höchste Priorität haben.

5. Fügen Sie bei Bedarf die Update-Quellen hinzu:

   a. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.



Update-Quellen

   a. Geben Sie die Adresse des FTP- oder HTTP-Servers, Netzwerkordners oder lokalen Ordners an, in den Kaspersky Security Center das Update-Paket, das von den Kaspersky-Update-Servern heruntergeladen wurde, kopieren soll.

      Die Adresse der Update-Quelle muss mit der Adresse übereinstimmen, die im Feld **Ordner zum Speichern von Updates** angegeben wurde, als der Update-Download in den Serverspeicher konfiguriert wurde (Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*).

   b. Klicken Sie auf **Auswählen**.

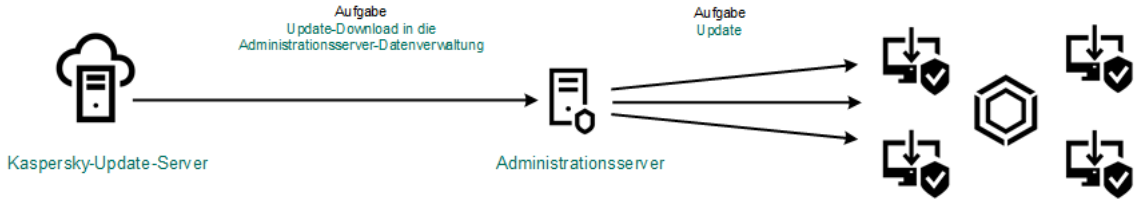
   Sie können eine Update-Quelle ausschließen, ohne sie aus der Liste der Update-Quellen zu entfernen. Setzen Sie dazu den Umschalter neben dem Objekt auf „Aus“.

6. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

Wenn ein Computer durch Kaspersky Security Center verwaltet wird, kann der Ausführungsmodus für die Aufgabe *Update der Datenbanken und Programm-Module* nicht konfiguriert werden. Die Aufgabe kann nur manuell ausgeführt werden.

7. Speichern Sie die vorgenommenen Änderungen.



Update aus dem Serverspeicher

Update aus dem gemeinsamen Ordner

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update der Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus einem gemeinsamen Ordner erfolgen soll. Dazu lädt ein Computer des lokalen Unternehmensnetzwerks die Update-Pakete vom Administrationsserver für Kaspersky Security Center oder von den Kaspersky-Update-Servern herunter und kopiert das heruntergeladene Update-Paket in einen gemeinsamen Ordner. In diesem Fall können die übrigen Computer des lokalen Unternehmensnetzwerks das Update-Paket aus dem gemeinsamen Ordner abrufen.

Die Version und Lokalisierung der Anwendung Kaspersky Endpoint Security, die das Update-Paket in einen freigegebenen Ordner kopiert, muss mit der Version und Lokalisierung der Anwendung übereinstimmen, die Datenbanken aus dem freigegebenen Ordner aktualisiert. Bei abweichenden Versionen oder Lokalisierungen der Anwendungen kann das Datenbanken-Update fehlschlagen.

Um das Update der Datenbanken und Programm-Module aus einem gemeinsamen Ordner einzurichten, sind folgende Schritte erforderlich:

1. Update der Datenbanken und Programm-Module aus einem Serverspeicher einzurichten.

2. Kopieren des Update-Pakets in einen gemeinsamen Ordner auf einem Computer des lokalen Firmennetzwerks aktivieren

   So aktivieren Sie über Verwaltungskonsole (MMC) das Kopieren des Update-Pakets in den gemeinsamen Ordner

   1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

   2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.

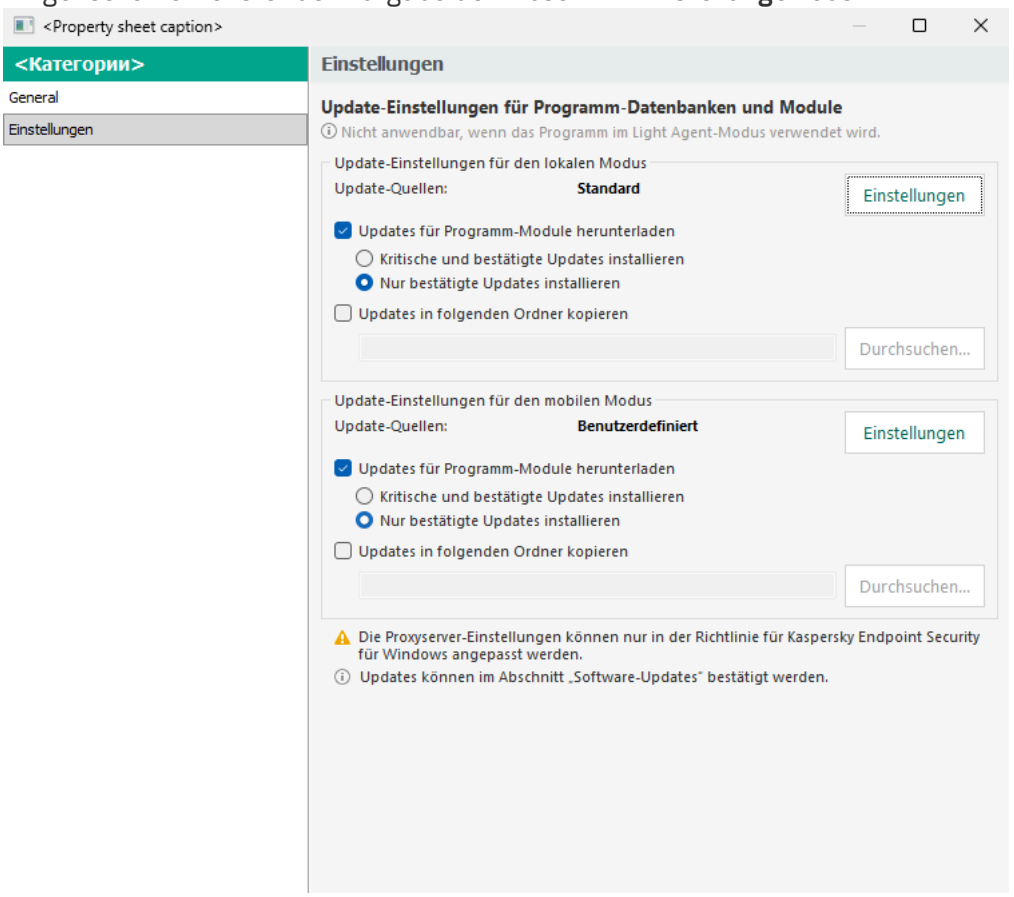
      Die Aufgabe *Update der Datenbanken und Programm-Module* muss einem bestimmten Computer zugewiesen werden, der als Update-Quelle dienen soll.

   3. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

      Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.



Einstellungen der Aufgabe Update der Datenbanken und Programm-Module

5. Klicken Sie im Block **Update-Einstellungen für den lokalen Modus** auf **Einstellungen**.

6. Passen Sie die Update-Quellen an.

   Als Update-Quellen können die Kaspersky-Update-Server, der Administrationsserver für Kaspersky Security Center oder andere FTP- oder HTTP-Server, lokale Ordner oder Netzwerkordner dienen.

7. Aktivieren Sie das Kontrollkästchen **Updates in folgenden Ordner kopieren**.

8. Geben Sie im Feld **Ordnerpfad** den UNC-Pfad des gemeinsamen Ordners an (z. B. `\\<server name>\KLSHARE\Updates`).

   Wenn das Feld leer bleibt, kopiert Kaspersky Endpoint Security das Update-Paket in den Ordner `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über Web Console und Cloud Console das Kopieren des Update-Pakets in den gemeinsamen Ordner

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

Die Aufgabe *Update* muss einem bestimmten Computer zugewiesen werden, der als Update-Quelle dienen soll.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Lokaler Modus** aus.

4. Passen Sie die Update-Quellen an.

   Als Update-Quellen können die Kaspersky-Update-Server, der Administrationsserver für Kaspersky Security Center oder andere FTP- oder HTTP-Server, lokale Ordner oder Netzwerkordner dienen.

5. Aktivieren Sie das Kontrollkästchen **Updates in folgenden Ordner kopieren**.

6. Geben Sie im Feld **Pfad** den UNC-Pfad des gemeinsamen Ordners an (z. B. `\\<server name>\KLSHARE\Updates`).

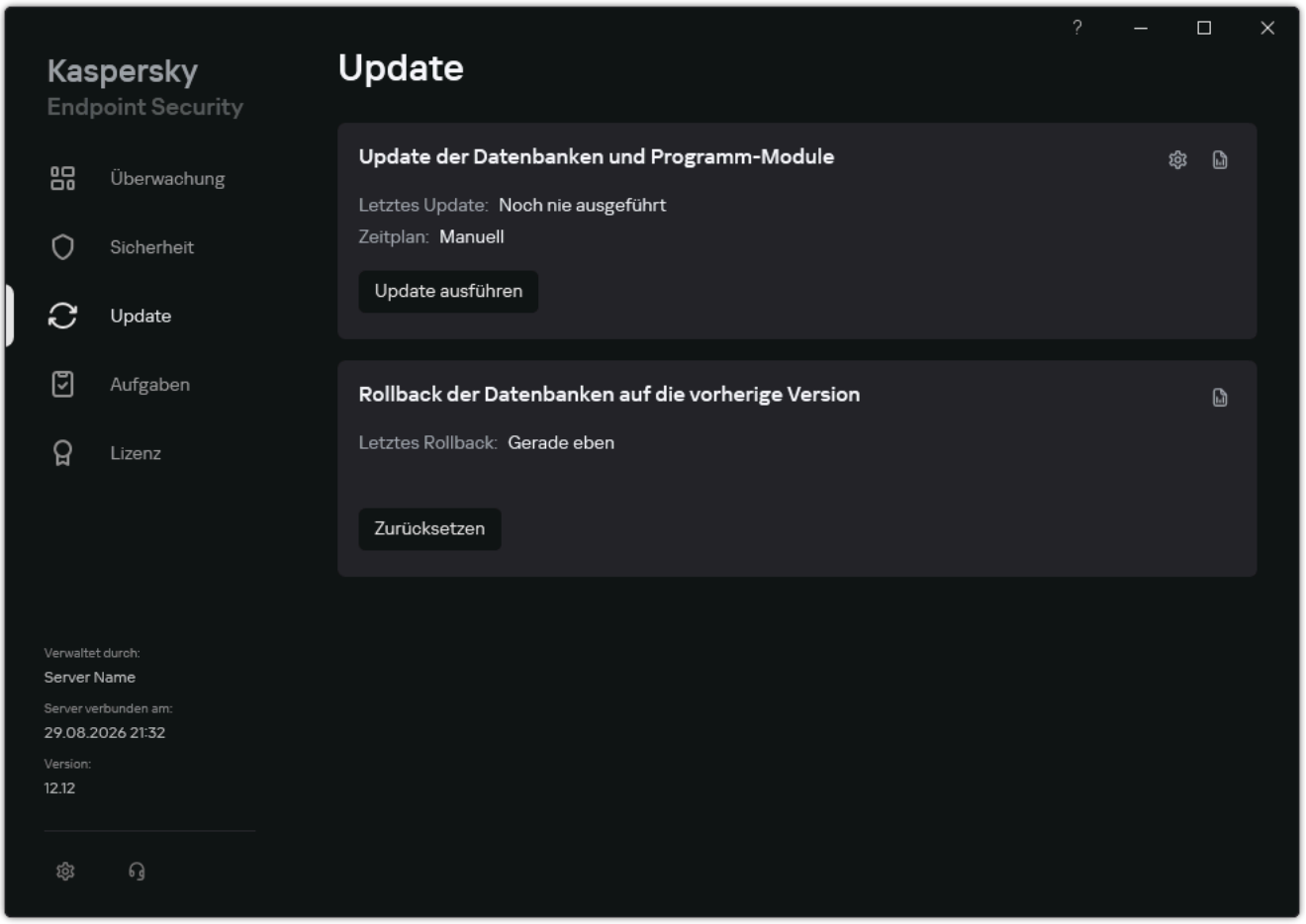
   Wenn das Feld leer bleibt, kopiert Kaspersky Endpoint Security das Update-Paket in den Ordner `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über die Benutzeroberfläche das Kopieren des Update-Pakets in den gemeinsamen Ordner

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Aktivieren Sie im Block **Verteilung von Updates** das Kontrollkästchen **Updates in folgenden Ordner kopieren**.

4. Geben Sie den UNC-Pfad des gemeinsamen Ordners an (z. B. `\\<server name>\KLSHARE\Updates`).

5. Speichern Sie die vorgenommenen Änderungen.

3. Anpassen des Updates für Datenbanken und Programm-Module aus dem festgelegten gemeinsamen Ordner für die Verteilung an die übrigen Computer des lokalen Unternehmensnetzwerks.

So konfigurieren Sie über die Verwaltungskonsole (MMC) die Updates aus dem gemeinsamen Ordner

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Update der Datenbanken und Programm-Module**.

4. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

5. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Update der Datenbanken und Programm-Module** aus.

Schritt 2. Update-Quellen auswählen

Fügen Sie als neue Update-Quelle einen gemeinsamen Ordner hinzu. Die Adresse der Quelle muss mit der Adresse übereinstimmen, die Sie zuvor im Feld **Ordnerpfad** angegeben haben, als Sie das Kopieren des Update-Pakets in einen gemeinsamen Ordner angepasst haben. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Die Aufgabe *Update der Datenbanken und Programm-Module* muss den übrigen Computern des lokalen Unternehmensnetzwerks zugewiesen werden, unter Ausnahme des Computers, der als Update-Quelle dient.

Schritt 4: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie eine Benutzerkonto für den Start der Aufgabe *Update der Datenbanken und Programm-Module* aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

Schritt 5. Zeitplan des Aufgabenstarts anpassen

Passen Sie einen Zeitplan für den Aufgabenstart an, beispielsweise manuell oder nachdem die Antiviren-Datenbanken in den Speicher geladen wurden.

Schritt 6. Aufgabennamen festlegen

Geben Sie den Namen der Aufgabe an, z. B. *Update aus einem gemeinsamen Ordner*.

Schritt 7. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Dadurch wird auf den Benutzercomputern die Update-Aufgabe nach dem festgelegten Zeitplan ausgeführt.

So konfigurieren Sie über Web Console und Cloud Console die Updates aus dem gemeinsamen Ordner

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

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

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Update aus einem gemeinsamen Ordner*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

   > Die Aufgabe *Update* muss den übrigen Computern des lokalen Unternehmensnetzwerks zugewiesen werden, unter Ausnahme des Computers, der als Update-Quelle dient.

4. Wählen Sie Geräte aus; berücksichtigen Sie dabei den ausgewählten Aufgabenbereich. Gehen Sie dann zum nächsten Schritt.

5. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabentabelle angezeigt.

6. Klicken Sie auf die neu erstellte Aufgabe *Update*.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

7. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Lokaler Modus** aus.

8. Klicken Sie im Block **Update-Quellen** auf **Hinzufügen**.

9. Geben Sie im folgenden Fenster den Pfad des gemeinsamen Ordners an.

   > Die Adresse der Quelle muss mit der Adresse übereinstimmen, die zuvor im Feld **Pfad** angegeben wurde, als das Kopieren des Update-Pakets in einen gemeinsamen Ordner angepasst wurde (s. Anleitung oben).

10. Klicken Sie auf **OK**.

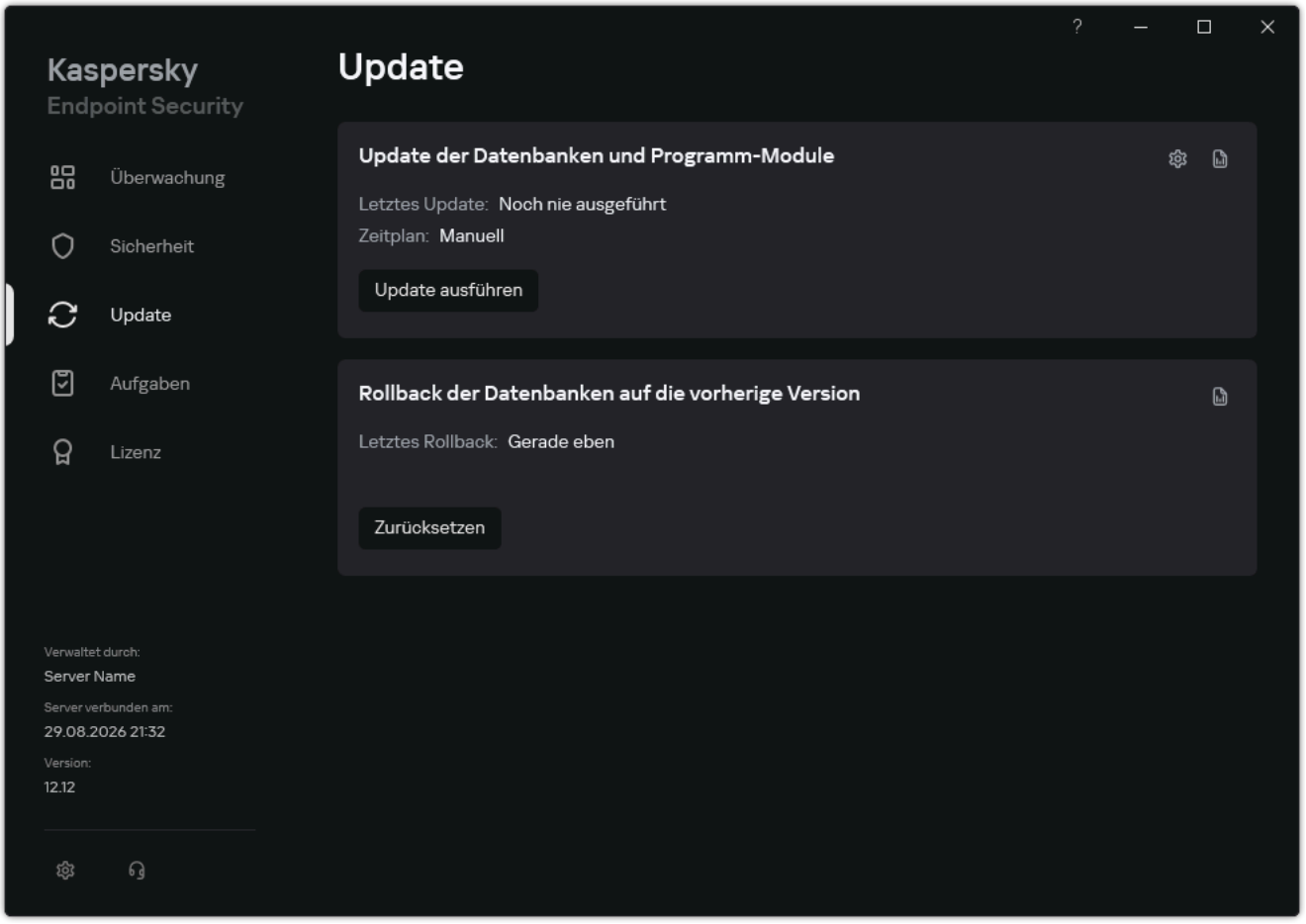
11. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

12. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die Benutzeroberfläche die Updates aus dem gemeinsamen Ordner

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Klicken Sie auf **Update-Quellen anpassen**.

4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

5. Geben Sie im folgenden Fenster den Pfad des gemeinsamen Ordners an.

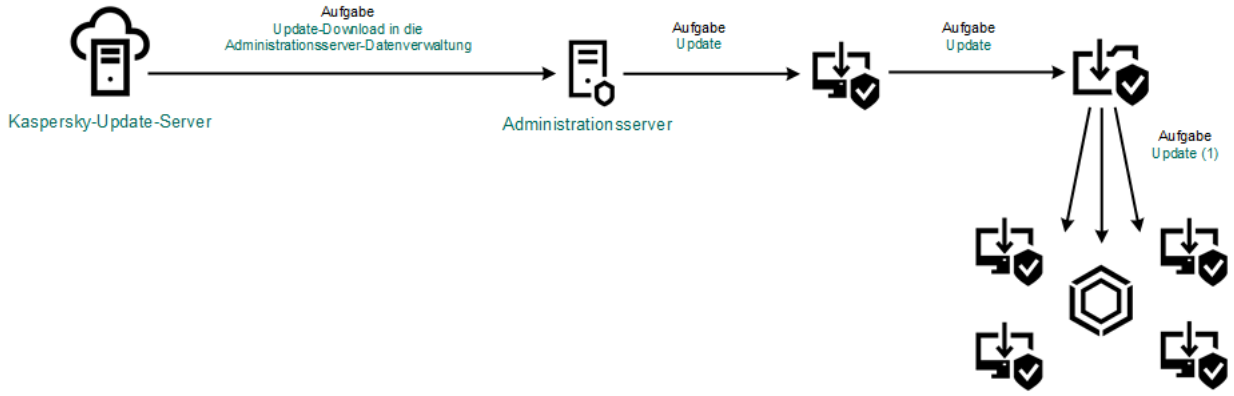
   Die Adresse der Quelle muss mit der Adresse übereinstimmen, die zuvor angegeben wurde, als das Kopieren des Update-Pakets in einen gemeinsamen Ordner angepasst wurde (s. Anleitung oben).

6. Klicken Sie auf **Auswählen**.

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

8. Speichern Sie die vorgenommenen Änderungen.



Update aus dem gemeinsamen Ordner

Update mithilfe von Kaspersky Update Utility

Um Internet-Datenverkehr einzusparen, können Sie festlegen, dass das Update für Datenbanken und Programm-Module auf den Computern des lokalen Unternehmensnetzwerks aus einem gemeinsamen Ordner mithilfe des Hilfsprogramms Kaspersky Update Utility erfolgen soll. Dazu lädt ein Computer des lokalen Unternehmensnetzwerks die Update-Pakete vom Administrationsserver für Kaspersky Security Center oder von den Kaspersky-Update-Servern herunter und kopiert die heruntergeladenen Update-Pakete mithilfe des Hilfsprogramms in einen gemeinsamen Ordner. In diesem Fall können die übrigen Computer des lokalen Unternehmensnetzwerks das Update-Paket aus dem gemeinsamen Ordner abrufen.

Die Version und Lokalisierung der Anwendung Kaspersky Endpoint Security, die das Update-Paket in einen freigegebenen Ordner kopiert, muss mit der Version und Lokalisierung der Anwendung übereinstimmen, die Datenbanken aus dem freigegebenen Ordner aktualisiert. Bei abweichenden Versionen oder Lokalisierungen der Anwendungen kann das Datenbanken-Update fehlschlagen.

Um das Update der Datenbanken und Programm-Module aus einem gemeinsamen Ordner einzurichten, sind folgende Schritte erforderlich:

1. Update der Datenbanken und Programm-Module aus einem Serverspeicher einzurichten.

2. Installation von Kaspersky Update Utility auf einem der Computer des lokalen Unternehmensnetzwerks.

3. Kopieren des Update-Pakets in einen gemeinsamen Ordner anpassen in den Einstellungen von Kaspersky Update Utility.

   Kaspersky Update Utility kann von der Website des Technischen Supports von Kaspersky heruntergeladen werden. Wählen Sie nach der Installation des Hilfsprogramms eine Update-Quelle aus (z. B. die Datenverwaltung des Administrationsservers) und einen gemeinsamen Ordner, in den Kaspersky Update Utility die Update-Pakete kopieren soll. Ausführliche Informationen über die Verwendung von Kaspersky Update Utility finden Sie in der Kaspersky-Wissensdatenbank.

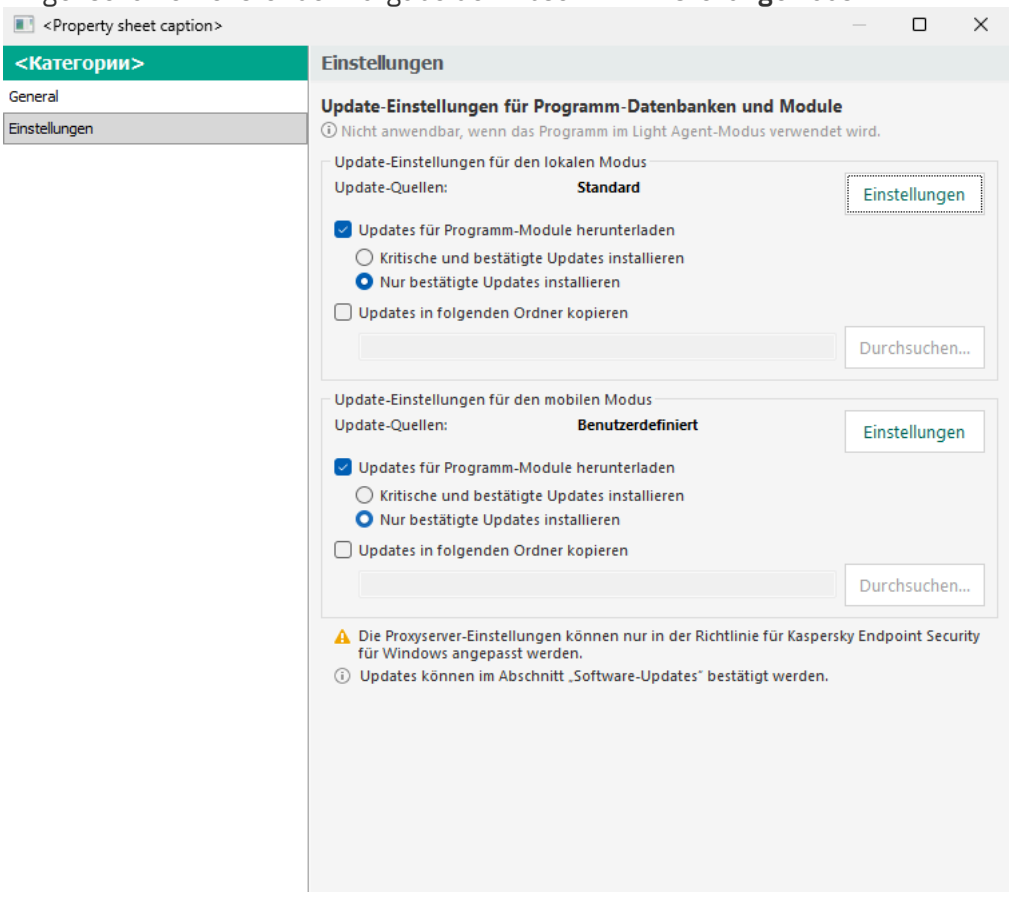
4. Anpassen des Updates für Datenbanken und Programm-Module aus dem festgelegten gemeinsamen Ordner für die Verteilung an die übrigen Computer des lokalen Unternehmensnetzwerks.

So konfigurieren Sie über die Verwaltungskonsole (MMC) die Updates aus dem gemeinsamen Ordner

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.



Einstellungen der Aufgabe Update der Datenbanken und Programm-Module

5. Klicken Sie im Block **Update-Einstellungen für den lokalen Modus** auf **Einstellungen**.
6. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.
7. Geben Sie im folgenden Fenster den UNC-Pfad des freigegebenen Ordners an (z. B. `\\<server name>\KLSHARE\Updates`).

   Die Adresse der Quelle muss mit der Adresse übereinstimmen, die in den Einstellungen von Kaspersky Update Utility angegeben ist.
8. Klicken Sie auf **OK**.

9. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über Web Console und Cloud Console die Updates aus dem gemeinsamen Ordner

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Lokaler Modus** aus.

4. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.

5. Geben Sie im folgenden Fenster den UNC-Pfad des freigegebenen Ordners an (z. B. `\\<server name>\KLSHARE\Updates`).

   > Die Adresse der Quelle muss mit der Adresse übereinstimmen, die in den Einstellungen von Kaspersky Update Utility angegeben ist.

6. Klicken Sie auf **OK**.

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

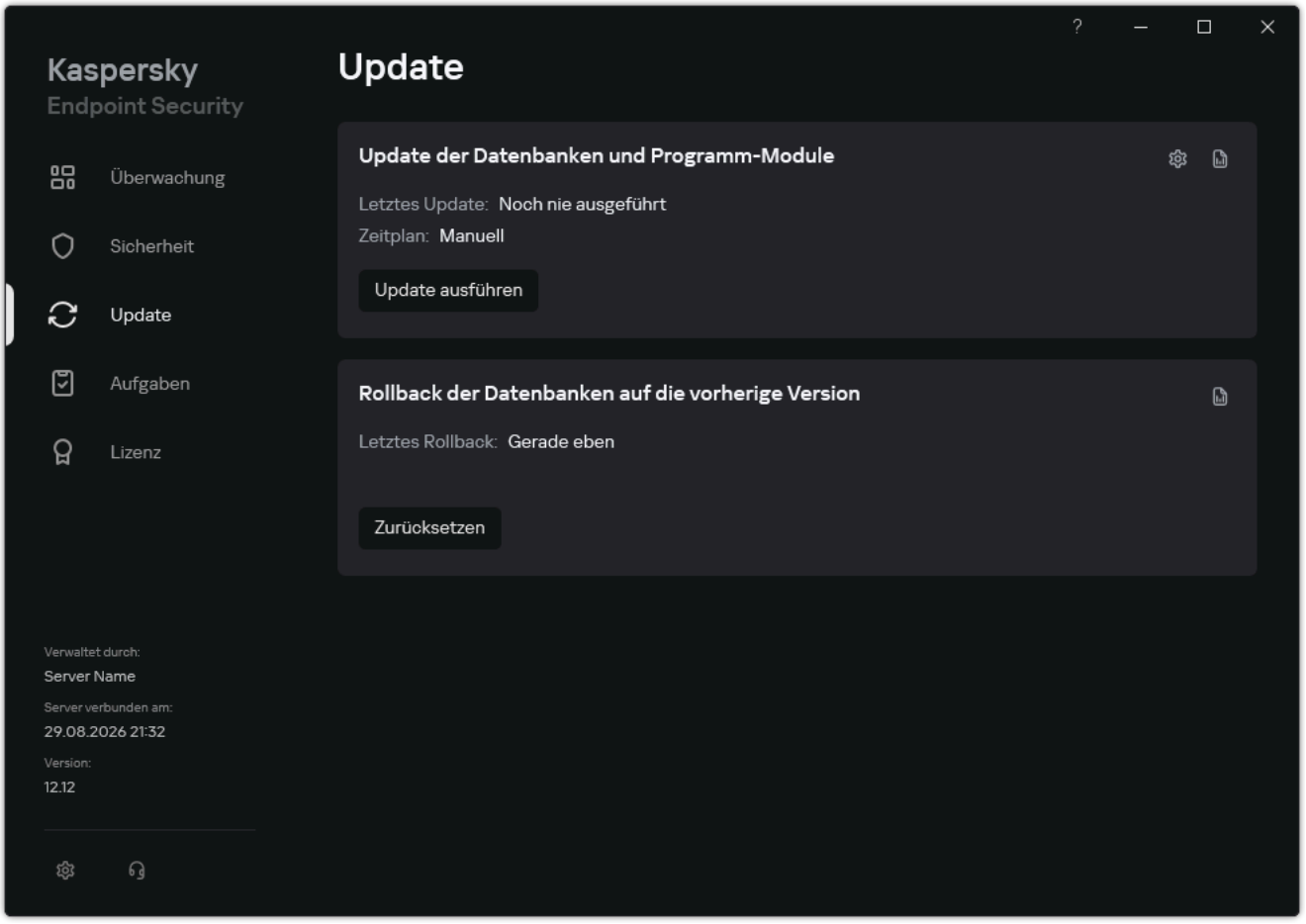
   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die Benutzeroberfläche die Updates aus dem gemeinsamen Ordner

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



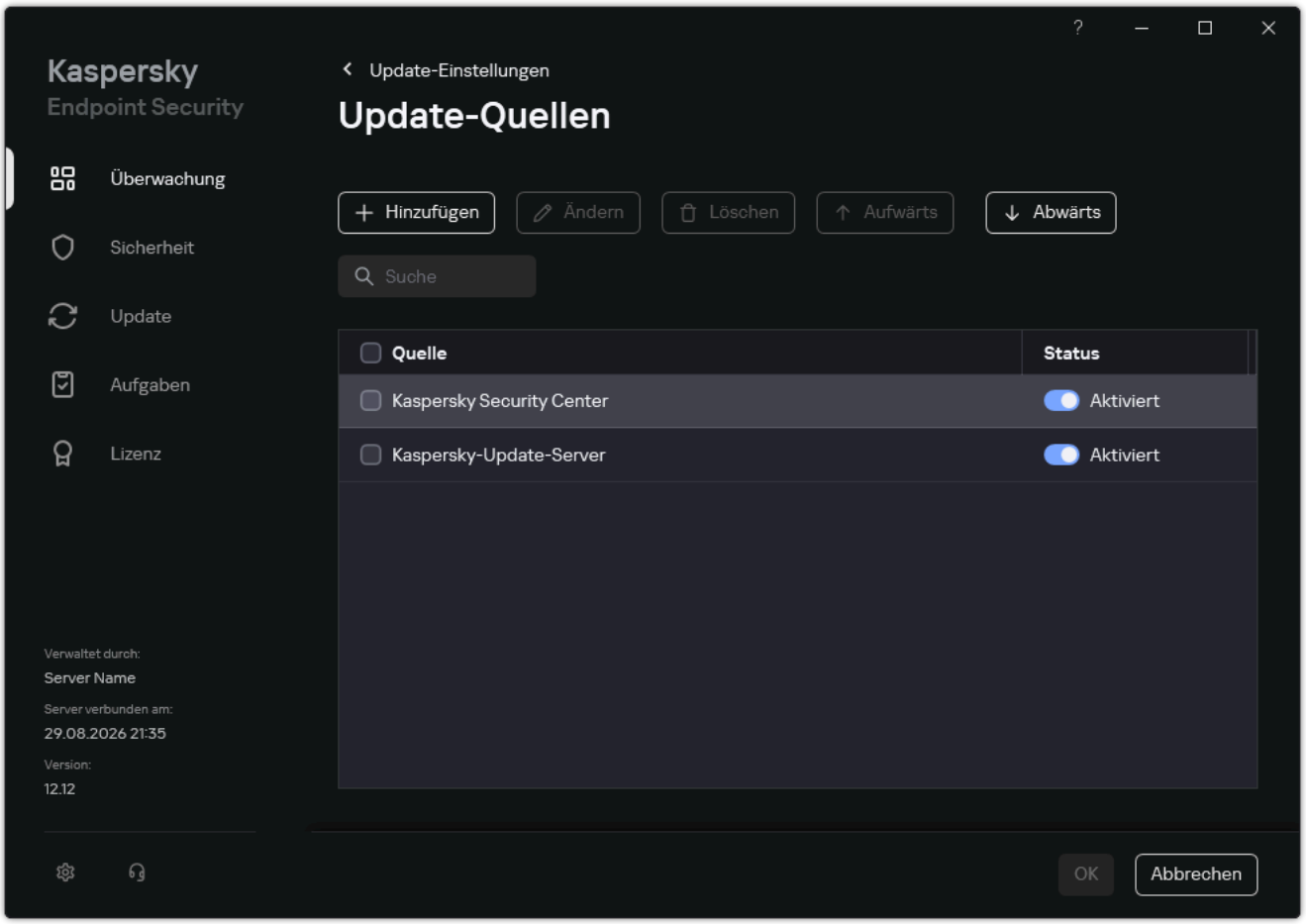
Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Klicken Sie im Eigenschaftenfenster auf **Update-Quellen anpassen**.

4. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.



Update-Quellen

5. Geben Sie den UNC-Pfad des gemeinsamen Ordners an (z. B. `\\<server name>\KLSHARE\Updates`).

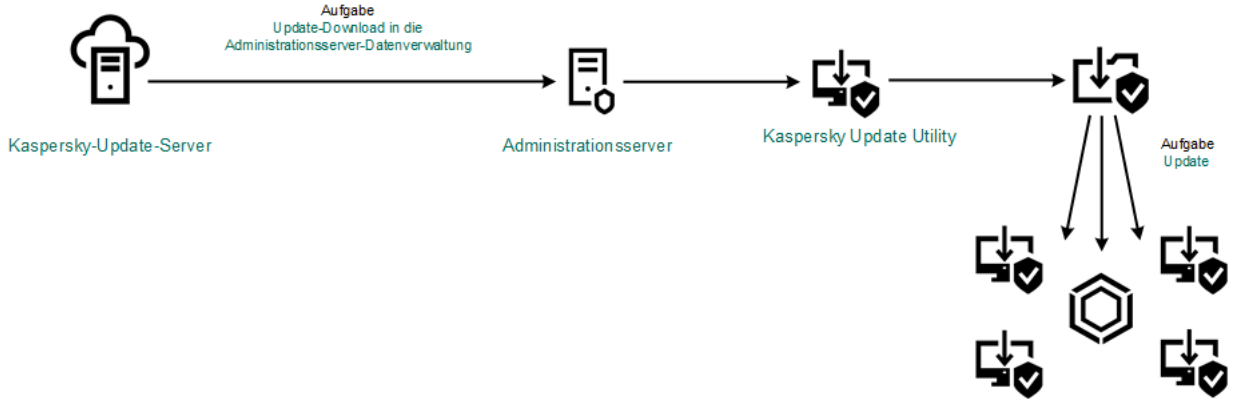
Die Adresse der Quelle muss mit der Adresse übereinstimmen, die in den Einstellungen von Kaspersky Update Utility angegeben ist.

6. Klicken Sie auf **Auswählen**.

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

8. Speichern Sie die vorgenommenen Änderungen.



Update mithilfe von Kaspersky Update Utility

Update im mobilen Modus

Der *mobile Modus* ist ein Modus von Kaspersky Endpoint Security, bei dem ein Computer den Perimeter des Unternehmensnetzwerks verlässt (*mobiler Computer*). Details über die Verwendung von Offline-Computern und über mobile Benutzer finden Sie in der Hilfe zu Kaspersky Security Center.

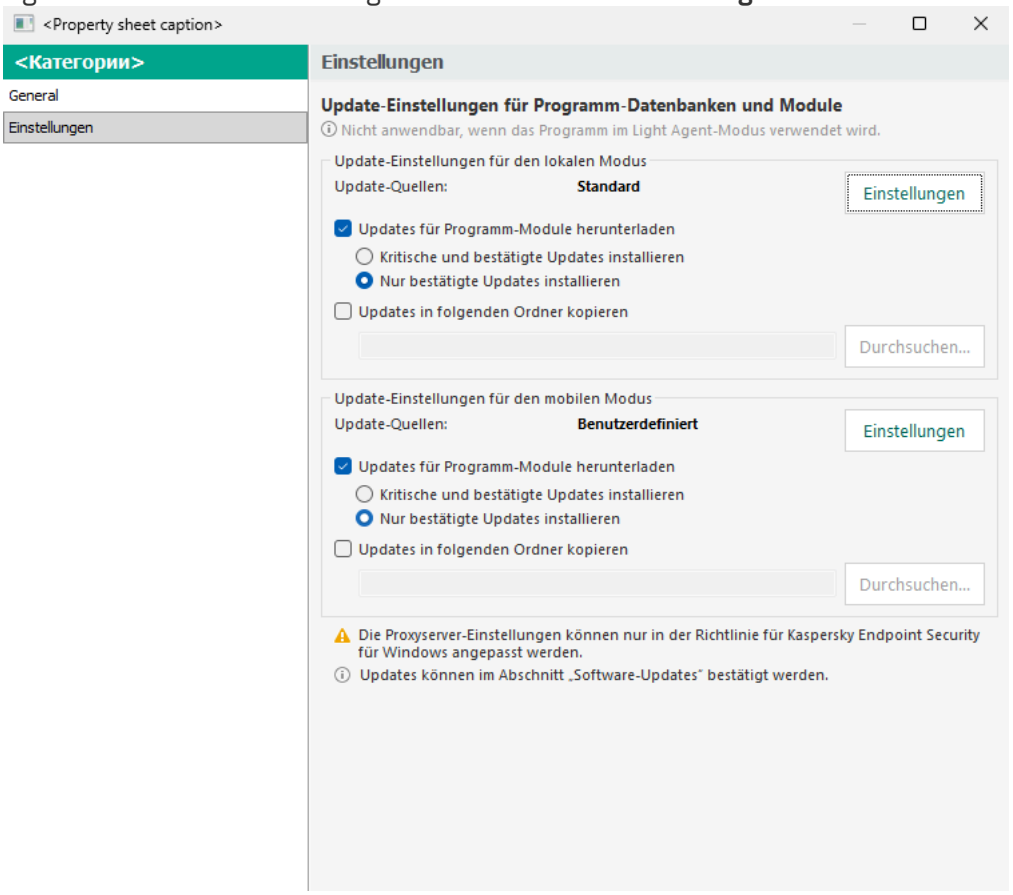
Mobile Computer außerhalb des Unternehmensnetzwerks besitzen keine Verbindung zum Administrationsserver, um die Datenbanken und Programm-Module zu aktualisieren. Im mobilen Modus werden für das Update der Datenbanken und Programm-Module standardmäßig nur die Kaspersky-Update-Server als Update-Quelle verwendet. Die Verwendung eines Proxyservers für die Internetverbindung wird durch eine spezielle mobile Richtlinie festgelegt. Die mobile Richtlinie muss separat erstellt werden. Nachdem Kaspersky Endpoint Security in den mobilen Modus gewechselt hat, wird die Update-Aufgabe alle zwei Stunden gestartet.

So konfigurieren Sie über die Verwaltungskonsole (MMC) die Update-Einstellungen für den mobilen Modus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.



Einstellungen der Aufgabe Update der Datenbanken und Programm-Module

5. Klicken Sie im Block **Update-Einstellungen für den mobilen Modus** auf **Einstellungen**.

6. Konfigurieren Sie die Update-Quellen. Als Update-Quellen können die Kaspersky-Update-Server oder andere FTP- oder HTTP-Server, lokale Ordner oder Netzwerkordner dienen.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über Web Console und Cloud Console die Update-Einstellungen für den mobilen Modus

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Mobiler Modus** aus.

4. Konfigurieren Sie die Update-Quellen. Als Update-Quellen können die Kaspersky-Update-Server oder andere FTP- oder HTTP-Server, lokale Ordner oder Netzwerkordner dienen.

5. Speichern Sie die vorgenommenen Änderungen.

Dadurch werden die Datenbanken und Programm-Module auf den Benutzercomputern bei einem Wechsel in den mobilen Modus aktualisiert.

Update-Aufgabe starten und abbrechen

Eine Update-Aufgabe für Kaspersky Endpoint Security kann unabhängig vom gewählten Startmodus für die Update-Aufgabe jederzeit gestartet oder abgebrochen werden.

Gehen Sie folgendermaßen vor, um die Update-Aufgabe zu starten oder zu beenden:

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.

2. Klicken Sie in der Kachel **Update der Datenbanken und Programm-Module** auf **Update**, wenn Sie die Update-Aufgabe starten möchten.

   Kaspersky Endpoint Security wird mit dem Update der Programm-Module und Datenbanken beginnen. Das Programm zeigt den Aufgabenfortschritt, die Größe der heruntergeladenen Dateien und die Update-Quelle an. Sie können die Aufgabe jederzeit beenden, indem Sie auf die Schaltfläche **Update abbrechen** klicken.

Um über die vereinfachte Programmoberfläche eine Update-Aufgabe zu starten oder abzubrechen:

1. Klicken Sie mit der rechten Maustaste auf das Programmsymbol, das sich im Infobereich der Taskleiste befindet.
2. Führen Sie im Kontextmenü in der Dropdown-Liste **Aufgaben** eine der folgenden Aktionen aus:
   - Wählen Sie eine nicht gestartete Update-Aufgabe aus, um sie zu starten.
   - Wählen Sie eine laufende Update-Aufgabe aus, um sie abzubrechen.
   - Wählen Sie eine angehaltene Update-Aufgabe aus, um sie erneut zu starten.

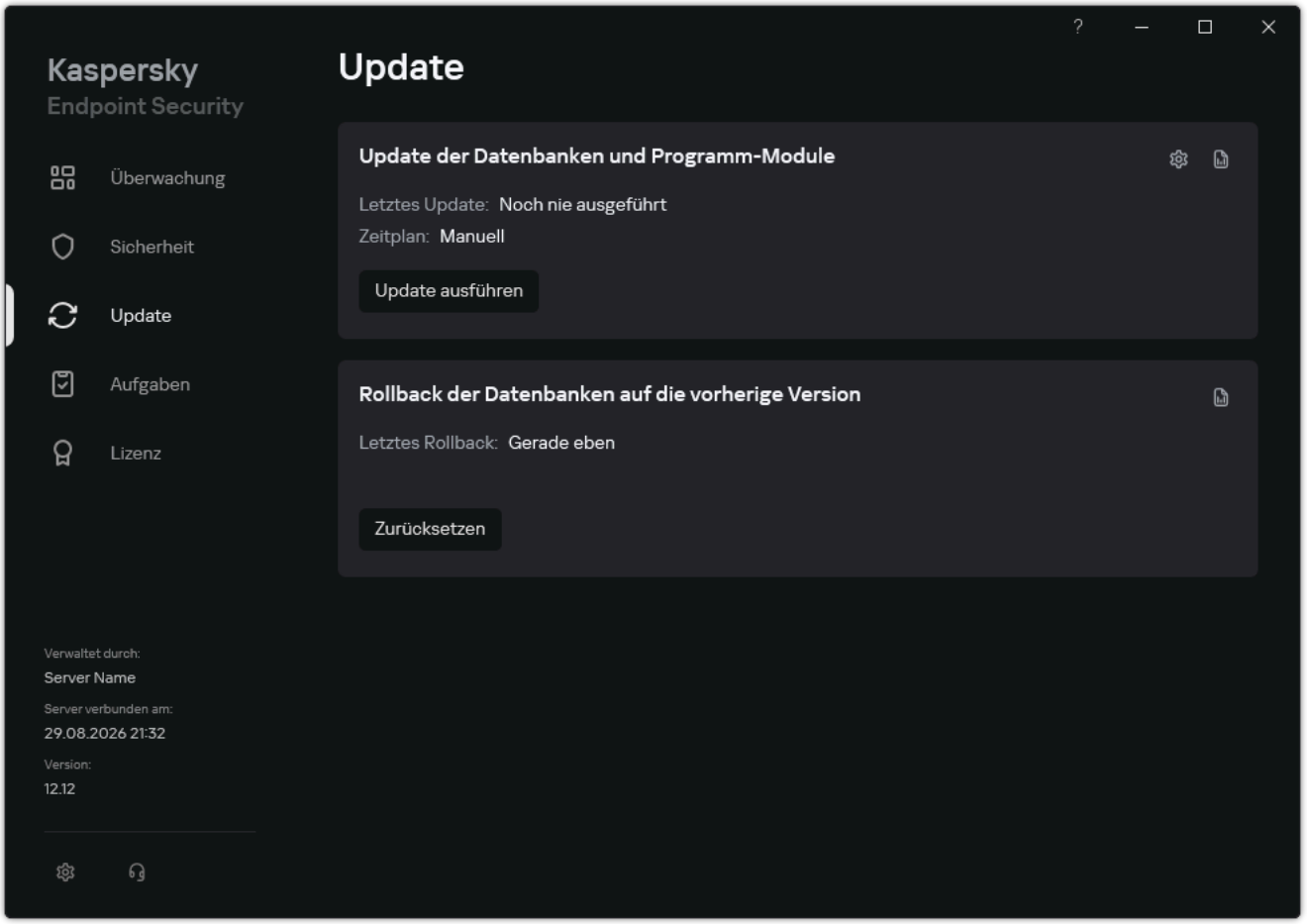
Update-Aufgabe mit den Rechten eines anderen Benutzers starten

Die Update-Aufgabe für Kaspersky Endpoint Security wird standardmäßig im Namen des Benutzers gestartet, mit dessen Rechten Sie sich im Betriebssystem angemeldet haben. Das Update für Kaspersky Endpoint Security kann aber auch aus einer Update-Quelle erfolgen, für welche der Benutzer keine Zugriffsrechte besitzt (z. B. aus einem gemeinsamen Ordner, welcher das Update-Paket enthält) oder für welche die Verwendung der Authentifizierung auf dem Proxyserver nicht angepasst ist. Sie können in den Programmeinstellungen einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Update-Aufgabe für Kaspersky Endpoint Security im Namen dieses Benutzers starten.

Gehen Sie folgendermaßen vor, um die Update-Aufgabe mit den Rechten eines anderen Benutzers zu starten:

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Klicken Sie auf **Updates der Datenbanken starten mit den Rechten des Benutzers**.

4. Wählen Sie im folgenden Fenster den Punkt **Folgender Benutzer** aus.

5. Geben Sie die Konto-Anmeldedaten eines Benutzers mit den erforderlichen Berechtigungen für den Zugriff auf die Update-Quelle ein.

6. Speichern Sie die vorgenommenen Änderungen.

Startmodus für die Update-Aufgabe wählen

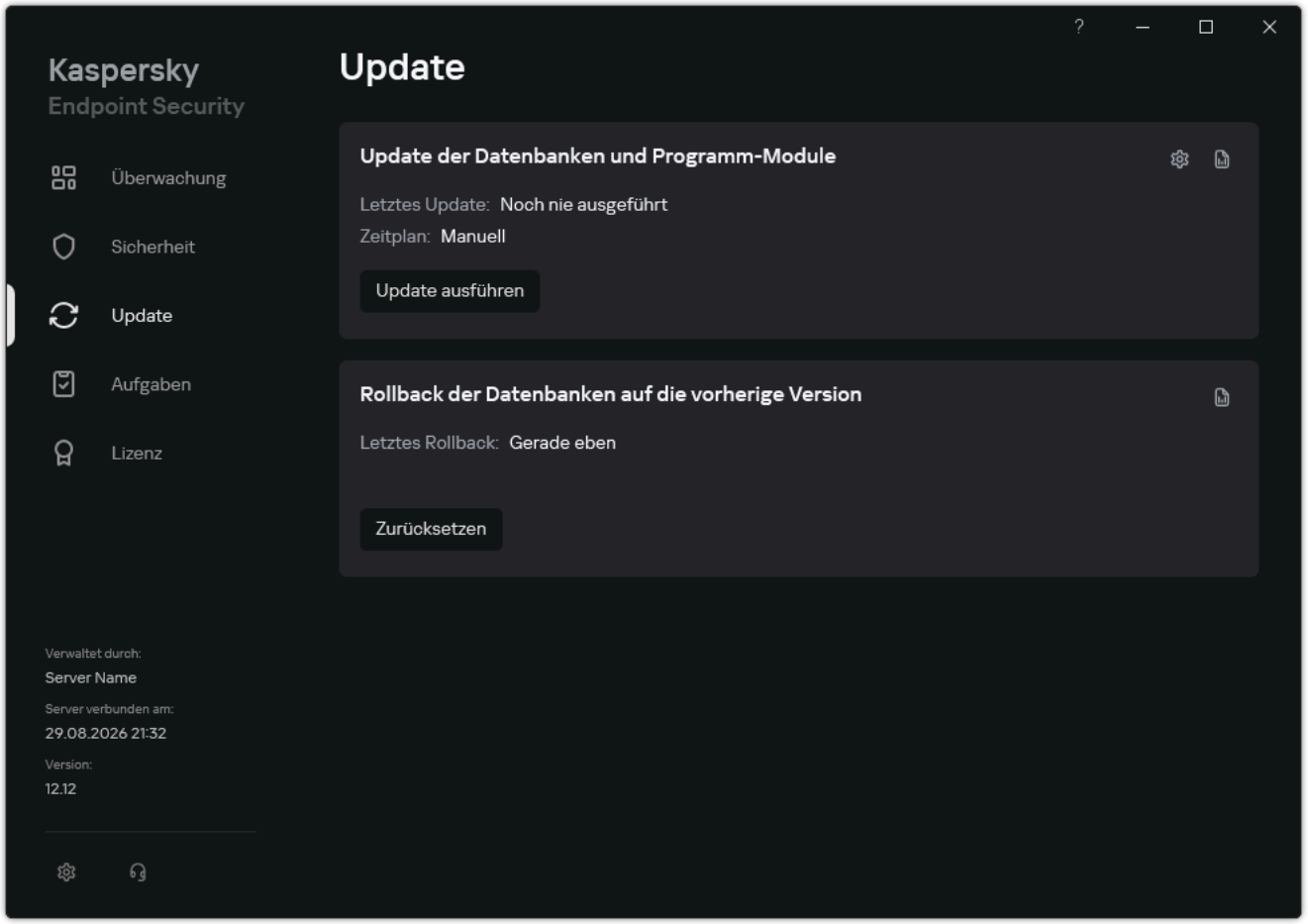
Ist der Start der Update-Aufgabe nicht möglich (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet ist), können Sie festlegen, dass der Start einer übersprungenen Update-Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Sie können festlegen, dass der Start der Update-Aufgabe nach dem Start des Programms aufgeschoben wird. Dies ist möglich, wenn Sie für die Update-Aufgabe den Startmodus **Nach Zeitplan** gewählt haben und der Startzeitpunkt von Kaspersky Endpoint Security mit dem Startzeitplan der Update-Aufgabe übereinstimmt. Die Update-Aufgabe wird erst dann gestartet, wenn der vorgegebene Zeitraum nach dem Start von Kaspersky Endpoint Security verstrichen ist.

Um einen Startmodus für die Update-Aufgabe zu wählen, gehen Sie wie folgt vor:

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Klicken Sie auf **Startmodus**.

4. Wählen Sie im folgenden Fenster den Ausführungsmodus der Update-Aufgabe aus:

   - Wählen Sie die Option **Automatisch**, damit Kaspersky Endpoint Security beim Start der Update-Aufgabe berücksichtigt, ob an der Update-Quelle ein Update-Paket vorhanden ist. Die Häufigkeit, mit der Kaspersky Endpoint Security nach einem neuen Update-Paket sucht, kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken.

   - Wählen Sie die Option **Manuell**, wenn Sie die Update-Aufgabe manuell starten möchten.

   - Um einen Zeitplan für die Ausführung der Update-Aufgabe anzupassen, können Sie weitere Optionen auswählen. Konfigurieren Sie die erweiterten Einstellungen für den Start der Update-Aufgabe:

     - Geben Sie im Feld **Ausführung nach Programmstart aufschieben für n Minuten** an, für welchen Zeitraum Sie den Start der Update-Aufgabe nach dem Start von Kaspersky Endpoint Security aufschieben möchten.

     - Aktivieren Sie das Kontrollkästchen **Geplante Untersuchung am nächsten Tag starten, falls Computer ausgeschaltet ist**, damit Kaspersky Endpoint Security übersprungene Update-Aufgaben bei der nächsten Gelegenheit ausführt. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen.

5. Speichern Sie die vorgenommenen Änderungen.

Update-Quelle hinzufügen

Eine *Update-Quelle* ist eine Ressource, die Updates der Datenbanken und der Programm-Module für Kaspersky Endpoint Security enthält.

Zu den Update-Quellen gehören der Kaspersky-Security-Center-Server, die Kaspersky-Update-Server sowie Netzwerkordner und lokale Ordner.

Wenn die Kaspersky-Update-Server nicht verfügbar sind, kann Kaspersky Endpoint Security alternative Domänen verwenden, um die Datenbanken und Programm-Module zu aktualisieren. Ausführliche Informationen finden Sie in der Wissensdatenbank der Technischen Supports.

Standardmäßig enthält die Liste für Update-Quellen den Server von Kaspersky Security Center und die Kaspersky-Update-Server. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden.

Kaspersky Endpoint Security unterstützt keine Updates von HTTPS-Servern, außer es sind Kaspersky-Update-Server.

Wurden mehrere Ressourcen als Update-Quellen gewählt, greift Kaspersky Endpoint Security bei einer Aktualisierung streng der Reihe nach darauf zu. Bei der Update-Aufgabe wird das Update-Paket aus der ersten verfügbaren Update-Quelle verwendet.

Standardmäßig verwendet Kaspersky Endpoint Security den Kaspersky Security Center-Server als primäre Update-Quelle. Dadurch wird beim Update Datenverkehr eingespart. Wenn keine Richtlinie auf den Computer angewendet wird, werden in den Einstellungen der lokalen *Update der Datenbanken und Programm-Module*-Aufgabe die Kaspersky-Server als primäre Update-Quelle ausgewählt, da die Anwendung möglicherweise keinen Zugriff auf den Kaspersky Security Center-Server hat.

Wenn das Programm im Light Agent-Modus ausgeführt wird, wird ein Ordner auf der SVM als Update-Quelle ausgewählt.

So fügen Sie über die Verwaltungskonsole (MMC) eine Update-Quelle hinzu

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

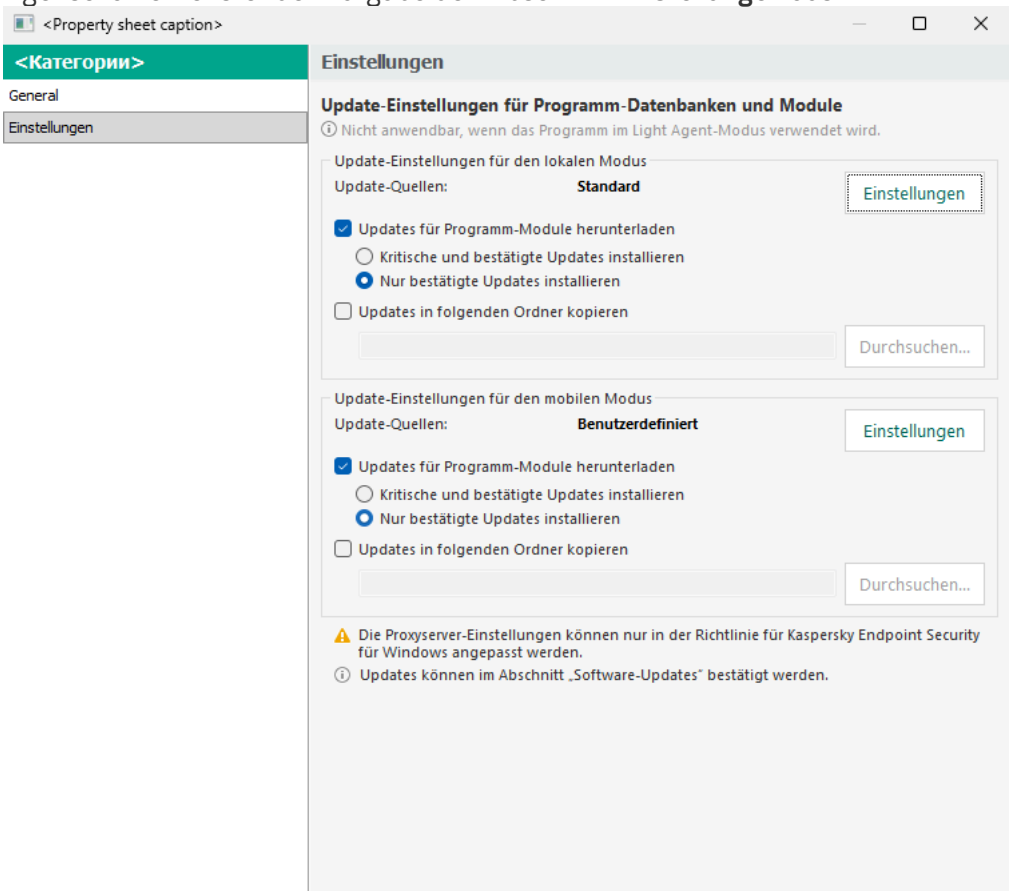
   Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

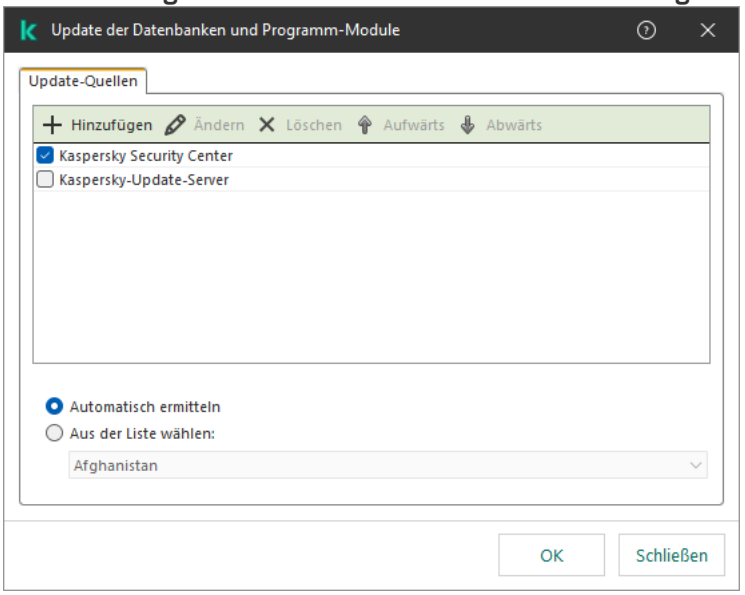
   Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

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



Einstellungen der Aufgabe Update der Datenbanken und Programm-Module

4. Klicken Sie im Block **Update-Einstellungen für den lokalen Modus** auf **Einstellungen**.



Update-Quellen

5. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.

6. Geben Sie im Feld **Update-Quellen** die Adresse des FTP- oder HTTP-Servers, des Netzwerkordners oder lokalen Ordners an, der das Update-Paket enthält.

   Das Format für den Pfad einer Update-Quelle sieht wie folgt aus:

   - Geben Sie für einen FTP- oder HTTP-Server die Webadresse oder die IP-Adresse der Website ein.

     Beispielsweise `http://dnl-01.geo.kaspersky.com/` oder `93.191.13.103`.

     Für einen FTP-Server ist die Angabe der Anmeldeparameter in folgendem Format möglich: `ftp://<Benutzername>:<Kennwort>@<Knoten>:<Port>`.

   - Geben Sie für einen Netzwerkordner den UNC-Pfad ein.

     Beispiel: `\\Server\Share\Update distribution`.

   - Geben Sie für einen lokalen Ordner den vollständigen Ordnerpfad ein.

     Zum Beispiel, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

   Sie können eine Update-Quelle ausschließen, ohne sie aus der Liste der Update-Quellen zu entfernen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

7. Klicken Sie auf **OK**.

8. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

9. Fügen Sie bei Bedarf eine Update-Quelle für den mobilen Modus hinzu. Der *mobile Modus* ist ein Modus von Kaspersky Endpoint Security, bei dem ein Computer den Perimeter des Unternehmensnetzwerks verlässt (*mobiler Computer*).

10. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine Update-Quelle in der Web Console hinzu

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

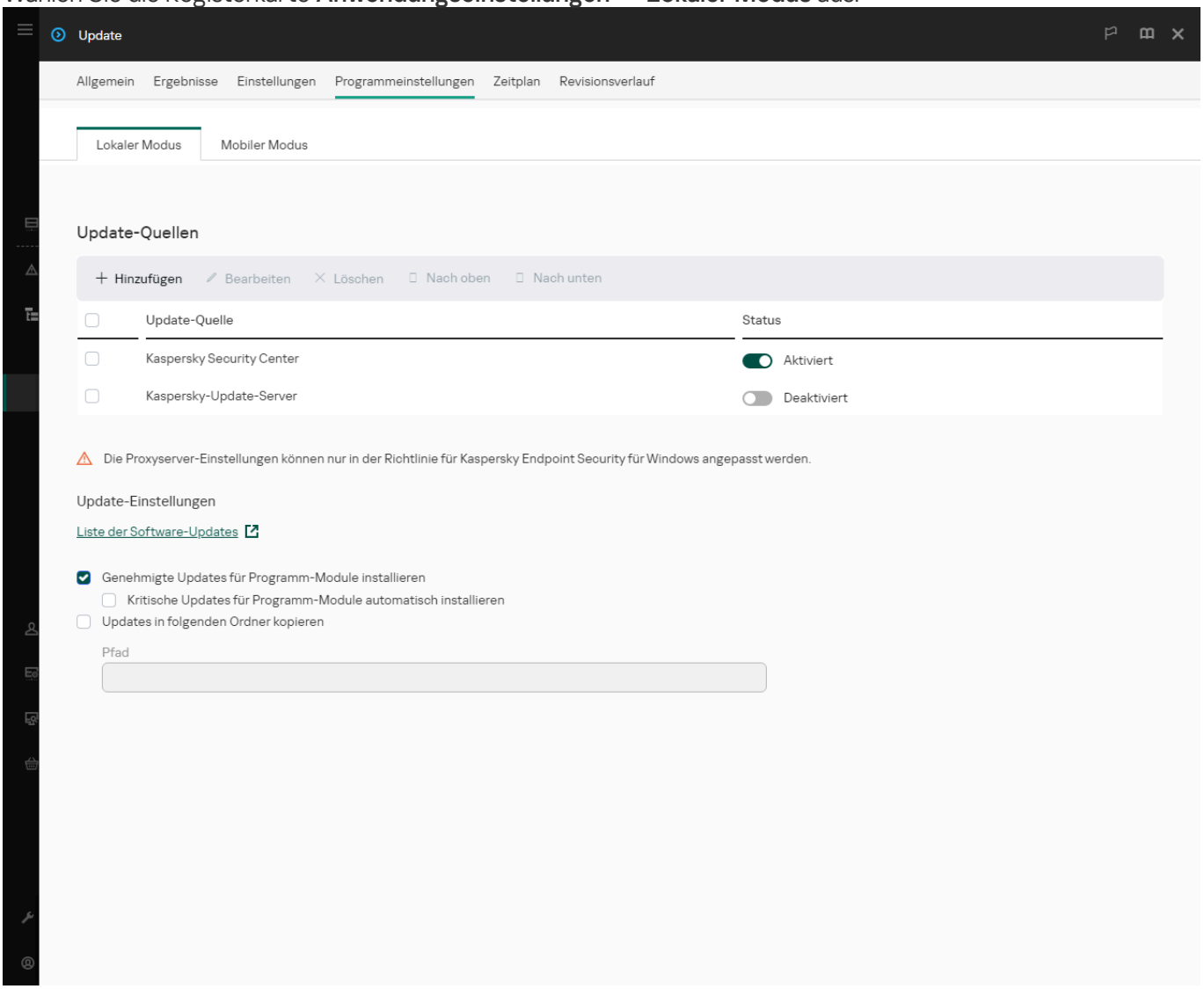
   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Lokaler Modus** aus.



Update-Quellen

4. Klicken Sie in der Liste der Update-Quellen auf **Hinzufügen**.

5. Geben Sie im folgenden Fenster die Adresse des FTP- oder HTTP-Servers, des Netzwerkordners oder lokalen Ordners an, der das Update-Paket enthält.

   Das Format für den Pfad einer Update-Quelle sieht wie folgt aus:

   - Geben Sie für einen FTP- oder HTTP-Server die Webadresse oder die IP-Adresse der Website ein.

     Beispielsweise `http://dnl-01.geo.kaspersky.com/` oder `93.191.13.103`.

Für einen FTP-Server ist die Angabe der Anmeldeparameter in folgendem Format möglich: `ftp://<Benutzername>:<Kennwort>@<Knoten>:<Port>`.

- Geben Sie für einen Netzwerkordner den UNC-Pfad ein.

  Beispiel: `\\Server\Share\Update distribution`.

- Geben Sie für einen lokalen Ordner den vollständigen Ordnerpfad ein.

  Zum Beispiel, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

Sie können eine Update-Quelle ausschließen, ohne sie aus der Liste der Update-Quellen zu entfernen. Setzen Sie dazu den Umschalter neben dem Objekt auf „Aus“.

6. Klicken Sie auf **OK**.

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

   Falls das Update nicht aus der ersten Update-Quelle ausgeführt werden kann, wechselt Kaspersky Endpoint Security automatisch zur nächsten Quelle.

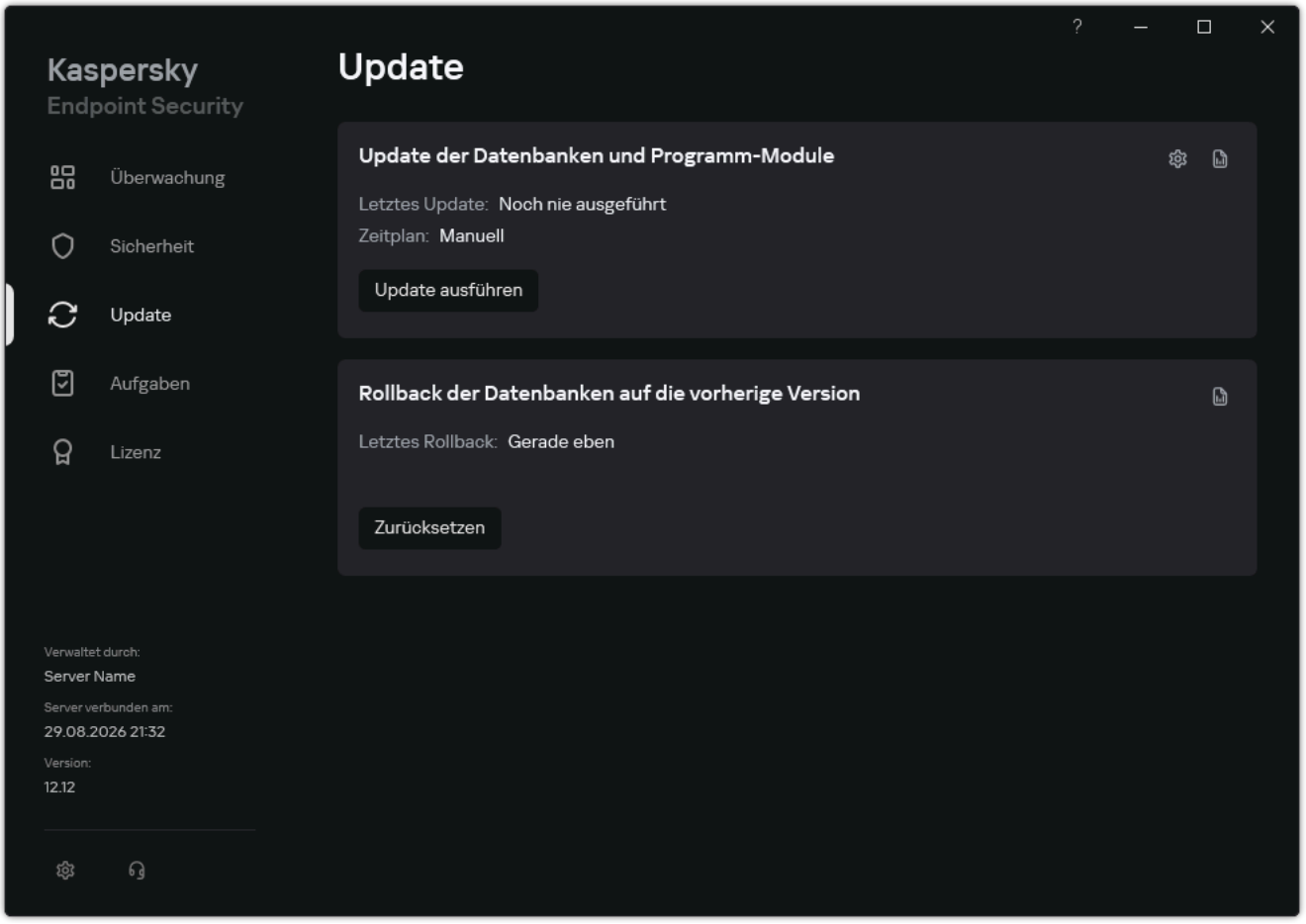
8. Fügen Sie bei Bedarf eine Update-Quelle für den mobilen Modus hinzu. Der *mobile Modus* ist ein Modus von Kaspersky Endpoint Security, bei dem ein Computer den Perimeter des Unternehmensnetzwerks verlässt (*mobiler Computer*).

9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie über die Benutzeroberfläche eine Update-Quelle hinzu

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



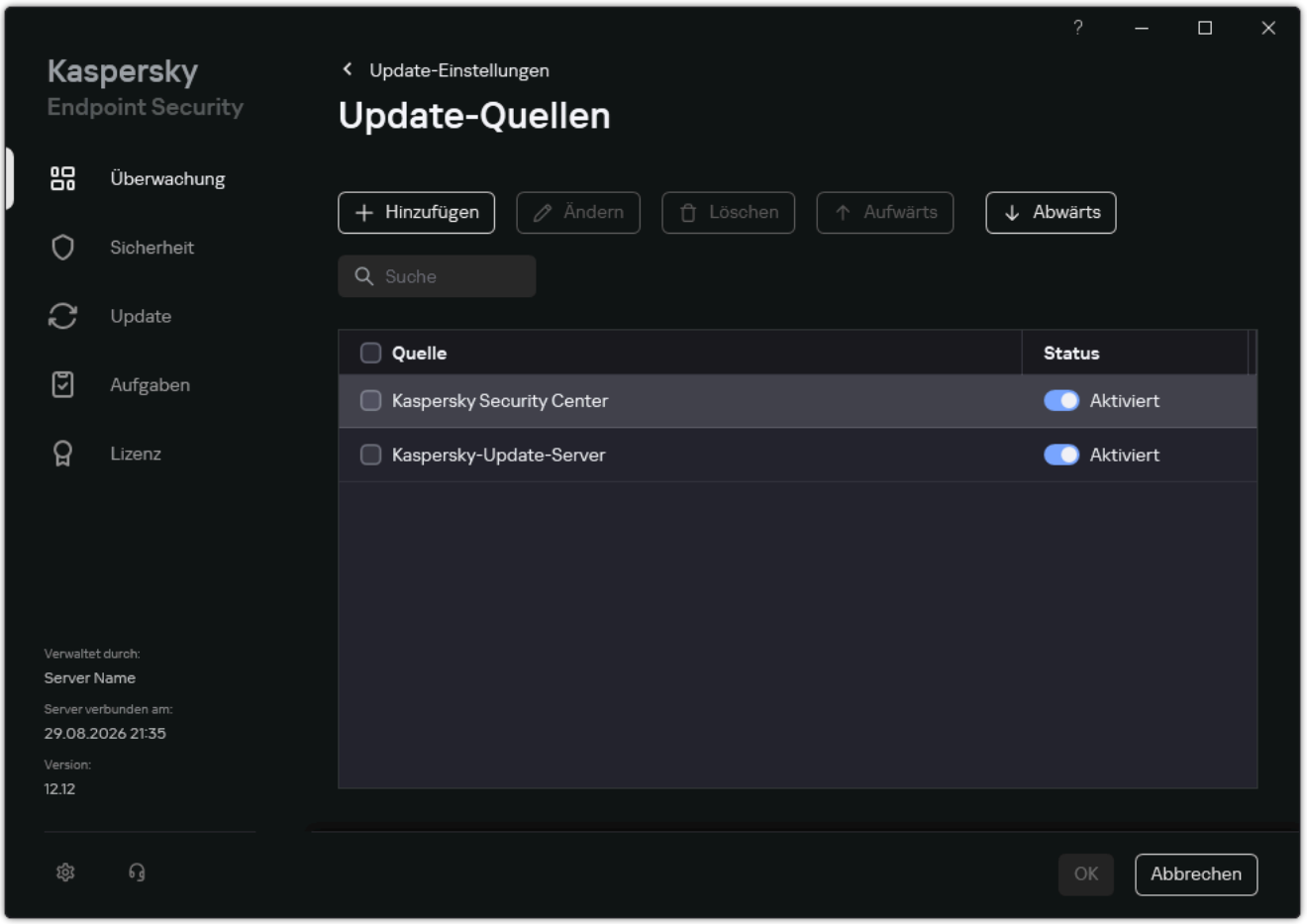
Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Klicken Sie auf **Update-Quellen anpassen**.

4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.



Update-Quellen

5. Geben Sie im folgenden Fenster die Adresse des FTP- oder HTTP-Servers, des Netzwerkordners oder lokalen Ordners an, der das Update-Paket enthält.

   Das Format für den Pfad einer Update-Quelle sieht wie folgt aus:

   - Geben Sie für einen FTP- oder HTTP-Server die Webadresse oder die IP-Adresse der Website ein.

     Beispielsweise `http://dnl-01.geo.kaspersky.com/` oder `93.191.13.103`.

     Für einen FTP-Server ist die Angabe der Anmeldeparameter in folgendem Format möglich: `ftp://<Benutzername>:<Kennwort>@<Knoten>:<Port>`.

   - Geben Sie für einen Netzwerkordner den UNC-Pfad ein.

     Beispiel: `\\Server\Share\Update distribution`.

   - Geben Sie für einen lokalen Ordner den vollständigen Ordnerpfad ein.

     Zum Beispiel, `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

6. Klicken Sie auf **Auswählen**.

7. Passen Sie die Prioritäten der Update-Quellen mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an.

8. Speichern Sie die vorgenommenen Änderungen.

Aktualisierung von Programm-Modulen

Programm-Modul-Updates beheben Fehler, verbessern die Leistung und fügen neue Funktionen hinzu. Wenn ein neues Programm-Modul-Update verfügbar wird, müssen Sie die Installation des Updates bestätigen. Sie können die Installation eines Programm-Modul-Updates entweder in der Programmoberfläche oder im Kaspersky Security Center bestätigen. Sobald ein Update verfügbar ist, zeigt das Programm im Hauptfenster von Kaspersky Endpoint Security eine Meldung an: . Falls für ein Programm-Modul-Update zuerst ein Lizenzvertrag gelesen und bestätigt werden muss, dann installiert das Programm das Update erst nach der Zustimmung zum Lizenzvertrag.

Nach der Installation eines Programm-Updates kann es erforderlich sein, dass Sie Ihren Computer neu starten müssen.

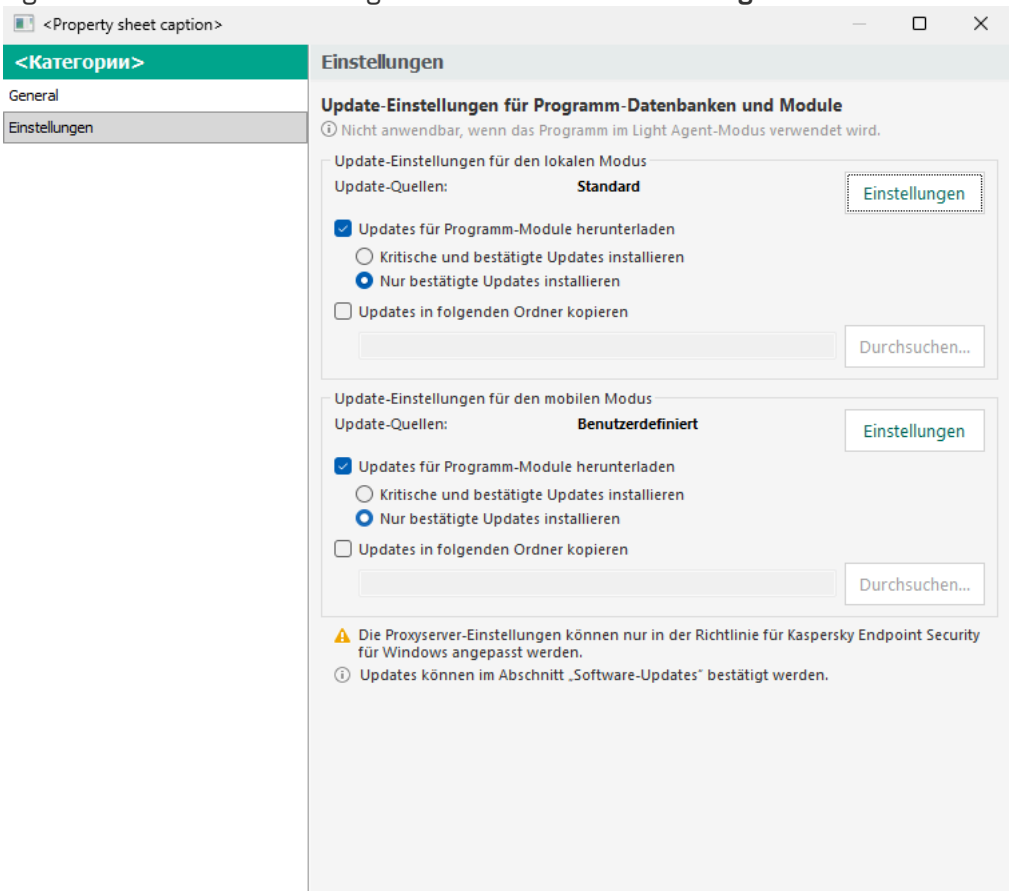
So konfigurieren Sie Programm-Modul-Updates über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.



Einstellungen der Aufgabe Update der Datenbanken und Programm-Module

5. Aktivieren Sie im Block **Update-Einstellungen für den lokalen Modus** das Kontrollkästchen **Updates für Programm-Module herunterladen**.

   Wenn Sie das Herunterladen von Programm-Modul-Updates verhindern möchten, deaktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen** und verbieten Sie die Verwendung lokaler Aufgaben durch Benutzer.

6. Wählen Sie die Programm-Modul-Updates aus, die Sie installieren möchten.

   - **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security zum Einen kritische Updates der Programm-Module automatisch und zum Andern alle übrigen Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde.

   - **Nur bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.

7. Bei Bedarf können Sie Programm-Modul-Updates für den mobilen Modus konfigurieren. Der *mobile Modus* ist ein Modus von Kaspersky Endpoint Security, bei dem ein Computer den Perimeter des Unternehmensnetzwerks verlässt (*mobiler Computer*).

8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Programm-Modul-Updates über die Web Console und Cloud Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

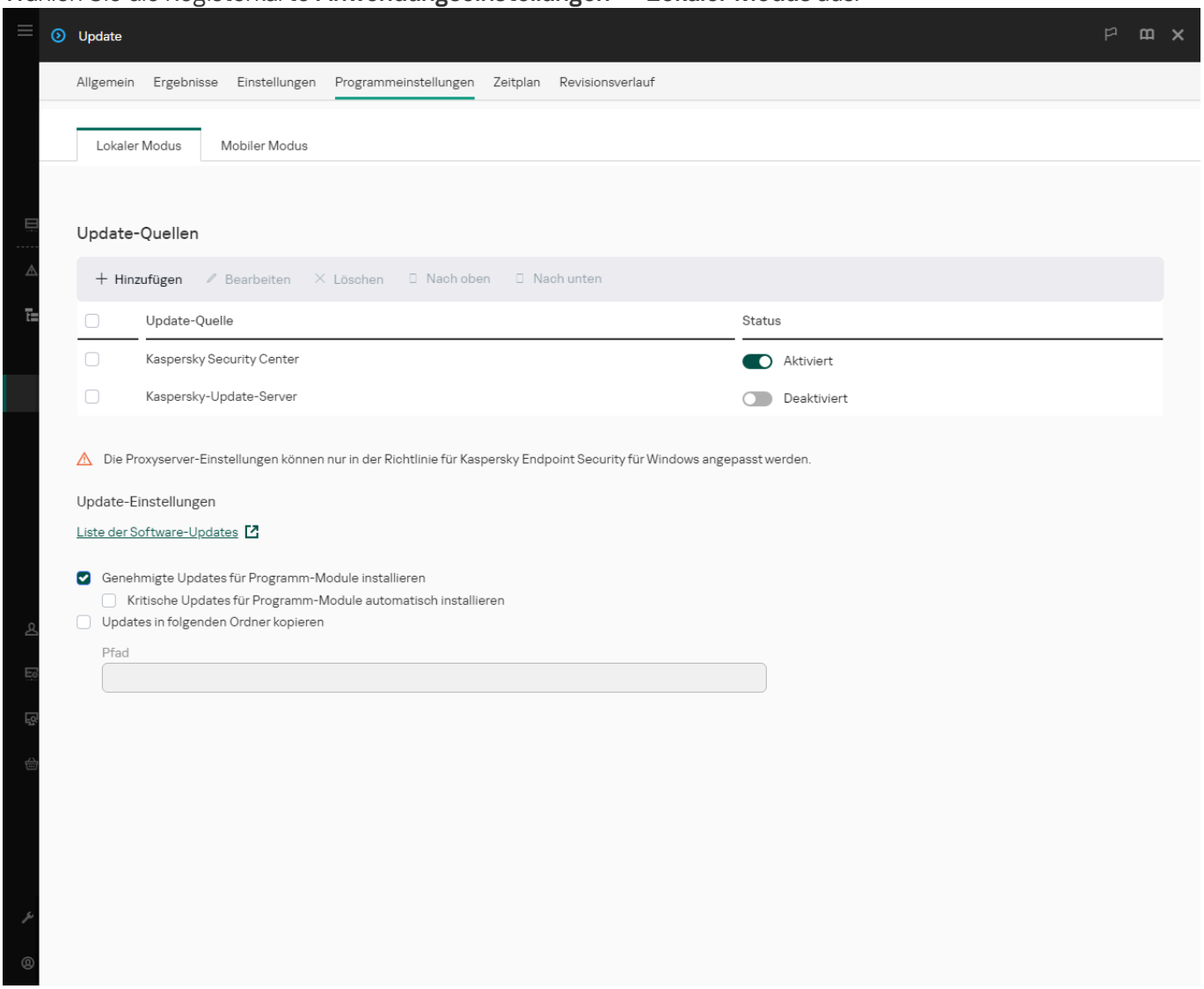
   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Update der Datenbanken und Programm-Module**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Die Aufgabe *Update der Datenbanken und Programm-Module* wird automatisch vom Schnellstartassistenten des Administrationsservers erstellt. Um die Aufgabe *Update der Datenbanken und Programm-Module* zu erstellen, installieren Sie mithilfe des Assistenten das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** → **Lokaler Modus** aus.



Einstellungen der Aufgabe Update

4. Wählen Sie unter **Update-Einstellungen** die zu installierenden Programm-Modul-Updates aus:

   - **Genehmigte Updates für Programm-Module installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.

   - **Kritische Updates für Programm-Module automatisch installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security zum Einen kritische Updates der Programm-Module automatisch und zum Andern alle übrigen Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde.

Wenn Sie das Herunterladen von Programm-Modul-Updates verhindern möchten, deaktivieren Sie die Kontrollkästchen **Genehmigte Updates für Programm-Module installieren** und **Kritische Updates für Programm-Module automatisch installieren** und verbieten Sie die Verwendung lokaler Aufgaben durch Benutzer.

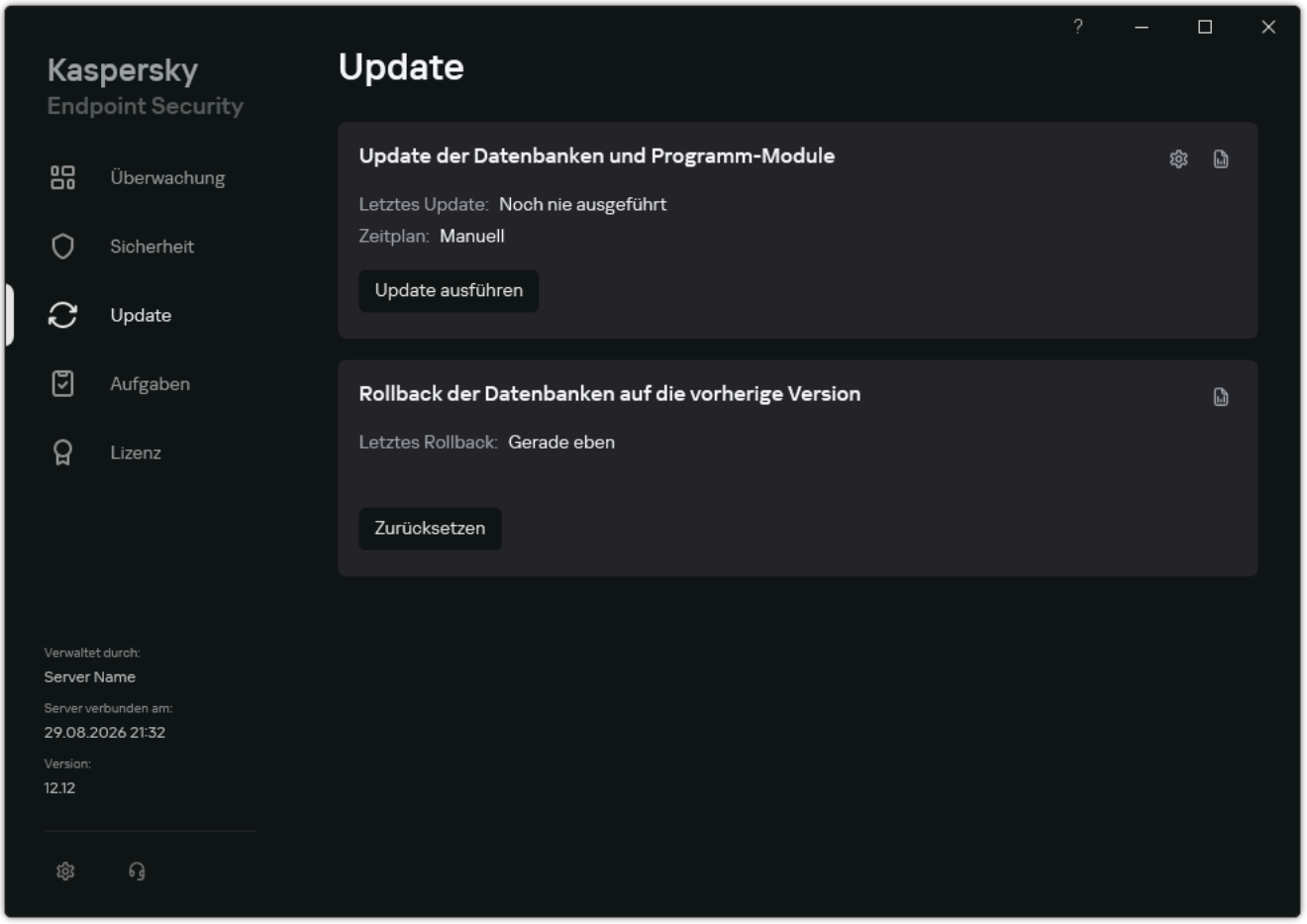
5. Bei Bedarf können Sie Programm-Modul-Updates für den mobilen Modus konfigurieren. Der *mobile Modus* ist ein Modus von Kaspersky Endpoint Security, bei dem ein Computer den Perimeter des Unternehmensnetzwerks verlässt (*mobiler Computer*).

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Programm-Modul-Updates über die Programmoberfläche

Die Gruppenaufgabe *Update der Datenbanken und Programm-Module* kann nicht über die App-Oberfläche konfiguriert werden. Dem Benutzer steht nur die lokale Update-Aufgabe *Update der Datenbanken und Programm-Module* zur Verfügung. Wird die Aufgabe *Update der Datenbanken und Programm-Module* nicht angezeigt, so hat der Administrator die Verwendung lokaler Aufgaben in der Richtlinie verboten.

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Dadurch wird die Aufgabenliste geöffnet. Wählen Sie die Aufgabe *Update der Datenbanken und Programm-Module* aus und klicken Sie auf ⚙.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Aktivieren Sie im Block **Updates für Programm-Module herunterladen und installieren** das Kontrollkästchen **Updates für Programm-Module herunterladen**.

4. Wählen Sie die Programm-Modul-Updates aus, die Sie installieren möchten.

   - **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security zum Einen kritische Updates der Programm-Module automatisch und zum Andern alle übrigen Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde.

   - **Nur bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.

5. Speichern Sie die vorgenommenen Änderungen.

Verwendung eines Proxyservers beim Update

Für den Download von Updates der Datenbanken und Programm-Module kann die Angabe von Proxyserver-Einstellungen erforderlich sein. Wenn mehrere Update-Quellen vorhanden sind, werden die Proxyserver-Einstellungen für alle Quellen verwendet. Wenn für bestimmte Update-Quellen kein Proxyserver erforderlich ist, können Sie die Verwendung des Proxyservers in den Richtlinieneigenschaften deaktivieren. Kaspersky Endpoint Security verwendet den Proxyserver auch für den Zugriff auf Kaspersky Security Network und auf die Aktivierungsserver.

Um die Verbindung mit den Update-Quellen über einen Proxyserver anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptfenster der „Web Console“ auf ⚙.

   Das Eigenschaftsfenster des Administrationsservers wird geöffnet.

2. Wechseln Sie zum Abschnitt **Konfiguration des Internetzugriffs**.

3. Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden**.

4. Passen Sie die Einstellungen für die Verbindung mit dem Proxyserver an: Adresse des Proxyservers, Port und Authentifizierungseinstellungen (Benutzername und Kennwort).

5. Speichern Sie die vorgenommenen Änderungen.

Um die Verwendung des Proxyservers für eine bestimmte Administrationsgruppe zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.

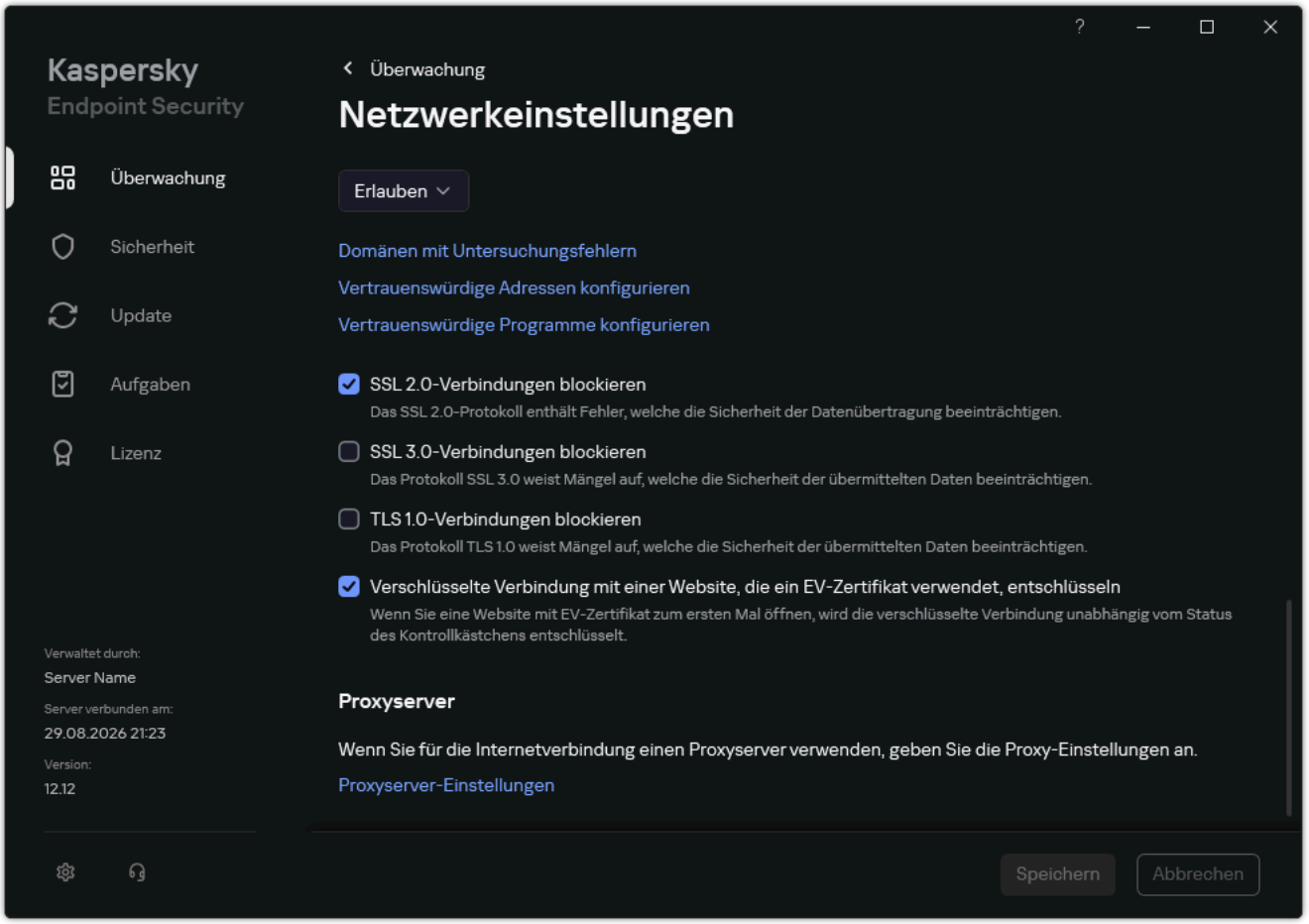
5. Klicken Sie im Block **Proxyserver** auf **Einstellungen**.

6. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Einen Proxyserver für lokale Adressen umgehen**.

7. Speichern Sie die vorgenommenen Änderungen.

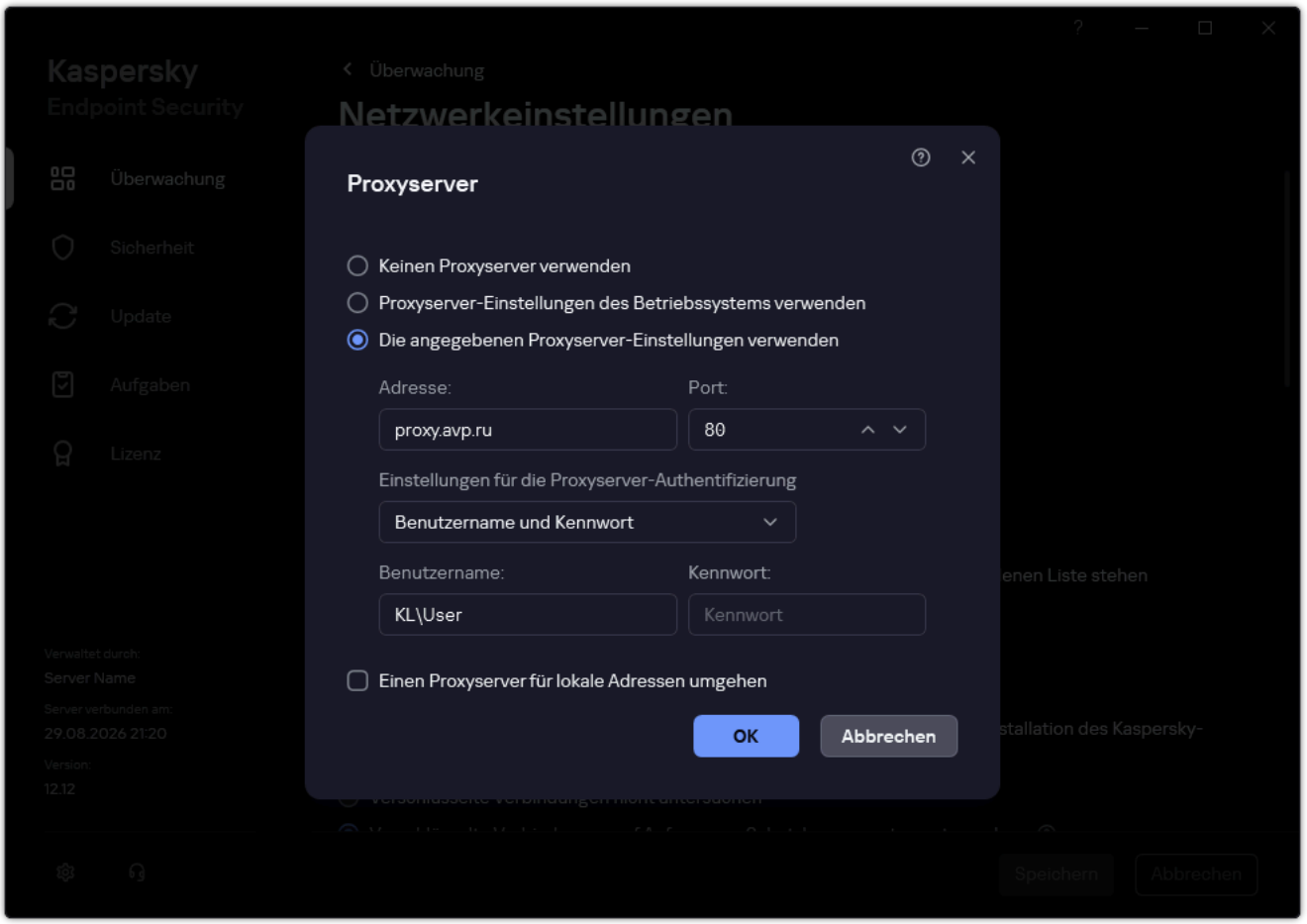
So konfigurieren Sie die Proxyserver-Einstellungen in der Programmoberfläche:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Netzwerkeinstellungen** aus.



Netzwerkeinstellungen für die App

3. Klicken Sie im Block **Proxyserver** auf den Link **Proxyserver-Einstellungen**.



Verbindungseinstellungen des Proxyservers

4. Wählen Sie im folgenden Fenster eine der folgenden Optionen aus, nach welcher die Proxyserveradresse ermittelt werden soll:

   - **Proxyserver-Einstellungen des Betriebssystems verwenden**.

     Dieser Status gilt als Standard. Kaspersky Endpoint Security verwendet die Proxyserver-Einstellungen, die in den Betriebssystemeinstellungen definiert sind.

   - **Die angegebenen Proxyserver-Einstellungen verwenden**.

     Wenn Sie diese Option ausgewählt haben, konfigurieren Sie die Einstellungen für die Verbindung mit dem Proxyserver: Proxyserver-Adresse und Port.

5. Wählen Sie aus, wie sich das Programm am Proxyserver authentifizieren soll. Standardmäßig verwendet das Programm die NTLM-Domänen-Authentifizierung des aktuellen Benutzers.

6. Damit kein Proxyserver verwendet wird, wenn die Datenbanken und Programm-Module aus einem gemeinsamen Ordner aktualisiert werden, aktivieren Sie das Kontrollkästchen **Einen Proxyserver für lokale Adressen umgehen**.

7. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen wird Kaspersky Endpoint Security den Proxyserver zum Herunterladen von Programmmodul- und Datenbanken-Updates verwenden. Kaspersky Endpoint Security wird den Proxyserver auch für den Zugriff auf KSN-Server und Kaspersky-Aktivierungsserver verwenden. Wenn eine Authentifizierung auf dem Proxyserver erforderlich ist, aber die Anmeldedaten für das Benutzerkonto nicht angegeben wurden oder falsch sind, fordert Kaspersky Endpoint Security Sie auf, den Benutzernamen und das Kennwort einzugeben.

Rollback des letzten Updates

Nach dem zweiten Update der Datenbanken und Programm-Module steht eine Rollback-Funktion zur Verfügung, mit der Sie zu den vorherigen Datenbanken und Programm-Modulen zurückkehren können.

Jedes Mal, wenn der Benutzer das Update startet, erstellt Kaspersky Endpoint Security zuerst eine Backup-Kopie der bisher verwendeten Datenbanken und Programm-Module und beginnt dann mit der Aktualisierung. Somit kann bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückgekehrt werden. Die Rollback-Funktion für das letzte Update ist beispielsweise nützlich, wenn die neue Datenbankversion einen Fehlalarm auslöst, durch den Kaspersky Endpoint Security eine harmlose Anwendung blockiert.

Im Light Agent-Modus wird die Aufgabe *Update-Rollback* von Kaspersky Endpoint Security nicht unterstützt.

So setzen Sie das letzte Update zurück (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

1. Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Update-Rollback** aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Zeitplan des Aufgabenstarts anpassen

Konfigurieren Sie den Aufgabenzeitplan, z. B. mit der Option „manuell“.

Schritt 4. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgabe ein.

Schritt 7. Erstellung der Aufgabe abschließen

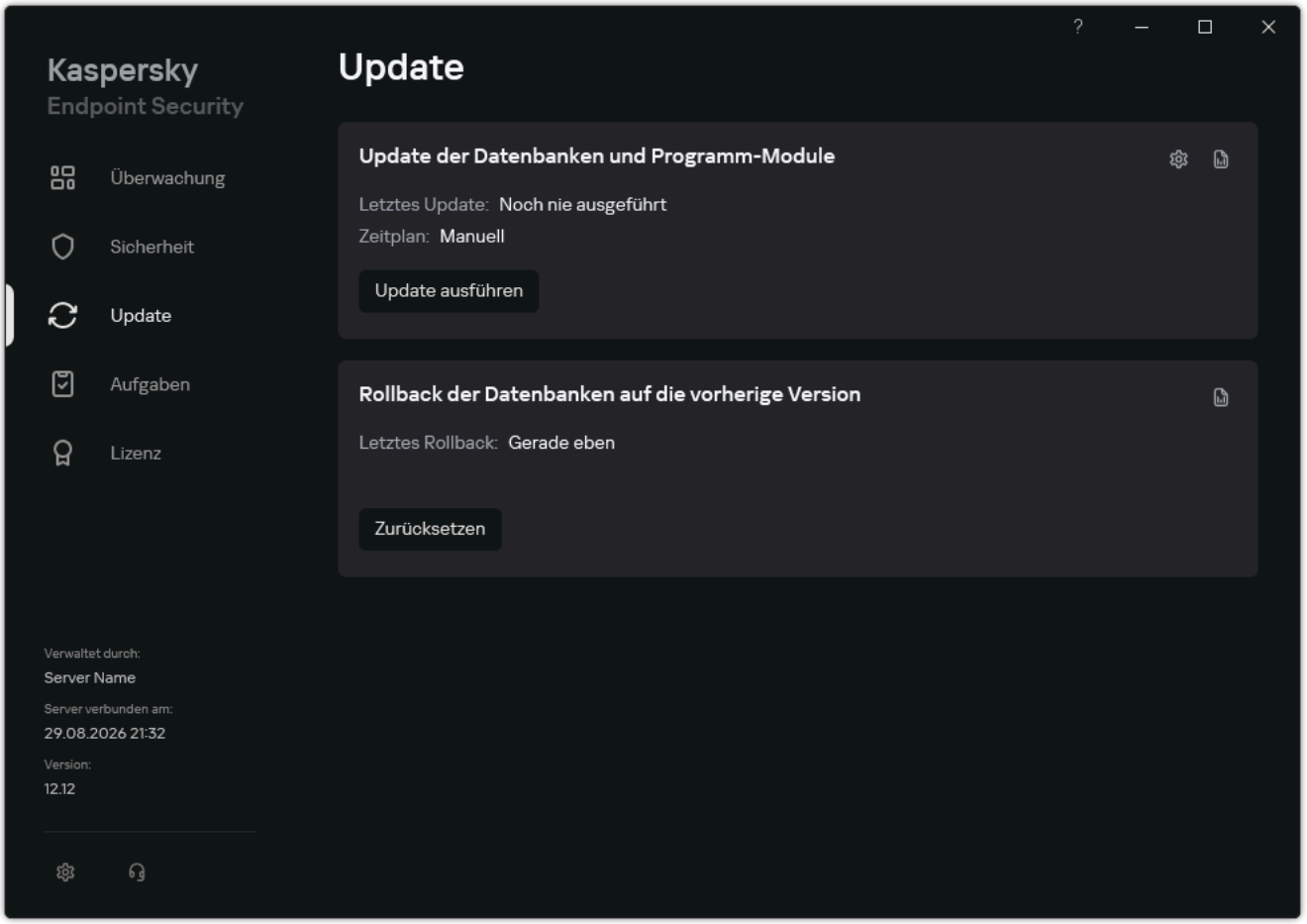
Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So setzen Sie das letzte Update zurück (in der Web Console)

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Hinzufügen**.
   Der Assistent für neue Aufgaben wird gestartet.
3. Passen Sie die Einstellungen der Aufgabe an:
   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.
   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Rollback**.
   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein (beispielsweise *Update-Rollback*).
   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.
4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt
5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.
6. Schließen Sie den Assistenten ab.
7. Die neue Aufgabe wird in der Aufgabenliste angezeigt.
8. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.
9. Klicken Sie auf **Starten**.

So setzen Sie das letzte Update zurück (in der Programmoberfläche)

1. Gehen Sie im Programmhauptfenster zum Abschnitt **Update**.



Lokale Update-Aufgaben

2. Klicken Sie in der Kachel **Rollback der Datenbanken auf die vorherige Version** auf **Zurücksetzen**.

Kaspersky Endpoint Security beginnt mit dem Zurücksetzen des letzten Datenbanken-Updates. Das Programm zeigt den Rollback-Fortschritt, die Größe der heruntergeladenen Dateien und die Update-Quelle an. Sie können die Aufgabe jederzeit beenden, indem Sie auf die Schaltfläche **Update abbrechen** klicken.

Technologie zur Aktiven Desinfektion

Zur Verarbeitung aktiver Bedrohungen verwendet Kaspersky Endpoint Security die Technologie „Aktive Desinfektion“. Die „Aktive Desinfektion“ funktioniert auf Workstations und Servern in unterschiedlicher Weise. Die aktive Desinfektion können Sie in den Einstellungen der Aufgabe *Schadsoftware-Untersuchung* und in den Programmeinstellungen anpassen.

Wenn Kaspersky Endpoint Security die Ausführung eines bestimmten Schadsoftware-Abschnitts nicht verhindern kann, können Sie die Technologie zur aktiven Desinfektion verwenden. Für Computer, die einer Richtlinie unterliegen, ist die Aktive Desinfektion standardmäßig deaktiviert, da diese Technologie die Computerressourcen stark beansprucht. Für Computer, die nicht unter eine Richtlinie fallen, ist die Aktive Desinfektion standardmäßig aktiviert.

Die „Aktive Desinfektion“ funktioniert auf Workstations und Servern in unterschiedlicher Weise. Um die Technologie auf Servern zu verwenden, müssen Sie die sofortige aktive Desinfektion in den Eigenschaften der Aufgabe *Schadsoftware-Untersuchung* aktivieren. Diese Voraussetzung ist nicht erforderlich, um die Technologie auf Workstations zu verwenden.

So aktivieren oder deaktivieren Sie die Technologie „Aktive Desinfektion“ in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
4. Aktivieren oder deaktivieren Sie im Block **Allgemein** das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**, um die Technologie zur aktiven Desinfektion zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Technologie „Aktive Desinfektion“ in der „Web Console“ und in der „Cloud Console“

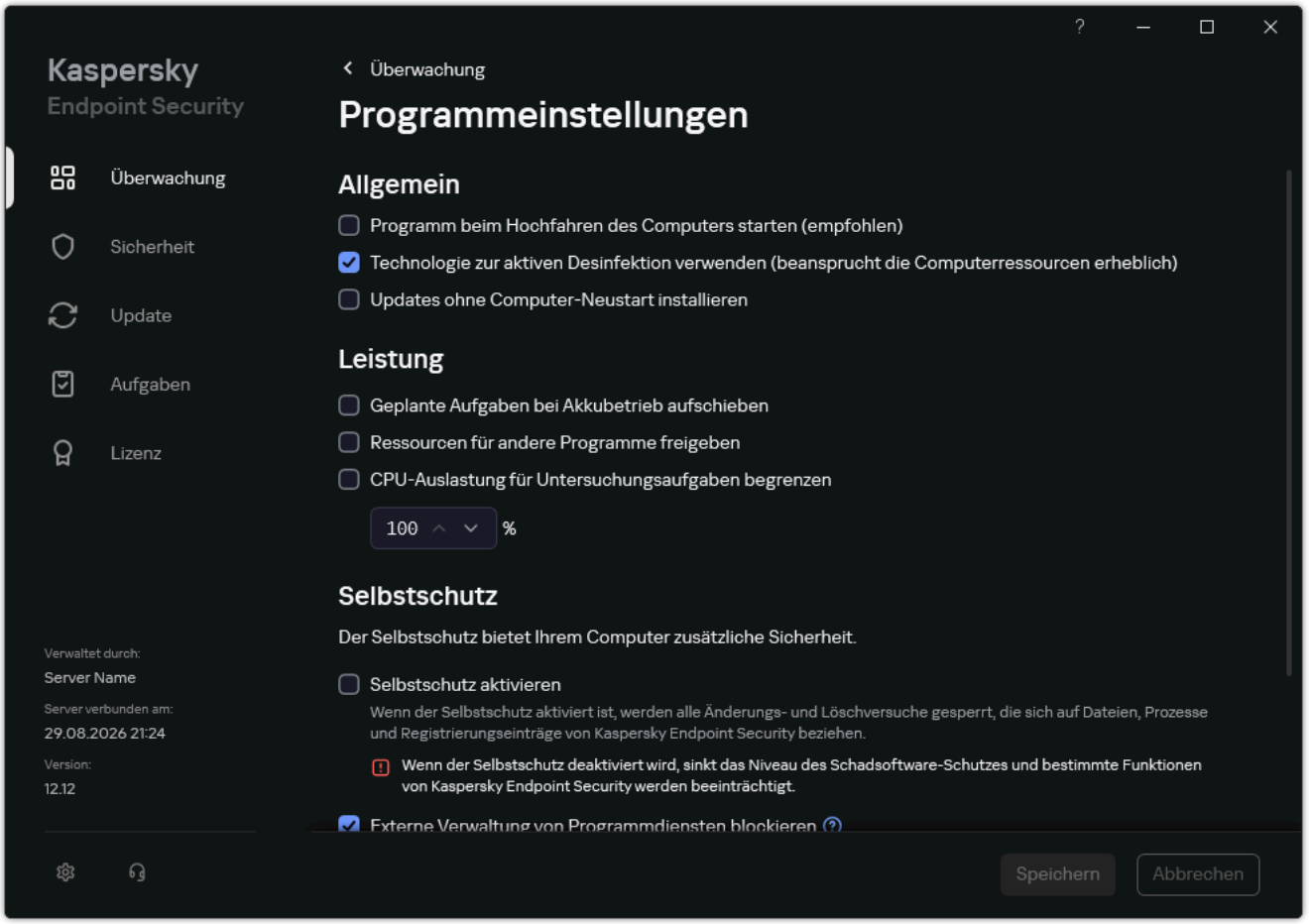
1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie die Option **Allgemeine Einstellungen → Erkennungseinstellungen** aus.
5. Aktivieren oder deaktivieren Sie im Block **Technologie zur Aktiven Desinfektion** den Schalter **Technologie zur Aktiven Desinfektion AKTIVIERT**, um die Technologie zur aktiven Desinfektion zu aktivieren bzw. zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Technologie „Aktive Desinfektion“ in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Aktivieren oder deaktivieren Sie im Block **Allgemein** das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden (beansprucht die Computerressourcen erheblich)**, um die Technologie zur aktiven Desinfektion zu aktivieren oder zu deaktivieren.

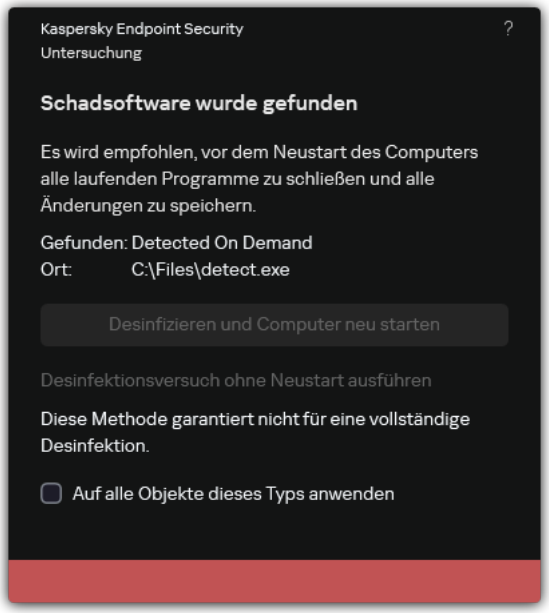
4. Speichern Sie die vorgenommenen Änderungen.

Während die „Aktive Desinfektion“ ausgeführt wird, kann der Benutzer die meisten Betriebssystemfunktionen nicht verwenden. Nach Abschluss der Desinfektion wird der Computer neu gestartet.

Desinfektion aktiver Bedrohungen auf Workstations

Um aktive Bedrohungen auf Workstations verarbeiten zu können, aktivieren Sie die Technologie zur aktiven Desinfektion in den Programmeinstellungen. Konfigurieren Sie als Nächstes die Benutzererfahrung in den Eigenschaften der Aufgabe *Schadsoftware-Untersuchung*. In den Aufgabeneigenschaften finden Sie ein Kontrollkästchen mit dem Titel **Aktive Desinfektion sofort ausführen**. Ist das Kontrollkästchen aktiviert, so führt Kaspersky Endpoint Security eine Desinfektion aus, ohne den Benutzer zu benachrichtigen. Nach Abschluss der Desinfektion wird der Computer neu gestartet. Ist das Kontrollkästchen deaktiviert, zeigt Kaspersky Endpoint Security eine Benachrichtigung über eine aktive Bedrohung an (s. Abb. unten). Sie können diese Benachrichtigung nicht schließen, ohne die Datei zu verarbeiten.

Wenn auf dem Computer eine Untersuchungsaufgabe ausgeführt wird, erfolgt nur dann eine aktive Desinfektion, wenn in den Eigenschaften der Richtlinie, die für diesen Computer gilt, die Aktive Desinfektion aktiviert ist.



Benachrichtigung über eine aktive Bedrohung

Desinfektion aktiver Bedrohungen auf Servern

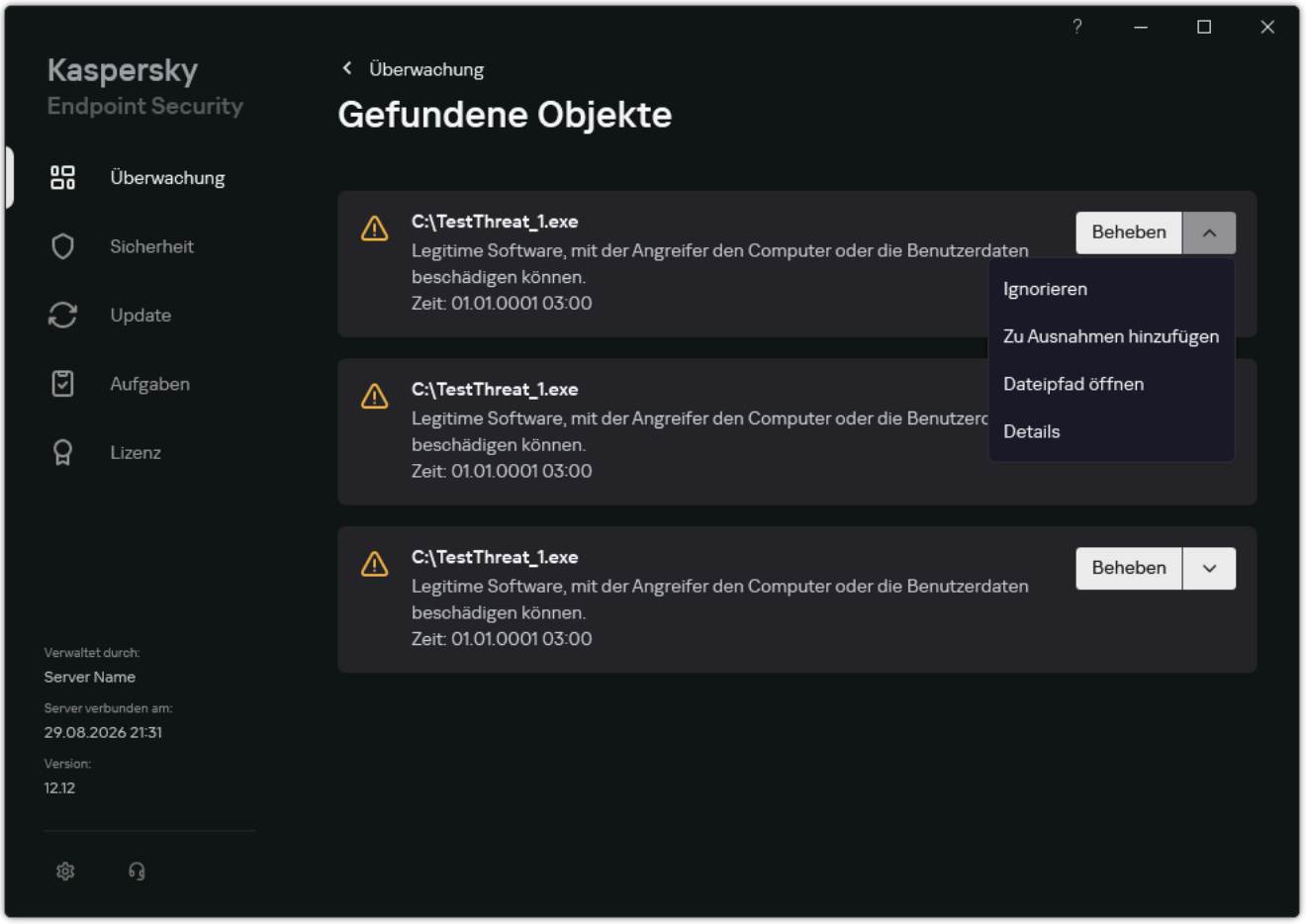
Gehen Sie wie folgt vor, um aktive Bedrohungen auf Servern zu verarbeiten:

- Aktivieren Sie die Technologie zur aktiven Desinfektion in den Programmeinstellungen.
- Aktivieren Sie die sofortige „Aktive Desinfektion“ in den Eigenschaften der Aufgabe *Schadsoftware-Untersuchung*.

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*. Dann müssen Sie eine Aufgabe *Schadsoftware-Untersuchung* starten.

Unverarbeitete Bedrohungen eliminieren

Kaspersky Endpoint Security protokolliert Informationen über Dateien, die aus bestimmten Gründen nicht verarbeitet wurden. Diese Informationen werden als Ereignisse in die Liste der aktiven Bedrohungen eingetragen (s. Abb. unten).



Eine Liste der aktiven Bedrohungen

Eine infizierte Datei wird als *verarbeitet* betrachtet, wenn Kaspersky Endpoint Security die Datei desinfiziert oder die Bedrohung entfernt hat, während der Computer auf Viren und andere Schadsoftware untersucht wurde.

Kaspersky Endpoint Security setzt die Datei auf die Liste der aktiven Bedrohungen, falls Kaspersky Endpoint Security bei der Untersuchung des Computers auf Viren und andere bedrohliche Programme mit dieser Datei eine Aktion ausgeführt hat, welche nicht in den Programmeinstellungen vorgesehen ist.

Dies ist in folgenden Fällen möglich:

- Die zu untersuchende Datei ist nicht verfügbar (Sie befindet sich beispielsweise auf einem Netzlaufwerk oder einem externen Laufwerk ohne Schreibrechte).
- In den Einstellungen der Aufgabe *Schadsoftware-Untersuchung* ist **Informieren** als Aktion beim Fund einer Bedrohung ausgewählt. Als dann die Benachrichtigung über infizierte Dateien auf dem Bildschirm angezeigt wurde, hat der Benutzer **Ignorieren** ausgewählt.

Falls unverarbeitete Bedrohungen vorhanden sind, ändert Kaspersky Endpoint Security das Symbol in . Im Programmhauptfenster wird die Bedrohungsmeldung angezeigt (siehe Abbildung unten). In der Kaspersky Security Center-Konsole ändert sich der Status des Computers in *Kritisch* – .

So verarbeiten Sie eine Bedrohung in der Verwaltungskonsole (MMC)

1. Gehen Sie in der Verwaltungskonsole zum Ordner **Administrationsserver** → **Erweitert** → **Datenverwaltung** → **Aktive Bedrohungen**.

   Die Liste der aktive Bedrohungen wird geöffnet.

2. Wählen Sie das Objekt aus, das Sie verarbeiten möchten.

3. Legen Sie fest, wie die Bedrohung behandelt werden soll:

   - **Desinfizieren**. 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.

   - **Löschen**. Wenn diese Option ausgewählt ist, löscht das Programm infizierte Dateien, die in der Datenverwaltung für aktive Bedrohungen gefunden wurden. In diesem Fall belässt das Programm die gefundene Datei im Arbeitsspeicher des Computers. Um die Bedrohung vom Computer zu entfernen, wählen Sie **Desinfizieren** aus.

So verarbeiten Sie eine Bedrohung in der „Web Console“ oder „Cloud Console“

1. Klicken Sie im Web Console-Hauptfenster auf **Vorgänge** → **Datenverwaltung** → **Aktive Bedrohungen**.

   Die Liste der aktive Bedrohungen wird geöffnet.

2. Wählen Sie das Objekt aus, das Sie verarbeiten möchten.

3. Legen Sie fest, wie die Bedrohung behandelt werden soll:

   - **Desinfizieren**. 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.

   - **Löschen**. Wenn diese Option ausgewählt ist, löscht das Programm infizierte Dateien, die in der Datenverwaltung für aktive Bedrohungen gefunden wurden. In diesem Fall belässt das Programm die gefundene Datei im Arbeitsspeicher des Computers. Um die Bedrohung vom Computer zu entfernen, wählen Sie **Desinfizieren** aus.

So verarbeiten Sie eine Bedrohung über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Die Sicherheit ist bedroht!**.

   Die Liste der aktive Bedrohungen wird geöffnet.

2. Wählen Sie das Objekt aus, das Sie verarbeiten möchten.

3. Legen Sie fest, wie die Bedrohung behandelt werden soll:

   - **Beheben**. 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.

   - **Zu Ausnahmen hinzufügen**. Wenn diese Aktion ausgewählt ist, schlägt Kaspersky Endpoint Security vor, die Datei zur Liste der Untersuchungsausnahmen hinzuzufügen. Die Einstellungen der Ausnahme werden automatisch konfiguriert. Wenn keine Ausnahmen hinzugefügt werden können, hat der Administrator diese Option in den Richtlinieneinstellungen deaktiviert.

- **Ignorieren**. Wenn diese Option ausgewählt wird, löscht Kaspersky Endpoint Security den Eintrag aus der Liste der aktive Bedrohungen. Wenn die Liste keine aktiven Bedrohungen mehr enthält, ändert sich der Computerstatus in *OK*. Wenn das Objekt erneut gefunden wird, fügt Kaspersky Endpoint Security einen neuen Eintrag zur Liste der aktiven Bedrohungen hinzu.

- **Dateipfad öffnen**. Wenn diese Option ausgewählt wird, öffnet Kaspersky Endpoint Security im Dateimanager den Ordner, der das Objekt enthält. Dann können Sie das Objekt entweder manuell löschen oder das Objekt in einen Ordner außerhalb des Schutzbereichs verschieben.

- **Details**. Wenn diese Option ausgewählt ist, öffnet Kaspersky Endpoint Security die Webseite Kaspersky-Datenbank für Schwachstellen und Bedrohungen.

Damit aktive Bedrohungen in der Kaspersky Security Center-Konsole verarbeitet werden können, müssen Sie die Übertragung von Informationen über unverarbeitete Dateien an den Administrationsserver aktivieren. Die Datenübertragung ist standardmäßig aktiviert.

So aktivieren Sie die Übertragung von Daten über unverarbeitete Dateien (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Berichte und Speicher** aus.
4. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Unverarbeitete Dateien**.
6. Speichern Sie die vorgenommenen Änderungen.

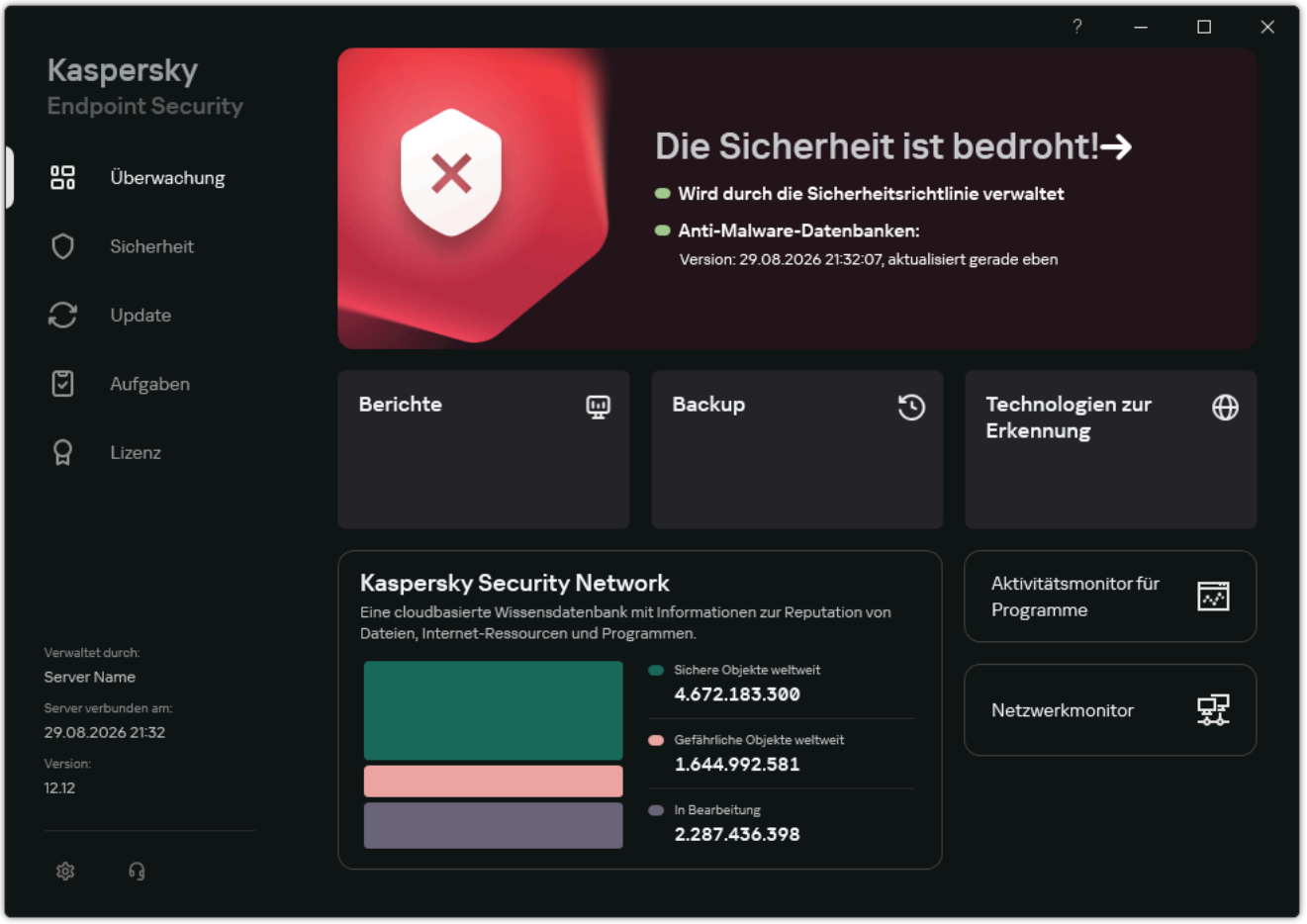
So aktivieren Sie die Übertragung von Daten über unverarbeitete Dateien (in der Web Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → KSC-Integration**.

5. Aktivieren Sie im Block **Datenübertragung an den Administrationsserver** das Kontrollkästchen **Über nicht verarbeitete Dateien**.

6. Speichern Sie die vorgenommenen Änderungen.



Programmhauptfenster, wenn eine Bedrohung erkannt wurde

Computerschutz

Echtzeit-Schutzstatus

Kaspersky Endpoint Security sendet die Einstellung **Status des Echtzeitschutzes** an den Kaspersky Security Center Administrationsserver. Der Wert dieser Einstellung hängt vom aktuellen Status der Schutzkomponenten des Programms auf dem geschützten Computer ab (siehe Tabelle unten).

Kaspersky Endpoint Security ermittelt den Echtzeit-Schutzstatus anhand des Status der folgenden Programmkomponenten:

- Schutz vor bedrohlichen Dateien.
- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.
- AMSI-Schutz.
- Schutz vor BadUSB-Angriffen.
- Schutz vor Netzwerkbedrohungen.
- Firewall.
- Exploit-Prävention.
- Verhaltensanalyse.
- Rollback von schädlichen Aktionen.
- Programm-Überwachung.

Sie können den Echtzeit-Schutzstatus des Programms in einer Konsole von Kaspersky Security Center überprüfen.

So ermitteln Sie den Echtzeit-Schutzstatus über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte** aus.

Der aktuelle Echtzeit-Schutzstatus wird in der Geräteliste in der Spalte **Status des Echtzeitschutzes** angezeigt. Wenn die Spalte **Status des Echtzeitschutzes** fehlt, verwalten Sie die Spalteneinstellungen, indem Sie auf den Link **Spalten hinzufügen oder löschen** klicken.

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte** aus.

Der aktuelle Echtzeit-Schutzstatus wird in der Geräteliste in der Spalte **Status des Echtzeitschutzes** angezeigt. Wenn die Spalte **Status des Echtzeitschutzes** fehlt, verwalten Sie die Spalteneinstellungen, indem Sie auf den Link **Spalten hinzufügen oder löschen** klicken.

So ermitteln Sie den Echtzeit-Computerschutz in der Web Console

Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Assets (Geräte)** aus.

Der aktuelle Echtzeit-Schutzstatus wird in der Geräteliste in der Spalte **Status des Echtzeitschutzes** angezeigt. Wenn die Spalte **Status des Echtzeitschutzes** fehlt, verwalten Sie die Spalteneinstellungen (⚙).

Mögliche Werte der Einstellung Status des Echtzeitschutzes

Wert	Beschreibung
Unbekannt	Der Administrationsserver verfügt über keine Informationen zum Echtzeit-Schutzstatus dieses Computers.
Nicht installiert	Es sind keine Komponenten installiert.
Von der Lizenz nicht unterstützt	Das Programm ist nicht aktiviert oder die Lizenz lässt den Betrieb der installierten Komponenten nicht zu.
Fehlgeschlagen	Bei einer oder mehreren Komponenten ist eine Fehlfunktion aufgetreten.
Beendet	Eine oder mehrere Komponenten sind deaktiviert.
Angehalten	Eine oder mehrere Komponenten sind angehalten.
Wird gestartet	Eine oder mehrere Komponenten werden aktiviert.
Wird ausgeführt	Die Programmkomponenten sind aktiviert und werden ausgeführt.

Wenn der Wert der Einstellung **Status des Echtzeitschutzes** in Kaspersky Security Center von *Wird ausgeführt* abweicht, überprüfen Sie, ob die installierten Komponenten von Kaspersky Endpoint Security aus der Liste aktiviert sind und das Programm aktiviert ist.

Schutz vor bedrohlichen Dateien

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.

Schutz vor bedrohlichen Dateien aktivieren und deaktivieren

Die Komponente „Schutz vor bedrohlichen Dateien“ ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Zum Schutz vor bedrohlichen Dateien kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** gilt als optimal und wird von den Kaspersky-Spezialisten empfohlen (siehe Tabelle unten). Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Die Komponente „Schutz vor bedrohlichen Dateien“ verwendet Daten, die von anderen Programmkomponenten empfangen wurden. Das Aktivieren dieser Komponenten ist optional. Diese Komponenten stellen zusätzliche Daten bereit:

- Kaspersky Security Network.
- Programm-Überwachung.
- Verhaltensanalyse.

So aktivieren und deaktivieren Sie die Komponente „Schutz vor bedrohlichen Dateien“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor bedrohlichen Dateien** aus.
4. Verwenden Sie das Kontrollkästchen **Schutz vor bedrohlichen Dateien**, um die Komponente zu aktivieren oder zu deaktivieren.

5. Wenn Sie die Komponente aktiviert haben, führen Sie im Block **Sicherheitsstufe** einen der folgenden Schritte aus:

   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:

     - **Hoch**. Auf dieser Sicherheitsstufe für Dateien kontrolliert die Komponente „Schutz vor bedrohlichen Dateien“ alle Dateien, die geöffnet, gespeichert und gestartet werden, mit höchster Genauigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht alle Dateitypen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Untersucht werden außerdem Archive, Installationspakete und eingebettete OLE-Objekte.

     - **Empfohlen**. Diese Sicherheitsstufe für Dateien wird von Kaspersky-Experten empfohlen. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht Archive oder Installationspakete nicht.

     - **Niedrig**. Diese Sicherheitsstufe für Dateien bietet eine maximale Untersuchungsgeschwindigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Zusammengesetzte Dateien werden von der Komponente „Schutz vor bedrohlichen Dateien“ nicht untersucht.

   - Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Einstellungen** und legen Sie Ihre eigenen Komponenteneinstellungen fest (siehe Tabelle unten).

     Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen. Klicken Sie dazu auf die Schaltfläche **Standard**.

6. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security mit schädlichen Objekten ausführen soll:

   - **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**. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert.

   - **Blockieren**. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch.

   - **Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.

   Bevor versucht wird, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Komponente „Schutz vor bedrohlichen Dateien“ über die Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Schutz vor bedrohlichen Dateien**.
5. Verwenden Sie den Schalter **Schutz vor bedrohlichen Dateien AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Um ein neues Objekt zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Wählen Sie unter **Erweiterte Einstellungen** die Registerkarte **Schutzbereich** aus.

   b. Klicken Sie auf **Hinzufügen**.

   c. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Objekte aus, die Sie dem Untersuchungsbereich hinzufügen möchten.

   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` funktioniert nicht.

   - 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.

   Sie können Masken überall in einem Datei- oder Ordnerpfad verwenden. Wenn Sie beispielsweise möchten, dass der Untersuchungsbereich den Ordner „Downloads“ für alle Benutzerkonten auf dem Computer umfasst, geben Sie folgende Maske ein: `C:\Users\*\Downloads\`.

   Sie können ein Objekt vom Schutz ausschließen, ohne es aus der Liste der Objekte im Schutzbereich zu entfernen. Setzen Sie dazu den Umschalter neben dem Objekt auf „Aus“.

   d. Speichern Sie die vorgenommenen Änderungen.

7. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security mit schädlichen Objekten ausführen soll:

   - **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**. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert.

   - **Blockieren**. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch.

   Bevor versucht wird, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.

8. Bearbeiten Sie bei Bedarf die erweiterten Einstellungen des Schutzes vor bedrohlichen Dateien.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Komponente „Schutz vor bedrohlichen Dateien“ über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Verwenden Sie den Schalter **Schutz vor bedrohlichen Dateien**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Wenn Sie die Komponente aktiviert haben, führen Sie im Block **Sicherheitsstufe** einen der folgenden Schritte aus:

   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:

     - **Hoch**. Auf dieser Sicherheitsstufe für Dateien kontrolliert die Komponente „Schutz vor bedrohlichen Dateien“ alle Dateien, die geöffnet, gespeichert und gestartet werden, mit höchster Genauigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht alle Dateitypen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Untersucht werden außerdem Archive, Installationspakete und eingebettete OLE-Objekte.

     - **Empfohlen**. Diese Sicherheitsstufe für Dateien wird von Kaspersky-Experten empfohlen. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht Archive oder Installationspakete nicht.

     - **Niedrig**. Diese Sicherheitsstufe für Dateien bietet eine maximale Untersuchungsgeschwindigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Zusammengesetzte Dateien werden von der Komponente „Schutz vor bedrohlichen Dateien“ nicht untersucht.

- Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Komponenteneinstellungen fest (siehe Tabelle unten).

  Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen. Klicken Sie dazu auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen**.

5. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security mit schädlichen Objekten ausführen soll:

   - **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**. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert.

   - **Blockieren**. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch.

   - **Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.

   Bevor versucht wird, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.

6. Speichern Sie die vorgenommenen Änderungen.

Von Kaspersky-Experten empfohlene Einstellungen zum Schutz vor bedrohlichen Dateien (empfohlene Sicherheitsstufe)

Einstellung	Wert	Beschreibung
Dateitypen	**Dateien nach Format untersuchen**	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.
Heuristische Analyse	**Oberflächlich**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Nur neue und veränderte Dateien untersuchen	**Ein**	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.
iSwift-Technologie verwenden	**Ein**	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

Einstellung	Wert	Beschreibung
iChecker-Technologie verwenden	**Ein**	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
Dateien in Microsoft Office-Formaten untersuchen	**Ein**	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Dateien in E-Mail-Formaten untersuchen	**Ein**	Untersucht Dateien im E-Mail-Format. Die App untersucht MSG- und EML-Dateien. E-Mail-Format-Dateien enthalten auch OLE-Objekte und MHT-Dateien. Dateien im E-Mail-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch Kaspersky Endpoint Security untersucht.
Untersuchungsmodus	**Intelligenter Modus**	In diesem Untersuchungsmodus untersucht die „Schutz vor bedrohlichen Dateien"-Funktion ein Objekt auf Basis einer Analyse von Vorgängen, die mit ihm ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.
Aktion beim Fund einer Bedrohung	**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.

Schutz vor bedrohlichen Dateien automatisch anhalten

Sie können festlegen, dass der Schutz vor bedrohlichen Dateien zu einem bestimmten Zeitpunkt oder bei der Arbeit mit bestimmten Programmen automatisch angehalten wird.

Es gilt als Notlösung, den Schutz vor bedrohlichen Dateien bei einem Konflikt mit bestimmten Programmen anzuhalten. Sollten während des Betriebs einer Komponente Konflikte auftreten, empfehlen wir Ihnen, sich an den technischen Support von Kaspersky zu wenden. Die Experten helfen Ihnen dabei, eine Lösung für die gleichzeitige Verwendung der Komponente „Schutz vor bedrohlichen Dateien" mit anderen Programmen auf Ihrem Computer zu finden.

Um das automatische Anhalten des Schutzes vor bedrohlichen Dateien anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Klicken Sie im Block **Schutz vor bedrohlichen Dateien anhalten** auf den Link **Schutz vor bedrohlichen Dateien anhalten**.

5. Konfigurieren Sie im angezeigten Fenster die Einstellungen für das Anhalten des „Schutzes vor bedrohlichen Dateien“:

   a. Konfigurieren Sie einen Zeitplan für das automatische Anhalten des Schutzes vor bedrohlichen Dateien.

   b. Erstellen Sie eine Liste von Programmen, deren Ausführung bewirken soll, dass der Schutz vor bedrohlichen Dateien seine Aktivitäten unterbricht.

6. Speichern Sie die vorgenommenen Änderungen.

Ändern der Aktion, welche die Komponente „Schutz vor bedrohlichen Dateien“ mit infizierten Dateien ausführen soll

Die Komponente „Schutz vor bedrohlichen Dateien“ versucht standardmäßig, alle gefundenen infizierten Dateien automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden diese Dateien von der Komponente „Schutz vor bedrohlichen Dateien“ gelöscht.

Zum Ändern der Aktion, welche die Komponente „Schutz vor bedrohlichen Dateien“ mit infizierten Dateien ausführen soll, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.

3. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option:

   - **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**. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert.

   - **Blockieren**. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch.

   Bevor versucht wird, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.

4. Speichern Sie die vorgenommenen Änderungen.

Schutzbereich für die Komponente „Schutz vor bedrohlichen Dateien”

Der Begriff Schutzbereich bezieht sich auf die Objekte, die von einer Komponente während ihrer Ausführung untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften. Der Schutzbereich für die Komponente „Schutz vor bedrohlichen Dateien“ wird durch die Eigenschaften Speicherort und Typ der zu untersuchenden Dateien definiert. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht standardmäßig nur infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers aus gestartet werden.

Bei der Auswahl des Typs für die zu untersuchenden Dateien sollte Folgendes beachtet werden:

1. Für bestimmte Dateiformate (z. B. TXT-Format) besteht eine geringe Wahrscheinlichkeit, dass schädlicher Code eindringt und dann aktiviert wird. Es gibt aber auch Dateiformate, die ausführbaren Code enthalten (z. B. die Formate EXE und DLL). Ausführbarer Code kann auch in Dateiformaten enthalten sein, die dafür nicht vorgesehen sind (z. B. das Format DOC). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist hoch.

2. Ein Angreifer kann einen Virus oder ein anderes bedrohliches Programm in einer ausführbaren Datei, deren Erweiterung in TXT geändert wurde, an Ihren Computer senden. Wenn Sie die Dateiuntersuchung nach Erweiterung festgelegt haben, überspringt das Programm eine solche Datei bei der Untersuchung. Wenn die Überprüfung von Dateien nach Format ausgewählt wird, analysiert Kaspersky Endpoint Security den Datei-Header unabhängig von seiner Erweiterung. Falls sich ergibt, dass die Datei das Format einer ausführbaren Datei (beispielsweise EXE) besitzt, so wird die Datei untersucht.

Gehen Sie folgendermaßen vor, um einen Schutzbereich zu erstellen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Geben Sie im Block **Dateitypen** den Typ der Dateien an, die von der Komponente „Schutz vor bedrohlichen Dateien“ untersucht werden sollen:

   - **Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung).

   - **Dateien nach Format untersuchen**. 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.

   - **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.

5. Klicken Sie auf den Link **Schutzbereich ändern**.

6. Wählen Sie im folgenden Fenster die Objekte aus, die Sie dem Schutzbereich hinzufügen oder von diesem ausschließen möchten.

   Objekte, die standardmäßig zum Schutzbereich gehören, können weder gelöscht noch geändert werden.

7. Um ein neues Objekt zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen**.

      Der Ordnerbaum wird geöffnet.

   b. Geben Sie im Feld **Pfad** den Ordner- oder Dateipfad ein.

      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` funktioniert nicht.

      - 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.

      Sie können Masken überall in einem Datei- oder Ordnerpfad verwenden. Wenn Sie beispielsweise möchten, dass der Untersuchungsbereich den Ordner „Downloads“ für alle Benutzerkonten auf dem Computer umfasst, geben Sie folgende Maske ein: `C:\Users\*\Downloads\`.

      Das Objekt **Dieser PC** in der Liste der Dateiressourcen des Computers enthält die folgenden Objekte: **Alle Festplatten**, **Alle Netzlaufwerke** und **Alle Wechseldatenträger**.

   Sie können ein Objekt von Untersuchungen ausschließen, ohne es aus der Liste der Objekte im Untersuchungsbereich zu löschen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

8. Speichern Sie die vorgenommenen Änderungen.

Untersuchungsmethoden verwenden

Kaspersky Endpoint Security verwendet die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse. Bei der Signaturanalyse vergleicht Kaspersky Endpoint Security ein gefundenes Objekt mit den Einträgen in den Programm-Datenbanken. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.

Sie können die heuristische Analyse verwenden, um den Schutz noch wirksamer zu gestalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.

Um die Verwendung der heuristischen Analyse für die Komponente „Schutz vor bedrohlichen Dateien“ anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Wenn das Programm die heuristische Analyse zum Schutz vor Dateibedrohungen verwenden soll, aktivieren Sie das Kontrollkästchen **Heuristische Analyse** im Block **Untersuchungsmethoden**. Legen Sie dann mit dem Schieberegler die Ebene der heuristischen Analyse fest: **Oberflächlich**, **Mittel** oder **Tief**.
5. Speichern Sie die vorgenommenen Änderungen.

Verwendung von Untersuchungstechnologien durch die Komponente „Schutz vor bedrohlichen Dateien”

Um die Verwendung der Untersuchungstechnologien für die Komponente „Schutz vor bedrohlichen Dateien“ anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Aktivieren Sie im Abschnitt **Untersuchungstechnologien** die Kontrollkästchen für die Technologien, die bei der Untersuchung verwendet werden sollen.

   - **iSwift-Technologie verwenden**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

   - **iChecker-Technologie verwenden**. Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

5. Speichern Sie die vorgenommenen Änderungen.

Dateiuntersuchung optimieren

Um die Dateiuntersuchung mit der Komponente „Schutz vor bedrohlichen Dateien“ zu optimieren, können Sie die Untersuchungsdauer verkürzen und die Leistung von Kaspersky Endpoint Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Sie können außerdem die Technologien iChecker und iSwift aktivieren, mit denen sich die Dateiuntersuchung beschleunigen lässt. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit der letzten Untersuchung nicht verändert wurden.

Gehen Sie folgendermaßen vor, um die Untersuchung von Dateien zu optimieren:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Aktivieren Sie im Block **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

5. Speichern Sie die vorgenommenen Änderungen.

Untersuchung von zusammengesetzten Dateien

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. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

Die Verarbeitungsmethode für eine zusammengesetzte infizierte Datei (Löschen oder Desinfektion) ist vom Dateityp abhängig.

Die Komponente „Schutz vor bedrohlichen Dateien“ desinfiziert zusammengesetzte Dateien der Formate ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR und ICE, und löscht Dateien aller übrigen Formate (unter Ausnahme von E-Mail-Datenbanken).

Gehen Sie folgendermaßen vor, um die Untersuchung von zusammengesetzten Dateien anzupassen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Geben Sie im Block **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Dateien im Mail- bzw. Office-Format.
5. Wenn die Untersuchung nur neuer und geänderter Dateien deaktiviert ist, konfigurieren Sie die Einstellungen für die Untersuchung jedes Typs von zusammengesetzten Dateien: „Alle Dateien dieses Typs untersuchen“ oder „Nur neue Dateien untersuchen“.

   Wenn die Untersuchung nur neuer und geänderter Dateien aktiviert ist, überprüft Kaspersky Endpoint Security nur neue und geänderte Dateien aller Arten von zusammengesetzten Dateien.
6. Konfigurieren Sie die erweiterten Einstellungen für die Untersuchung von zusammengesetzten Dateien.

   - **Große zusammengesetzte Dateien nicht entpacken**.

     Ist das Kontrollkästchen aktiviert, so werden zusammengesetzte Dateien, welche die festgelegte Größe überschreiten, nicht von Kaspersky Endpoint Security untersucht.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Endpoint Security zusammengesetzte Dateien unabhängig von ihrer Größe.

     Unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist, werden umfangreiche Dateien beim Extrahieren aus Archiven von Kaspersky Endpoint Security untersucht.

   - **Zusammengesetzte Dateien im Hintergrund entpacken**.

Wenn das Kontrollkästchen aktiviert ist, gewährt Kaspersky Endpoint Security den Zugriff auf zusammengesetzte Dateien, die größer sind als der festgelegte Wert. Der Zugriff wird gewährt, bevor diese Dateien untersucht werden. Dabei entpackt und untersucht Kaspersky Endpoint Security die zusammengesetzten Dateien im Hintergrundmodus.

Kaspersky Endpoint Security 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 Kaspersky Endpoint Security den Zugriff auf zusammengesetzte Dateien, erst nachdem die Dateien beliebiger Größe entpackt und untersucht wurden.

7. Speichern Sie die vorgenommenen Änderungen.

Untersuchungsmodus für Dateien ändern

Untersuchungsmodus bedeutet eine Bedingung, unter welcher die Komponente „Schutz vor bedrohlichen Dateien“ die Untersuchung einer Datei starten soll. Kaspersky Endpoint Security verwendet standardmäßig den intelligenten Untersuchungsmodus für Dateien. Um zu entscheiden, ob eine Untersuchung von Dateien erforderlich ist, analysiert die Komponente „Schutz vor bedrohlichen Dateien“ in diesem Modus die Vorgänge, die von einem Benutzer, von einem Programm im Auftrag eines Benutzers (mit dessen Benutzerdaten eine Anmeldung im Betriebssystem erfolgte, oder eines anderen Benutzers) oder vom Betriebssystem ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Word-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Dateien zu ändern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Wählen Sie im Block **Untersuchungsmodus** den erforderlichen Modus aus:

   - **Intelligenter Modus**. In diesem Untersuchungsmodus untersucht die „Schutz vor bedrohlichen Dateien“-Funktion ein Objekt auf Basis einer Analyse von Vorgängen, die mit ihm ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

   - **Bei Zugriff und Veränderungen**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ Objekte jedes Mal untersucht, wenn versucht wird, diese zu öffnen oder zu bearbeiten.

   - **Bei Zugriff**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ nur dann Objekte untersucht, wenn versucht wird, sie zu öffnen.

   - **Bei Ausführung**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien“ nur dann Objekte untersucht, wenn versucht wird, sie zu starten.

5. Speichern Sie die vorgenommenen Änderungen.

Container untersuchen

Ein *Container* ist eine isolierte Umgebung, in der ein Programm ohne direkte Interaktion mit dem Betriebssystem ausgeführt werden kann. Die Verwendung von Containern birgt folgende Risiken:

- Hacker können Schwachstellen in der Containerisierung ausnutzen, um Anwendungen innerhalb des Containers zu kompromittieren.
- Hacker können eine unsichere Konfiguration der Container-Umgebung ausnutzen, um sich unbefugten Zugriff auf die Daten auf dem Computer zu verschaffen oder die Systemintegrität zu gefährden.
- Wenn der Angriff auf einen Container erfolgreich ist, kann ein Hacker auf die Daten auf dem Computer zugreifen.
- Hacker können Schwachstellen im Netzwerk ausnutzen, um den Netzwerkverkehr abzufangen.

Kaspersky Endpoint Security untersucht Dateien nicht nur auf Festplatten, sondern auch in Containern. Kaspersky Endpoint Security ist also ein externes Tool zur Erkennung bösartiger Aktivitäten in Containern. Dadurch wird die Leistung von Containern aufrechterhalten und Konflikte mit anderen Anwendungen innerhalb des Containers werden vermeiden. Die Installation von Kaspersky Endpoint Security innerhalb des Containers wird nicht unterstützt.

Kaspersky Endpoint Security bietet Sicherheit für Container und die Programmkontrolle ermöglicht die Verwaltung von Anwendungen in Containern. Die Programmkontrolle wird für Container genauso konfiguriert wie für Anwendungen, die auf dem Computer installiert sind. Die Überwachung der Systemintegrität unterstützt auch Container.

Anforderungen an Container

- Der Container muss ein Docker-Container sein. Andere Containerisierungs-Tools werden nicht unterstützt.
- Der Container muss im Prozess-Isolationsmodus ausgeführt werden. Der Isolationsmodus Hyper-V wird nicht unterstützt.
- Der Container muss sich auf einem Server mit Windows Server 2016, 2019 oder 2022 befinden (Docker Host).
- Der Container muss ein Windows-Image enthalten (Docker Image). Windows 10 und 11 werden nicht unterstützt. Linux-Images werden nicht unterstützt.

Aktion beim Fund einer Bedrohung

Wenn in einem Container eine Bedrohung gefunden wird, wendet das Programm die Aktion an, die für die Komponente Schutz vor bedrohlichen Dateien ausgewählt wurde. Die Untersuchung von Containern bietet zusätzliche Einstellungen (siehe Anleitung unten). Wenn eine Bedrohung erkannt wird, blockiert das Programm die bösartige Aktivität und führt die ausgewählte Aktion aus (z. B. Objekt desinfizieren). Kaspersky Endpoint Security kann den Container anhalten, wenn das gefundene Objekt nicht desinfiziert werden kann. Die Funktion zum Anhalten von Containern ist standardmäßig deaktiviert.

So konfigurieren Sie die Untersuchung von Containern in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor bedrohlichen Dateien** aus.
4. Klicken Sie auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Erweitert**-Registerkarte aus.
6. Konfigurieren Sie im Block **Untersuchung von Dateivorgängen, die in Windows-Containern ausgeführt werden** die Einstellungen für die Untersuchung von Containern:
   - **Container anhalten, wenn 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.
   - **Dateivorgänge, die in Windows-Containern ausgeführt werden, nicht untersuchen**. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm den Container nur beim Starten des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung von Containern in der Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz → Schutz vor bedrohlichen Dateien**.
5. Wählen Sie unter **Erweiterte Einstellungen** die Registerkarte **Leistung** aus.
6. Konfigurieren Sie im Block **Untersuchung optimieren** die Einstellungen für die Untersuchung von Containern:
   - **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.
   - **Dateivorgänge, die in Windows-Containern ausgeführt werden, nicht untersuchen**. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm den Container nur beim Starten des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung von Containern in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor bedrohlichen Dateien** aus.
3. Konfigurieren Sie im Block **Untersuchung von Dateivorgängen, die in Windows-Containern ausgeführt werden** die Einstellungen für die Untersuchung von Containern:
   - **Container anhalten, wenn 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.
   - **Dateivorgänge, die in Windows-Containern ausgeführt werden, nicht untersuchen**. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm den Container nur beim Starten des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.
4. Speichern Sie die vorgenommenen Änderungen.

Programm-Überwachung

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Programm-Überwachung“ (HIPS, Host Intrusion Prevention System) hindert Programme daran, systemgefährdende Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und persönliche Daten. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken und des Cloud-Dienstes Kaspersky Security Network

Die Komponente kontrolliert Programme mithilfe von *Programmrechten*. Programmrechte beinhalten die folgenden Zugriffseinstellungen:

- Zugriff auf Betriebssystemressourcen (z. B. Autostart-Einstellungen und Registrierungsschlüssel)
- Zugriff auf persönliche Daten (z. B. auf Dateien und Programme)

Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.

Wenn ein Programm zum ersten Mal gestartet wird, führt die Komponente „Programm-Überwachung“ die folgenden Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.

2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Programm-Überwachung“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Platziert das Programm in einer der Vertrauensgruppen: *Vertrauenswürdig*, *Schwach beschränkt*, *Stark beschränkt*, *Nicht vertrauenswürdig*.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

   Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

   Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung“ aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Aktionen des Programms. Für Programme aus der Sicherheitsgruppe „*Stark beschränkt*“ ist beispielsweise der Zugriff auf Module des Betriebssystems verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde ein Programm nicht verändert, so wendet die Komponente die aktuellen Rechte für Programme darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Programm-Überwachung aktivieren und deaktivieren

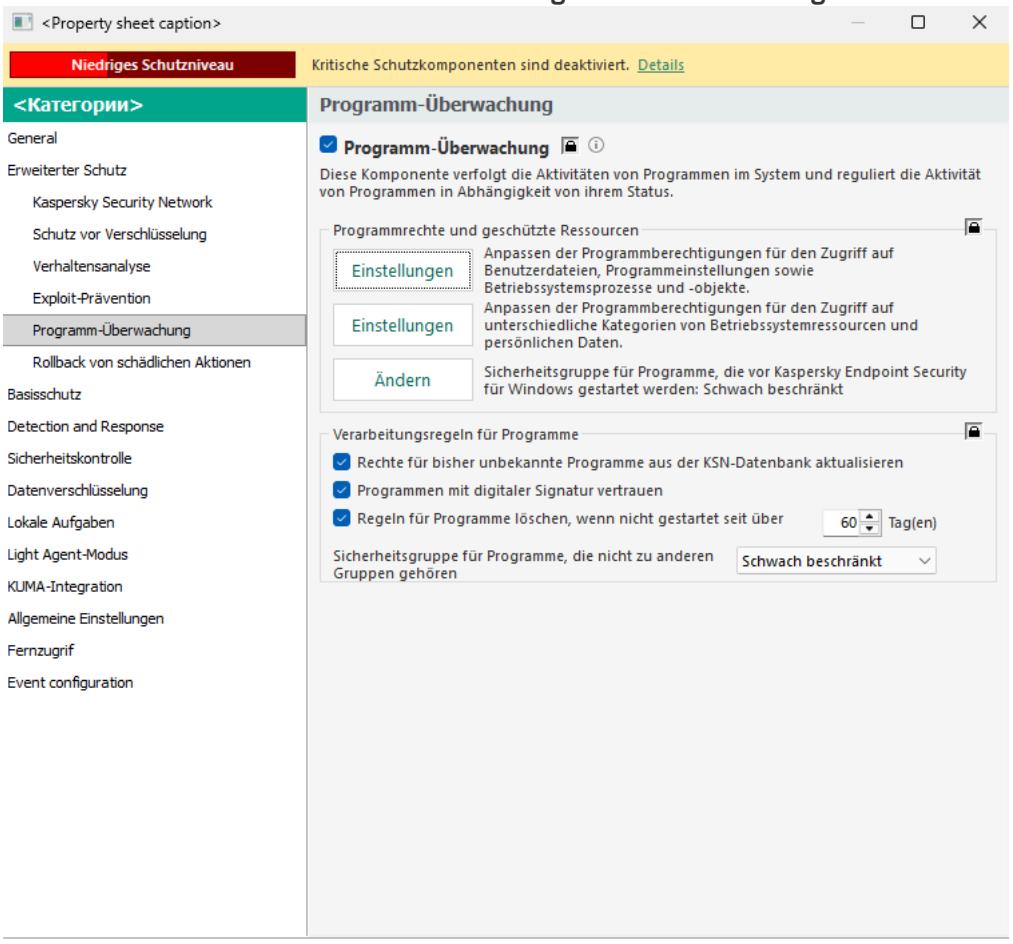
Die Programm-Überwachung ist standardmäßig aktiviert und läuft im Modus, der von Kaspersky empfohlen wird.

So aktivieren und deaktivieren Sie die Komponente „Programm-Überwachung“ in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Verwenden Sie das Kontrollkästchen **Programm-Überwachung**, um die Komponente zu aktivieren oder zu deaktivieren.

5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Programm-Überwachung“ in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.

5. Verwenden Sie den Schalter **Programm-Überwachung AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Programm-Überwachung“ in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Verwenden Sie den Schalter **Programm-Überwachung**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn die Komponente „Programm-Überwachung“ aktiviert ist, fügt Kaspersky Endpoint Security Programme zu Sicherheitsgruppen hinzu und berücksichtigt dabei die Stufe der Bedrohung, die das jeweilige Programm für den Computer darstellen kann. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe.

Sicherheitsgruppe für Programme verwenden

Wenn ein Programm zum ersten Mal gestartet wird, überprüft die Komponente „Programm-Überwachung“, ob das Programm sicher ist, und ordnet es einer Sicherheitsgruppe zu.

Beim ersten Schritt überprüft Kaspersky Endpoint Security, ob das Programm in der internen Datenbank für bekannte Programme verzeichnet ist, und sendet gleichzeitig eine Anfrage an die Datenbank von Kaspersky Security Network (sofern eine Internetverbindung besteht). Abhängig von den Ergebnissen der Überprüfung mit der internen Datenbank und der Datenbank von Kaspersky Security Network wird das Programm einer Sicherheitsgruppe zugeordnet. Bei jedem künftigen Programmstart sendet Kaspersky Endpoint Security eine neue Anfrage an die KSN-Datenbank, und weist das Programm einer anderen Sicherheitsgruppe zu, falls sich die Reputation des Programms in der KSN-Datenbank geändert hat.

Sie können eine Sicherheitsgruppe auswählen, der alle unbekannten Programme automatisch zugewiesen werden sollen. Programme, die vor dem Start von Kaspersky Endpoint Security ausgeführt wurden, werden automatisch der Sicherheitsgruppe zugewiesen, die in den Einstellungen der Programm-Überwachung festgelegt ist.

Für die Programme, die vor Kaspersky Endpoint Security gestartet wurden, wird nur die Netzwerkaktivität kontrolliert. Die Kontrolle erfolgt gemäß den Netzwerkregeln, die in den Firewall-Einstellungen festgelegt sind.

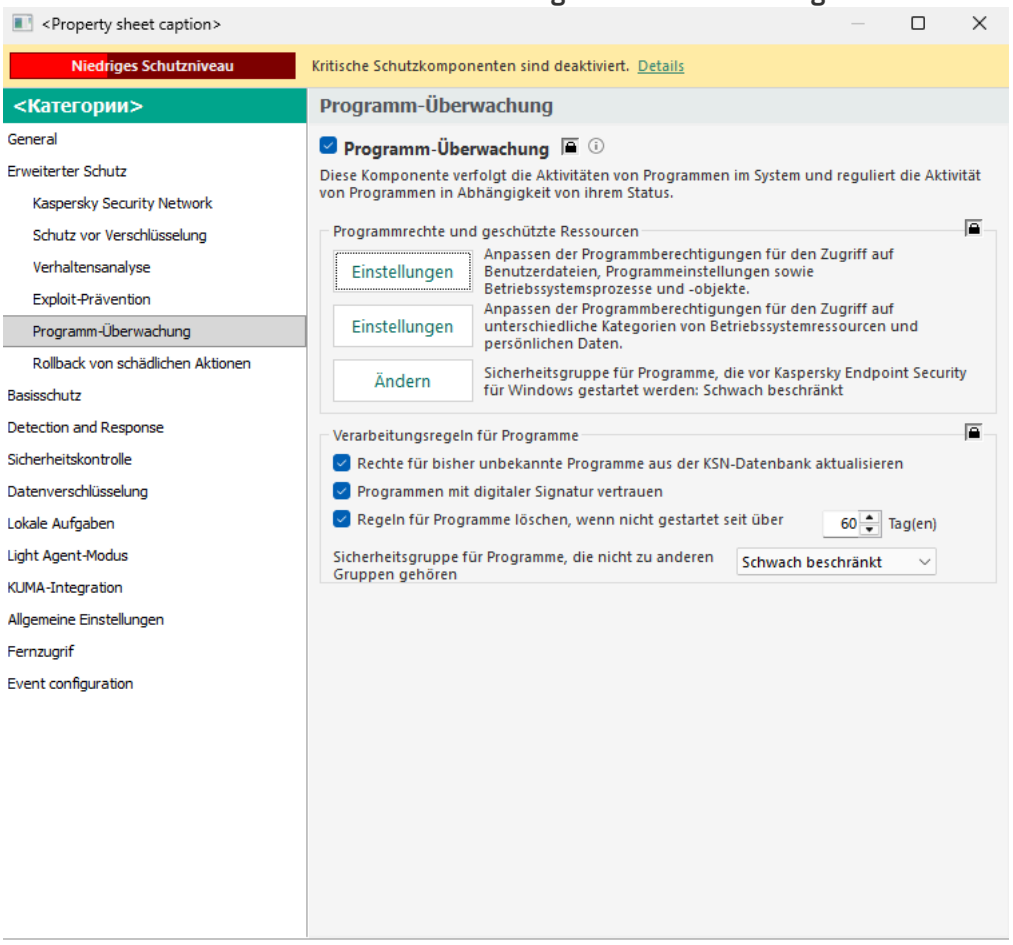
Die Sicherheitsgruppe eines Programms ändern

Wenn ein Programm zum ersten Mal gestartet wird, überprüft die Komponente „Programm-Überwachung“, ob das Programm sicher ist, und ordnet es einer Sicherheitsgruppe zu.

Die Kaspersky-Experten warnen davor, Programme aus einer Sicherheitsgruppe, der sie automatisch zugewiesen wurde, in andere Sicherheitsgruppen zu verschieben. Ändern Sie stattdessen bei Bedarf die Rechte für ein bestimmtes Programm.

So ändern Sie die Sicherheitsgruppe eines Programms in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
5. Wählen Sie die Registerkarte **Rechte für Programme** aus.
6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie im angezeigten Fenster die Suchkriterien für die Anwendung ein, deren Sicherheitsgruppe Sie ändern möchten.

   Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
8. Klicken Sie auf **Aktualisieren**.

   Kaspersky Endpoint Security sucht in der konsolidierten Liste der auf den verwalteten Computern installierten Programme nach dem Programm. Kaspersky Endpoint Security zeigt eine Liste der Programme an, die Ihren Suchkriterien entsprechen.
9. Wählen Sie das erforderliche Programm.

10. Wählen Sie in der Dropdown-Liste **Ausgewähltes Programm zur Sicherheitsgruppe hinzufügen** die entsprechende Sicherheitsgruppe für das Programm aus.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So ändern Sie die Sicherheitsgruppe eines Programms in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.

5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.

6. Wählen Sie die Registerkarte **Rechte für Programme** aus.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.

7. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms zu einer Sicherheitsgruppe wird gestartet.

8. Wählen Sie die entsprechende Sicherheitsgruppe für das Programm.

9. Wählen Sie den Typ **Programm** aus. Weiter zum nächsten Schritt

   Wenn Sie die Sicherheitsgruppe für mehrere Programme ändern möchten, wählen Sie den Typ **Gruppe** aus und legen Sie den Namen der Programmgruppe fest.

10. Wählen Sie in der geöffneten Liste mit Programmen die Programme aus, deren Sicherheitsgruppe Sie ändern möchten.

    Verwenden Sie einen Filter. Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

11. Schließen Sie den Assistenten ab.

    Das Programm wird der Sicherheitsgruppe hinzugefügt.

12. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie die Sicherheitsgruppe eines Programms in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.

3. Klicken Sie auf **Programme verwalten**.

   Dadurch wird die Liste der installierten Programme geöffnet.

4. Wählen Sie das erforderliche Programm.

5. Klicken Sie im Kontextmenü des Programms auf **Beschränkungen → <Sicherheitsgruppe>**.

6. Speichern Sie die vorgenommenen Änderungen.

Daraufhin wird das Programm zu einer anderen Sicherheitsgruppe hinzugefügt. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe. Dem Programm wird der Status *(benutzerdefiniert)* zugewiesen. Wenn sich die Reputation des Programms in Kaspersky Security Network ändert, lässt die Komponente „Programm-Überwachung“ die Sicherheitsgruppe dieses Programms unverändert.

Rechte von Sicherheitsgruppen konfigurieren

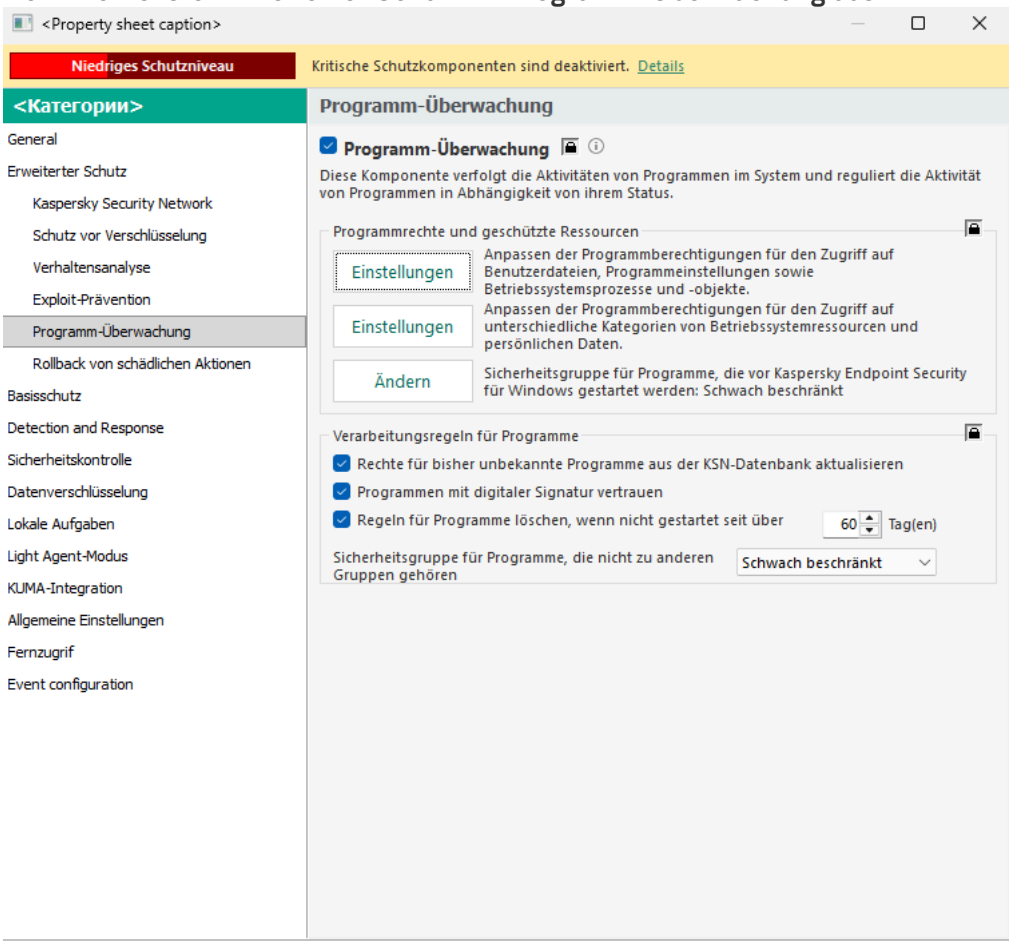
Die optimalen Programmrechte werden standardmäßig für verschiedene Sicherheitsgruppen erstellt. Die Einstellungen für die Rechte von Programmgruppen, die zu einer Sicherheitsgruppe gehören, erben die Einstellungswerte der Rechte für die Sicherheitsgruppen.

So ändern Sie die Rechte von Sicherheitsgruppen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.

5. Gehen Sie zur Registerkarte **Rechte für Programme**.
6. Wählen Sie die gewünschte Sicherheitsgruppe aus.
7. Wählen Sie im Kontextmenü der Sicherheitsgruppe den Punkt **Rechte der Gruppe** aus.

   Die Eigenschaften der Sicherheitsgruppe werden geöffnet.
8. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.
   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

   Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.
9. Öffnen Sie für die gewünschte Ressource in der Spalte der entsprechenden Aktion durch Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** (✓) oder **Verbieten** (⊘).
10. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **Protokollieren** (✓ / ⊘).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.
11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So ändern Sie die Rechte einer Sicherheitsgruppe in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Gehen Sie zur Registerkarte **Rechte für Programme**.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.
7. Wählen Sie im linken Bereich des Fensters die gewünschte Sicherheitsgruppe aus.

8. Führen Sie im rechten Bereich des Fensters in der Dropdown-Liste eine der folgenden Aktionen aus:

   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.
   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

   Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.

9. Wählen Sie für die Ressource in der Spalte der entsprechenden Aktion die erforderliche Option aus: **Erben**, **Erlauben** (), **Blockieren** ().

10. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **Ereignisse protokollieren** (/).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

11. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie Sicherheitsgruppenrechte in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Klicken Sie auf **Programme verwalten**.

   Dadurch wird die Liste der installierten Programme geöffnet.

4. Wählen Sie die gewünschte Sicherheitsgruppe aus.
5. Wählen Sie im Kontextmenü der Sicherheitsgruppe den Punkt **Details und Regeln** aus.

   Die Eigenschaften der Sicherheitsgruppe werden geöffnet.

6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.
   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

   Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.

7. Öffnen Sie für die gewünschte Ressource in der Spalte der entsprechenden Aktion durch Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** () oder **Verbieten** ().

8. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **Ereignisse protokollieren** ( ).

   Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

9. Speichern Sie die vorgenommenen Änderungen.

Die Rechte der Sicherheitsgruppe werden geändert. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe. Der Status ■ (*Benutzerdefinierte Einstellungen*) wird der Sicherheitsgruppe zugewiesen.

Sicherheitsgruppe für Programme wählen, die vor Kaspersky Endpoint Security gestartet werden

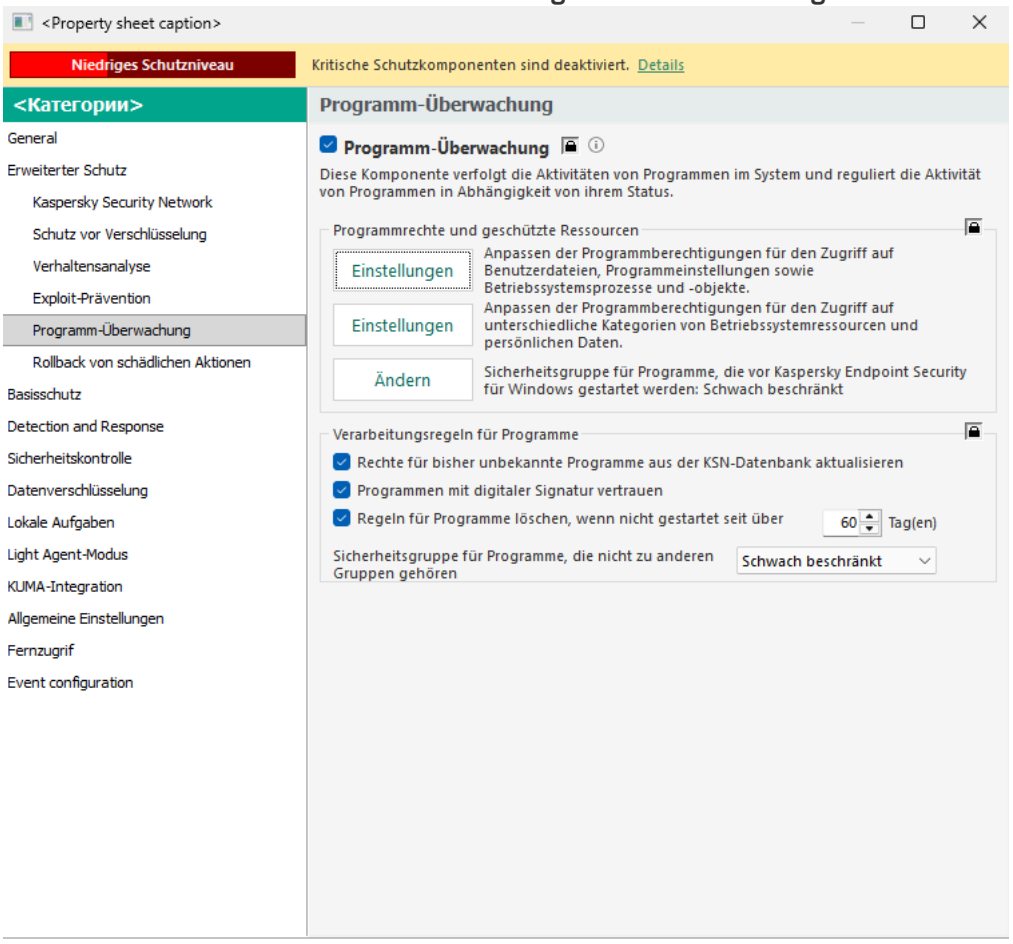
Für die Programme, die vor Kaspersky Endpoint Security gestartet wurden, wird nur die Netzwerkaktivität kontrolliert. Die Kontrolle erfolgt gemäß den Netzwerkregeln, die in den Firewall-Einstellungen festgelegt sind. Um festzulegen, durch welche Netzwerkregeln die Kontrolle der Netzwerkaktivität solcher Programme reguliert werden soll, muss eine Sicherheitsgruppe angegeben werden.

So wählen Sie eine Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden, in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf **Ändern**.

5. Wählen Sie die entsprechende Sicherheitsgruppe für die Einstellung **Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden**.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie eine Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden, in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.

5. Wählen Sie die entsprechende Sicherheitsgruppe für die Einstellung **Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden**.

6. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden, in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Wählen Sie im Block **Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden** die passende Sicherheitsgruppe aus.
4. Speichern Sie die vorgenommenen Änderungen.

Von nun an werden Programme, die vor Kaspersky Endpoint Security gestartet werden, zu einer anderen Sicherheitsgruppe hinzugefügt. Kaspersky Endpoint Security blockiert von nun an die Aktionen des Programms abhängig von der Sicherheitsgruppe.

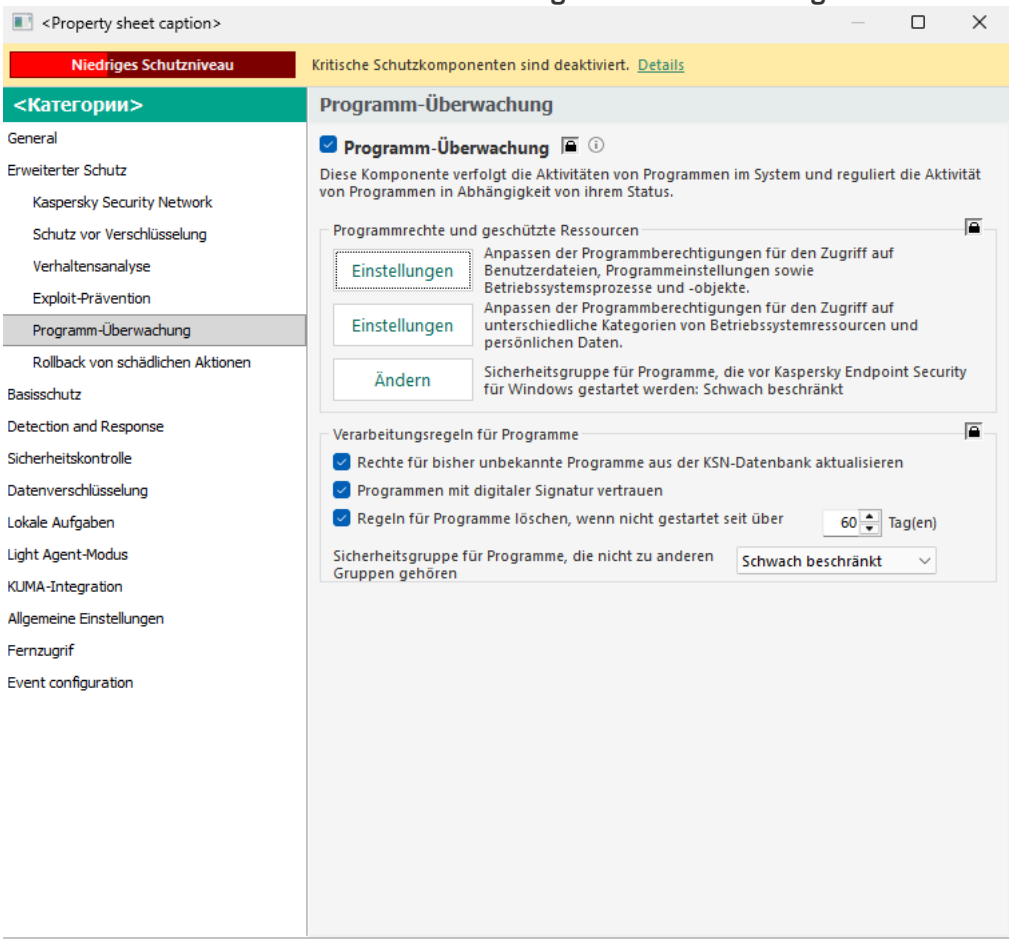
Eine Sicherheitsgruppe für unbekannte Programme auswählen

Wenn ein Programm zum ersten Mal gestartet wird, ermittelt die Komponente „Programm-Überwachung“ die geeignete Sicherheitsgruppe für das Programm. Wenn Sie keinen Internetzugang haben oder wenn Kaspersky Security Network keine Informationen zu diesem Programm hat, ordnet Kaspersky Endpoint Security das Programm standardmäßig der Gruppe „*Schwach beschränkt*“ zu. Sobald Informationen zu einem zuvor unbekannten Programm in KSN gefunden werden, aktualisiert Kaspersky Endpoint Security die Rechte dieses Programms. Die Programmrechte können danach manuell angepasst werden.

So wählen Sie eine Sicherheitsgruppe für unbekannte Programme in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Verwenden Sie im Block **Verarbeitungsregeln für Programme** die Dropdown-Liste **Sicherheitsgruppe für Programme, die nicht zu anderen Gruppen gehören**, um die gewünschte Sicherheitsgruppe auszuwählen.

   Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente „Programm-Überwachung“ vorgegeben.

5. Verwenden Sie das Kontrollkästchen **Rechte für bisher unbekannte Programme aus der KSN-Datenbank aktualisieren**, um das automatische Update der Rechte unbekannter Programme zu konfigurieren.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie eine Sicherheitsgruppe für unbekannte Programme in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.

5. Verwenden Sie im Block **Verarbeitungsregeln für Programme** die Dropdown-Liste **Sicherheitsgruppe für Programme, die nicht zu anderen Gruppen gehören**, um die gewünschte Sicherheitsgruppe auszuwählen.

   Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente „Programm-Überwachung“ vorgegeben.

6. Verwenden Sie das Kontrollkästchen **Rechte für bisher unbekannte Programme aus der KSN-Datenbank aktualisieren**, um das automatische Update der Rechte unbekannter Programme zu konfigurieren.

7. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für unbekannte Programme in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.

3. Wählen Sie im Block **Verarbeitungsregeln für Programme** die entsprechende Sicherheitsgruppe aus.

   Wenn die Teilnahme an Kaspersky Security Network aktiviert ist, sendet Kaspersky Endpoint Security jedes Mal, wenn ein Programm gestartet wird, eine Reputationsabfrage an KSN. Aufgrund der Antwort kann das Programm in eine andere Sicherheitsgruppe verschoben werden, als in den Einstellungen der Komponente „Programm-Überwachung“ vorgegeben.

4. Verwenden Sie das Kontrollkästchen **Regeln für bisher unbekannte Programme aus KSN aktualisieren**, um das automatische Update der Rechte unbekannter Programme zu konfigurieren.

5. Speichern Sie die vorgenommenen Änderungen.

Eine Sicherheitsgruppe für digital signierte Programme wählen

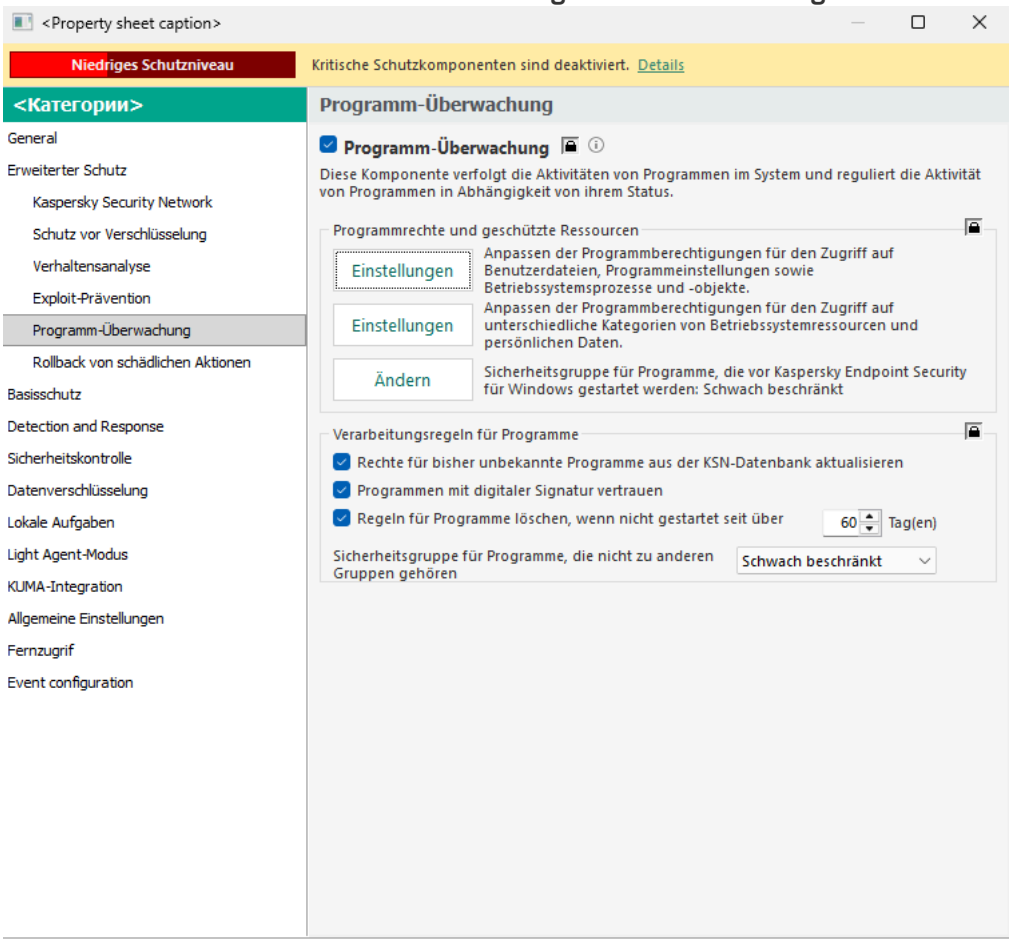
Programme, die mit Microsoft-Zertifikaten oder mit Kaspersky-Zertifikaten signiert sind, werden von Kaspersky Endpoint Security immer der Sicherheitsgruppe „*Vertrauenswürdig*“ zugeordnet.

So wählen Sie eine Sicherheitsgruppe für digital signierte Programme in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Verwenden Sie im Block **Verarbeitungsregeln für Programme** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, um für Programme mit der digitalen Signatur eines vertrauenswürdigen Herstellers die automatische Zuweisung zur Sicherheitsgruppe Vertrauenswürdig zu aktivieren bzw. zu deaktivieren.

   Vertrauenswürdige Hersteller sind Softwareanbieter, die Kaspersky in die vertrauenswürdige Gruppe aufgenommen hat. Sie können ein Herstellerzertifikat auch manuell zum Systemspeicher für vertrauenswürdige Zertifikate hinzufügen.

   Ist das Kontrollkästchen deaktiviert, so werden Programme, die eine digitale Signatur besitzen, von der Komponente „Programm-Überwachung“ nicht als vertrauenswürdig eingestuft und anhand anderer Kriterien auf die Sicherheitsgruppen verteilt.

5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie eine Sicherheitsgruppe für digital signierte Programme in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.

5. Verwenden Sie im Block **Verarbeitungsregeln für Programme** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, um für Programme mit der digitalen Signatur eines vertrauenswürdigen Herstellers die automatische Zuweisung zur Sicherheitsgruppe Vertrauenswürdig zu aktivieren bzw. zu deaktivieren.

   Vertrauenswürdige Hersteller sind Softwareanbieter, die Kaspersky in die vertrauenswürdige Gruppe aufgenommen hat. Sie können ein Herstellerzertifikat auch manuell zum Systemspeicher für vertrauenswürdige Zertifikate hinzufügen.

   Ist das Kontrollkästchen deaktiviert, so werden Programme, die eine digitale Signatur besitzen, von der Komponente „Programm-Überwachung“ nicht als vertrauenswürdig eingestuft und anhand anderer Kriterien auf die Sicherheitsgruppen verteilt.

6. Speichern Sie die vorgenommenen Änderungen.

So wählen Sie eine Sicherheitsgruppe für digital signierte Programme in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.
3. Verwenden Sie im Block **Verarbeitungsregeln für Programme** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, um für Programme mit der digitalen Signatur eines vertrauenswürdigen Herstellers die automatische Zuweisung zur Sicherheitsgruppe Vertrauenswürdig zu aktivieren bzw. zu deaktivieren.

   Vertrauenswürdige Hersteller sind Softwareanbieter, die Kaspersky in die vertrauenswürdige Gruppe aufgenommen hat. Sie können ein Herstellerzertifikat auch manuell zum Systemspeicher für vertrauenswürdige Zertifikate hinzufügen.

   Ist das Kontrollkästchen deaktiviert, so werden Programme, die eine digitale Signatur besitzen, von der Komponente „Programm-Überwachung“ nicht als vertrauenswürdig eingestuft und anhand anderer Kriterien auf die Sicherheitsgruppen verteilt.

4. Speichern Sie die vorgenommenen Änderungen.

Verwendung von Rechten für Programme

Standardmäßig basiert die Aktivitätskontrolle für Programme auf Programmrechten. Diese Rechte werden für die jeweilige Sicherheitsgruppe festgelegt, in die das Programm bei seinem ersten Start von Kaspersky Endpoint Security verschoben wurde. Bei Bedarf können Sie die Programmrechte für eine gesamte Sicherheitsgruppe, für ein einzelnes Programm oder für eine Programmgruppe innerhalb einer Sicherheitsgruppe bearbeiten.

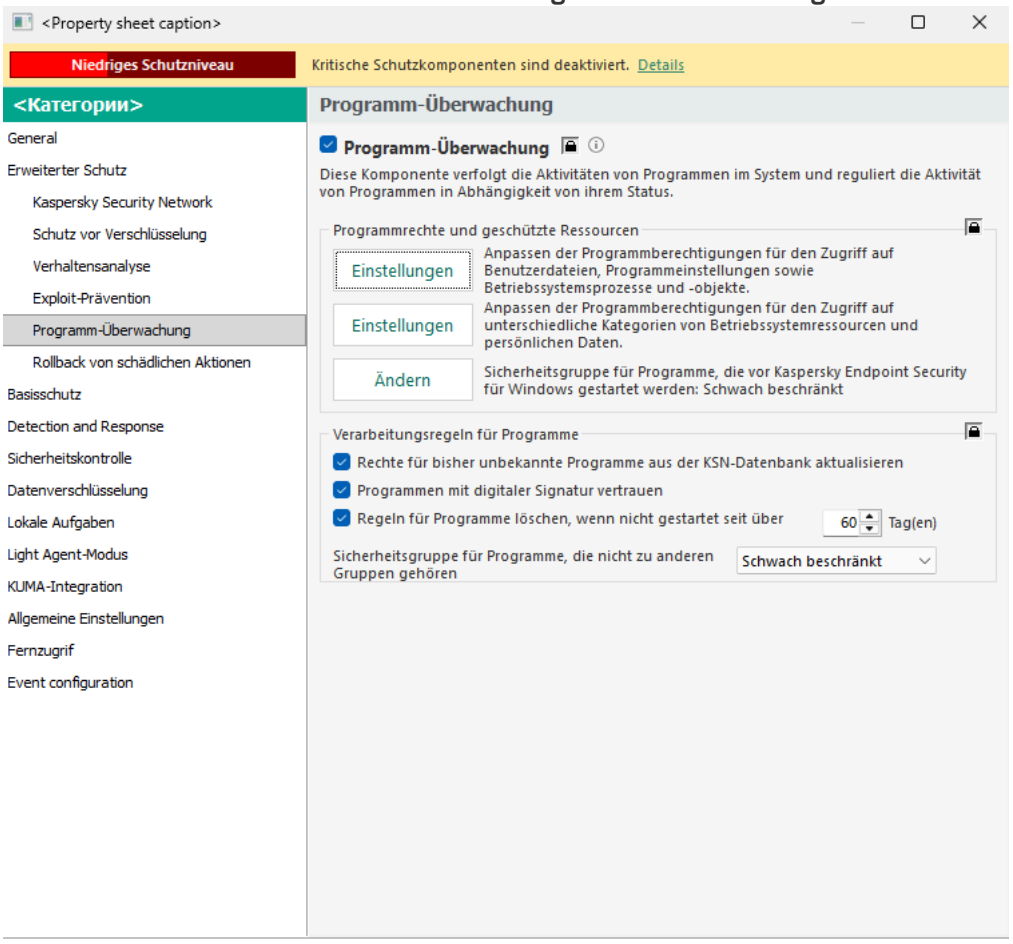
Manuell festgelegte Programmrechte haben eine höhere Priorität als Programmrechte, die für eine Sicherheitsgruppe festgelegt wurden. Mit anderen Worten: Wenn manuell angelegte Programmrechte sich von den für die Sicherheitsgruppe festgelegten Programmrechten unterscheiden, kontrolliert die Komponente „Programm-Überwachung“ die Programmaktivität gemäß den manuell angelegten Programmrechten.

Die Regeln, die Sie für Programme erstellen, werden für untergeordnete Programme übernommen. Wenn Sie beispielsweise alle Netzwerkaktivitäten für cmd.exe verbieten, so werden auch für notepad.exe alle Netzwerkaktivitäten verboten, wenn dieses Programm über cmd.exe gestartet wird. Wenn ein Programm nicht dem Programm untergeordnet ist, von dem es ausgeführt wird, werden die Regeln nicht vererbt.

So ändern Sie die Programmrechte in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.

5. Gehen Sie zur Registerkarte **Rechte für Programme**.

6. Klicken Sie auf **Hinzufügen**.

7. Geben Sie im angezeigten Fenster die Suchkriterien für die Anwendung ein, deren Anwendungsrechte Sie ändern möchten.

   Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

8. Klicken Sie auf **Aktualisieren**.

   Kaspersky Endpoint Security sucht in der konsolidierten Liste der auf den verwalteten Computern installierten Programme nach dem Programm. Kaspersky Endpoint Security zeigt eine Liste der Programme an, die Ihren Suchkriterien entsprechen.

9. Wählen Sie das erforderliche Programm.

10. Wählen Sie in der Dropdown-Liste **Ausgewähltes Programm zur Sicherheitsgruppe hinzufügen** den Punkt **Ursprüngliche Gruppen** aus und klicken Sie auf **OK**.

    Das Programm wird der Standardgruppe hinzugefügt.

11. Wählen Sie das gewünschte Programm aus und klicken Sie dann auf **Rechte für Programme** im Kontextmenü des Programms.

    Dadurch werden die Programmeigenschaften geöffnet.

12. Führen Sie eine der folgenden Aktionen aus:

    - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.
    - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

    Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.

13. Öffnen Sie für die gewünschte Ressource in der Spalte der entsprechenden Aktion durch Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** (✓) oder **Verbieten** (⊘).

14. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **Protokollieren** (✓ / ⊘).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

15. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So ändern Sie die Programmrechte in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Programm-Überwachung**.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Gehen Sie zur Registerkarte **Rechte für Programme**.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.
7. Klicken Sie auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms zu einer Sicherheitsgruppe wird gestartet.
8. Wählen Sie die entsprechende Sicherheitsgruppe für das Programm.
9. Wählen Sie den Typ **Programm** aus. Weiter zum nächsten Schritt

   Wenn Sie die Sicherheitsgruppe für mehrere Programme ändern möchten, wählen Sie den Typ **Gruppe** aus und legen Sie den Namen der Programmgruppe fest.

10. Wählen Sie in der geöffneten Liste mit Programmen die Programme aus, deren Programmrechte Sie ändern möchten.

    Verwenden Sie einen Filter. Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

11. Schließen Sie den Assistenten ab.

    Das Programm wird der Sicherheitsgruppe hinzugefügt.

12. Klicken Sie im linken Fensterbereich auf das gewünschte Programm.

13. Führen Sie im rechten Bereich des Fensters in der Dropdown-Liste eine der folgenden Aktionen aus:

    - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.

    - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

    > Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.

14. Wählen Sie für die Ressource in der Spalte der entsprechenden Aktion die erforderliche Option aus: **Erben**, **Erlauben** (), **Blockieren** ().

15. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **Ereignisse protokollieren** (/).

    Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

16. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie Programmrechte in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Programm-Überwachung** aus.

3. Klicken Sie auf **Programme verwalten**.

    Dadurch wird die Liste der installierten Programme geöffnet.

4. Wählen Sie das erforderliche Programm.

5. Wählen Sie im Kontextmenü des Programms den Punkt **Details und Regeln** aus.

    Dadurch werden die Programmeigenschaften geöffnet.

6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, welche die Vorgänge mit der Registrierung des Betriebssystems, mit Benutzerdateien und mit Programmeinstellungen regeln, wählen Sie **Dateien und Systemregistrierung** aus.

   - Wenn Sie die Sicherheitsgruppenrechte bearbeiten möchten, die den Zugriff auf Prozesse und Objekte des Betriebssystems regeln, wählen Sie **Rechte** aus.

7. Öffnen Sie für die gewünschte Ressource in der Spalte der entsprechenden Aktion durch Rechtsklick das Kontextmenü und wählen Sie die erforderliche Option aus: **Erben**, **Erlauben** () oder **Verbieten** ().

8. Wenn Sie die Verwendung von Computerressourcen überwachen möchten, wählen Sie **Ereignisse protokollieren** ().

   Kaspersky Endpoint Security speichert Informationen über den Betrieb der Komponente „Programm-Überwachung“. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

9. Wählen Sie die Registerkarte **Ausnahmen** und konfigurieren Sie die erweiterten Einstellungen des Programms (siehe Tabelle unten).

10. Speichern Sie die vorgenommenen Änderungen.

Erweiterte Einstellungen des Programms

Einstellung	Beschreibung
Dateien, die dieses Programm öffnet, nicht untersuchen	Alle Dateien, die vom Programm geöffnet werden, sind von der Überprüfung durch Kaspersky Endpoint Security ausgeschlossen. Wenn Sie z. B. Programme zum Backup von Dateien verwenden, trägt diese Funktion dazu bei, den Ressourcenverbrauch von Kaspersky Endpoint Security zu reduzieren.
Programmaktivität nicht überwachen	Kaspersky Endpoint Security überwacht die Datei- und Netzwerkaktivität des Programms im Betriebssystem nicht. Sie können die Überwachung der Programmaktivität für verschiedene Komponenten von Kaspersky Endpoint Security konfigurieren: • **Nicht überwachen für Schutz- und Kontrollkomponenten**. Die Programmaktivität wird durch die folgenden Komponenten überwacht: Verhaltensanalyse, Exploit-Prävention, Programm-Überwachung, Rollback von schädlichen Aktionen und Firewall. • **Nicht überwachen für Managed Detection and Response und Endpoint Detection and Response**. Die Programmaktivität wird überwacht vom integrierten MDR-Agent und vom integrierten EDR (KATA) Agent. • **Interaktive Konsoleneingaben für Endpoint Detection and Response nicht abfangen**. Telemetriedaten über die Verwaltung der App in der Konsole werden durch Kaspersky Endpoint Security nicht gesendet. Telemetriedaten werden von Kaspersky Anti Targeted Attack Platform (EDR) verwendet.
Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen	Die für den übergeordneten Prozess konfigurierten Einschränkungen werden von Kaspersky Endpoint Security nicht auf einen untergeordneten Prozess angewendet. Der übergeordnete Prozess wird von einem Programm gestartet, für das Programmrechte (Host Intrusion Prevention) und Netzwerkregeln für das Programm (Firewall) konfiguriert sind.
Aktivität von Unterprogrammen nicht überwachen	Kaspersky Endpoint Security überwacht nicht die Datei- und Netzwerkaktivität der Programme, die von diesem Programm gestartet werden. Sie können die Ausnahme rekursiv anwenden. Dadurch wird erreicht, dass die App nicht die Aktivität der gesamten Kette von untergeordneten Programmen überwacht.

Einstellung	Beschreibung
Interaktion mit der Programmoberfläche von Kaspersky Endpoint Security zulassen	Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security blockiert alle Versuche, Programme von einem Remote-Computer aus zu verwalten. Ist dieses Kontrollkästchen aktiviert, wird einem Remote-Administrationsprogramm erlaubt, Einstellungen für Kaspersky Endpoint Security über die Benutzeroberfläche von Kaspersky Endpoint Security zu verwalten.
Verschlüsselten Datenverkehr nicht untersuchen / Gesamten Datenverkehr nicht untersuchen	Der von diesem Programm initiierte Netzwerkverkehr wird von den Untersuchungen durch Kaspersky Endpoint Security ausgeschlossen. Sie können entweder den gesamten Verkehr oder nur den verschlüsselten Verkehr von den Untersuchungen ausschließen. Sie können auch einzelne IP-Adressen und Portnummern von Untersuchungen ausschließen. Kaspersky Endpoint Security Version 14.0 oder früher unterstützt den Ausschluss von Netzwerkverkehr nicht, wenn für ein vertrauenswürdiges Programm anstelle eines Pfads ein Hash angegeben ist.

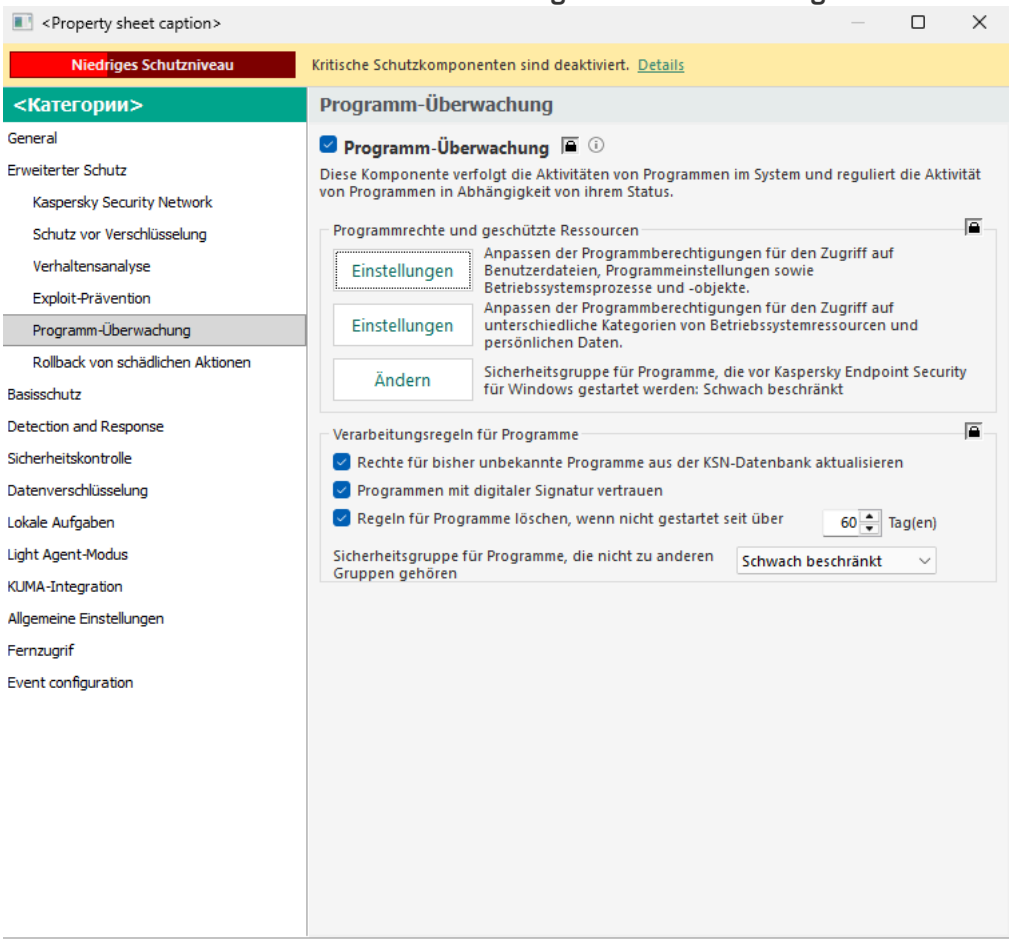
Schutz für Betriebssystemressourcen und persönliche Daten

Die Komponente „Programm-Überwachung“ verwaltet die Rechte von Programmen hinsichtlich ihren Vorgängen mit diversen Ressourcenkategorien des Betriebssystems und persönlichen Daten. Die Kaspersky-Experten haben Kategorien für geschützte Ressourcen vordefiniert. So enthält z. B. die Kategorie *Betriebssystem* die Unterkategorie *Starteinstellungen*, in der alle Registrierungsschlüssel aufgelistet sind, die mit dem Autostart von Programmen verknüpft sind. Die für geschützte Ressourcen vorgegebenen Kategorien und die damit zusammenhängenden geschützten Ressourcen können nicht geändert oder gelöscht werden.

Hinzufügen oder Löschen einer geschützten Ressource in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf **Einstellungen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.

5. Gehen Sie zur Registerkarte **Geschützte Ressourcen**.

   Im linken Bereich des Fensters sehen Sie eine Liste mit geschützten Ressourcen und die entsprechenden Rechte für den Zugriff auf diese Ressourcen, abhängig von der jeweiligen Sicherheitsgruppe.

6. Wählen Sie die Kategorie der geschützten Ressourcen aus, zu der Sie eine neue geschützte Ressource hinzufügen möchten.

   Wenn Sie eine Unterkategorie hinzufügen möchten, klicken Sie auf **Hinzufügen** → **Kategorie**.

7. Klicken Sie auf die Schaltfläche **Hinzufügen**. Wählen Sie in der Dropdown-Liste den Typ der Ressource aus, die Sie hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.

8. Wählen Sie im folgenden Fenster eine Datei, einen Ordner oder einen Registrierungsschlüssel aus.

   Sie können die Programmrechte für den Zugriff auf die hinzugefügten Ressourcen anzeigen. Wählen Sie dazu im linken Bereich des Fensters eine hinzugefügte Ressource aus. Kaspersky Endpoint Security zeigt daraufhin die Zugriffsrechte für jede Sicherheitsgruppe an. Die Kontrolle der Programmaktivität für Ressourcen kann auch mithilfe des Kontrollkästchens neben der neuen Ressource deaktiviert werden.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie eine geschützte Ressource in der Web Console und der Cloud Console hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz → Programm-Überwachung**.
5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Programmrechte und geschützte Ressourcen**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.
6. Gehen Sie zur Registerkarte **Geschützte Ressourcen**.

   Im linken Bereich des Fensters sehen Sie eine Liste mit geschützten Ressourcen und die entsprechenden Rechte für den Zugriff auf diese Ressourcen, abhängig von der jeweiligen Sicherheitsgruppe.
7. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Ressourcen wird gestartet.
8. Wählen Sie im Block **Gruppenname** die Kategorie der geschützten Ressourcen aus, der Sie die neue geschützte Ressource hinzufügen möchten.

   Wenn Sie eine Unterkategorie hinzufügen möchten, wählen Sie die Option **Kategorie für geschützte Ressourcen** aus.
9. Wählen Sie den Typ der Ressource aus, die Sie hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.
10. Wählen Sie eine Datei, einen Ordner oder einen Registrierungsschlüssel aus.
11. Schließen Sie den Assistenten ab.

    Sie können die Programmrechte für den Zugriff auf die hinzugefügten Ressourcen anzeigen. Wählen Sie dazu im linken Bereich des Fensters eine hinzugefügte Ressource aus. Kaspersky Endpoint Security zeigt daraufhin die Zugriffsrechte für jede Sicherheitsgruppe an. Die Kontrolle der Programmaktivität für Ressourcen kann auch mithilfe des Kontrollkästchens in der Spalte **Status** deaktiviert werden.
12. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine geschützte Ressource in der Programmoberfläche hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz → Programm-Überwachung** aus.
3. Klicken Sie auf **Ressourcen verwalten**.

   Die Liste der geschützten Ressourcen wird geöffnet.
4. Wählen Sie die Kategorie der geschützten Ressourcen aus, zu der Sie eine neue geschützte Ressource hinzufügen möchten.

   Wenn Sie eine Unterkategorie hinzufügen möchten, klicken Sie auf **Hinzufügen → Kategorie**.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**. Wählen Sie in der Dropdown-Liste den Typ der Ressource aus, die Sie hinzufügen möchten: **Datei oder Ordner** oder **Registrierungsschlüssel**.

6. Wählen Sie im folgenden Fenster eine Datei, einen Ordner oder einen Registrierungsschlüssel aus.

   Sie können die Programmrechte für den Zugriff auf die hinzugefügten Ressourcen anzeigen. Wählen Sie dazu im linken Bereich des Fensters eine hinzugefügte Ressource aus. Kaspersky Endpoint Security zeigt daraufhin eine Liste mit Programmen und die Zugriffsrechte für jedes Programm an. Die Kontrolle der Programmaktivität für Ressourcen kann auch mithilfe der Schaltfläche **Kontrolle aktivieren** in der Spalte **Status** deaktiviert werden.

7. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Endpoint Security steuert den Zugriff auf die hinzugefügten Betriebssystemressourcen und auf persönliche Daten. Kaspersky Endpoint Security steuert den Zugriff eines Programms auf Ressourcen unter Berücksichtigung der Sicherheitsgruppe, die dem Programm zugewiesen wurde. Die Sicherheitsgruppe eines Programms kann geändert werden.

Löschen von Informationen über nicht verwendete Programme

Kaspersky Endpoint Security kontrolliert mithilfe von Programmrechten die Verwendung von Programmen. Die Rechte eines Programms sind von der Sicherheitsgruppe abhängig. Kaspersky Endpoint Security ordnet ein Programm einer Sicherheitsgruppe zu, wenn das Programm zum ersten Mal gestartet wird. Sie können die Sicherheitsgruppe für ein Programm manuell ändern. Außerdem können Sie die Rechte für ein bestimmtes Programm manuell anpassen. Kaspersky Endpoint Security speichert die folgenden Informationen über ein Programm: Sicherheitsgruppe und Rechte des Programms.

Kaspersky Endpoint Security löscht automatisch Informationen über nicht verwendete Programme, um Computer-Ressourcen zu sparen. Um Informationen über Programme zu löschen, richtet sich Kaspersky Endpoint Security nach folgenden Regeln:

- Wenn die Sicherheitsgruppe und die Programmrechte automatisch festgelegt wurden, löscht Kaspersky Endpoint Security die Informationen über dieses Programm nach 30 Tagen. Es ist nicht möglich, die Speicherdauer für Informationen über ein Programm zu ändern oder das automatische Löschen zu deaktivieren.

- Wenn Sie das Programm einer Sicherheitsgruppe zugewiesen oder die Programmrechte manuell angepasst haben, löscht Kaspersky Endpoint Security die Informationen über dieses Programm nach 60 Tagen (Standardwert). Sie können die Speicherdauer für Informationen über das Programm ändern oder das automatische Löschen deaktivieren (siehe Anleitung unten).

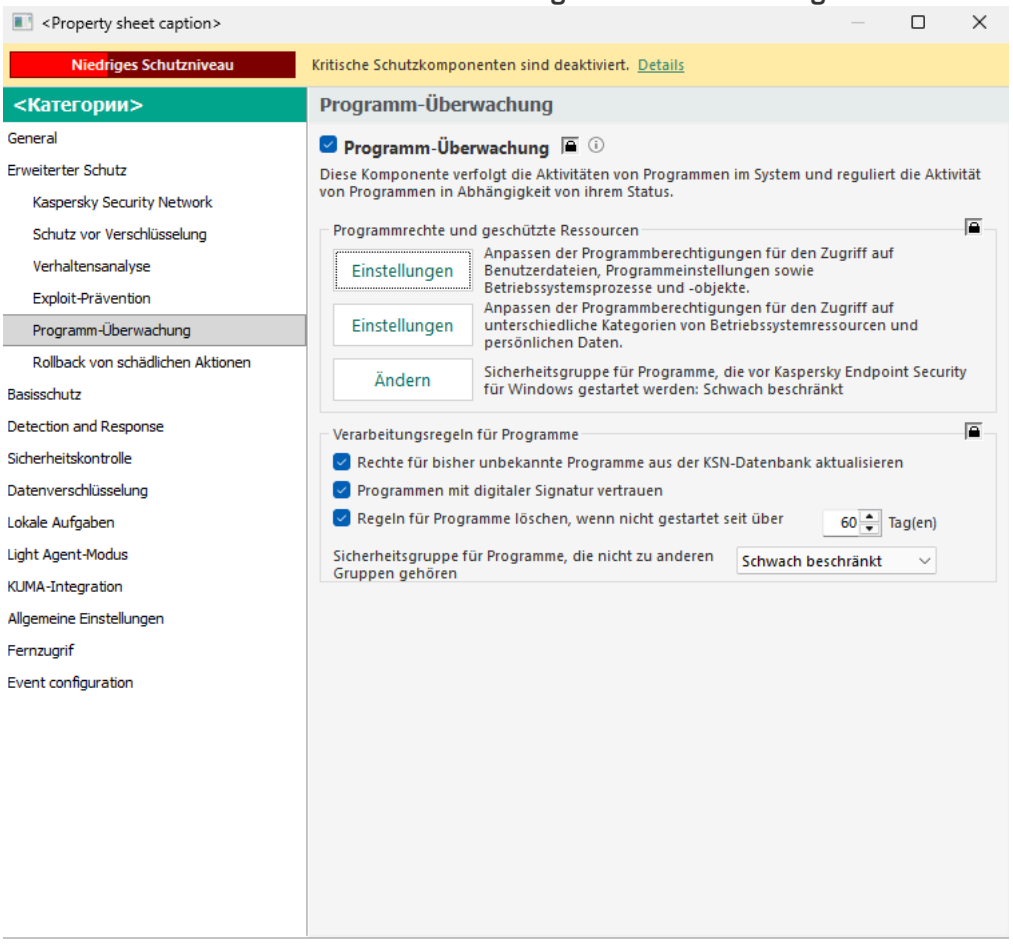
Wenn ein Programm gestartet wird, über das Informationen gelöscht wurden, untersucht Kaspersky Endpoint Security das Programm wie beim ersten Start.

So konfigurieren Sie das automatische Löschen von Informationen zu nicht verwendeten Programmen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Programm-Überwachung** aus.



Einstellungen der Programm-Überwachung

4. Führen Sie im Block **Verarbeitungsregeln für Programme** eine der folgenden Aktionen aus:

   - Wenn Sie das automatische Löschen konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit über n Tag(en)** und geben Sie die Anzahl der Tage ein.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, werden von Kaspersky Endpoint Security nach dem festgelegten Zeitraum gelöscht. Nach 30 Tagen löscht Kaspersky Endpoint Security auch Informationen über die Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

   - Wenn Sie das automatische Löschen ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit über n Tag(en)**.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, speichert Kaspersky Endpoint Security unbefristet. Nach 30 Tagen löscht Kaspersky Endpoint Security nur Informationen über jene Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie das automatische Löschen von Informationen zu nicht verwendeten Programmen in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz → Programm-Überwachung**.

5. Führen Sie im Block **Verarbeitungsregeln für Programme** eine der folgenden Aktionen aus:

   - Wenn Sie das automatische Löschen konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit (Tagen, 1 bis 90)** und geben Sie die Anzahl der Tage ein.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, werden von Kaspersky Endpoint Security nach dem festgelegten Zeitraum gelöscht. Nach 30 Tagen löscht Kaspersky Endpoint Security auch Informationen über die Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

   - Wenn Sie das automatische Löschen ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit (Tagen, 1 bis 90)**.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, speichert Kaspersky Endpoint Security unbefristet. Nach 30 Tagen löscht Kaspersky Endpoint Security nur Informationen über jene Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie das automatische Löschen von Informationen zu nicht verwendeten Programmen in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz → Programm-Überwachung** aus.

3. Führen Sie im Block **Verarbeitungsregeln für Programme** eine der folgenden Aktionen aus:

   - Wenn Sie das automatische Löschen konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit über n Tagen** und geben Sie die Anzahl der Tage ein.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, werden von Kaspersky Endpoint Security nach dem festgelegten Zeitraum gelöscht. Nach 30 Tagen löscht Kaspersky Endpoint Security auch Informationen über die Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

   - Wenn Sie das automatische Löschen ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit über n Tagen**.

     Informationen über Programme, die Sie einer Sicherheitsgruppe zugewiesen haben oder für welche Sie die Zugriffsrechte manuell angepasst haben, speichert Kaspersky Endpoint Security unbefristet. Nach 30 Tagen löscht Kaspersky Endpoint Security nur Informationen über jene Programme, für welche die Sicherheitsgruppe und die Programmrechte automatisch ermittelt wurden.

4. Speichern Sie die vorgenommenen Änderungen.

Übersicht über die Programm-Überwachung

Sie können Berichte über den Betrieb der Komponente „Programm-Überwachung“ abrufen. Die Berichte enthalten Informationen zu Vorgängen, die das Programm mit den mit Computerressourcen ausgeführt hat (erlaubt oder verboten). Die Berichte enthalten außerdem Informationen zu den Programmen, welche die jeweilige Ressource verwenden.

Um den Betrieb der „Programm-Überwachung“ zu verfolgen, müssen Sie das Erstellen von Berichten aktivieren. So können Sie z. B. die Weiterleitung von Berichten für einzelne Programme in den Einstellungen der Komponente „Programm-Überwachung“ aktivieren.

Berücksichtigen Sie bei der Konfiguration von „Programm-Überwachung“ die mögliche Netzwerkauslastung, wenn Sie Ereignisse an Kaspersky Security Center weiterleiten. Alternativ kann das Speichern von Berichten nur im lokalen Protokoll von Kaspersky Endpoint Security aktiviert werden.

Schutz des Zugriffs auf Audio und Video

Die Funktionen zum Schutz von Audiosignalen und zum Schutz des Webcam-Zugriffs werden auf Arm-basierten Computern nicht unterstützt.

Cyberkriminelle können mithilfe spezieller Programme versuchen, auf Geräte zuzugreifen, die Audio und Video aufzeichnen (z. B. Mikrofone und Webcams). Kaspersky Endpoint Security steuert, wann ein Programm einen Audio- oder Videostream empfangen darf, und schützt Daten vor unbefugtem Abfangen.

Kaspersky Endpoint Security erlaubt standardmäßig den Empfang von Audio- und Videostreams nur für Programme aus der Gruppe *Vertrauenswürdig*. Die Anwendungen aus den Gruppen *Schwach beschränkt*, *Stark beschränkt* und *Nicht vertrauenswürdig* sind nicht berechtigt, Audiostreams und Videostreams von Geräten zu empfangen. Es ist möglich, Programmen manuell zu erlauben, den Audio- und Videostream zu empfangen.

Besondere Funktionen zum Schutz des Audiostreams

Die Funktionalität zum Schutz des Audiostreams besitzt folgende Besonderheiten:

- Damit die Funktionalität einwandfrei funktioniert, muss die Komponente „Programm-Überwachung“ aktiviert sein.
- Hat ein Programm bereits begonnen, ein Audiosignal zu empfangen, bevor die Komponente „Programm-Überwachung“ gestartet wurde, so erlaubt Kaspersky Endpoint Security dem Programm den Empfang des Audiosignals und zeigt keine Benachrichtigungen an.
- Wenn Sie ein Programm in die Gruppe *Nicht vertrauenswürdig* oder *Stark beschränkt* verschoben haben, nachdem das Programm bereits begonnen hat, ein Audiosignal zu empfangen, so erlaubt Kaspersky Endpoint Security dem Programm den Empfang des Audiosignals und zeigt keine Benachrichtigungen an.

- Nachdem die Einstellungen für den Zugriff eines Programms auf Tonaufnahmegeräte geändert werden (wenn z. B. einem Programm verboten wird, den Audiostream zu empfangen), muss dieses Programm neu gestartet werden, damit es keinen Audiostream mehr empfängt.

- Die Kontrolle für den Empfang des Audiosignals von Tonaufnahmegeräten ist nicht von den Einstellungen für den Webcam-Schutz abhängig.

- Kaspersky Endpoint Security schützt nur den Zugriff auf integrierte und externe Mikrofone. Andere Tonübertragungsgeräte werden nicht unterstützt.

- Für Audiosignale, die von Geräten wie DSLR-Kameras, tragbaren Videokameras und Action-Cams übertragen werden, kann das Programm Kaspersky Endpoint Security keinen Schutz garantieren.

- Wenn Kaspersky Endpoint Security nach der Installation zum ersten Mal gestartet wird, kann es vorkommen, dass die Wiedergabe oder Aufzeichnung von Audio- und Videodaten in entsprechenden Programmen abgebrochen wird. Dies ist erforderlich, um die Überwachung des Zugriffs von Programmen auf Tonaufnahmegeräte zu aktivieren. Der Systemdienst für die Verwaltung von Audiogeräten wird beim ersten Start des Programms Kaspersky Endpoint Security neu gestartet.

Besondere Funktionen zum Schutz des Zugriffs von Programmen auf die Webcam

Die Funktionalität für den Webcam-Schutz besitzt folgende Besonderheiten und Einschränkungen:

- Das Programm kontrolliert Videos und statische Bilder, die auf Webcam-Daten basieren.

- Das Programm kontrolliert Audiosignale, wenn diese zu einem Videostream der Webcam gehören.

- Das Programm kontrolliert nur Webcams, die über eine USB- oder IEEE1394-Schnittstelle angeschlossen und im Microsoft-Geräte-Manager als Bildverarbeitungsgerät (Imaging Device) angezeigt werden.

- Kaspersky Endpoint Security unterstützt folgende Webcams:

  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  Kaspersky garantiert nicht, dass Webcams, die nicht in dieser Liste genannt sind, unterstützt werden.

Schutz vor modifizierten USB-Geräten

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.

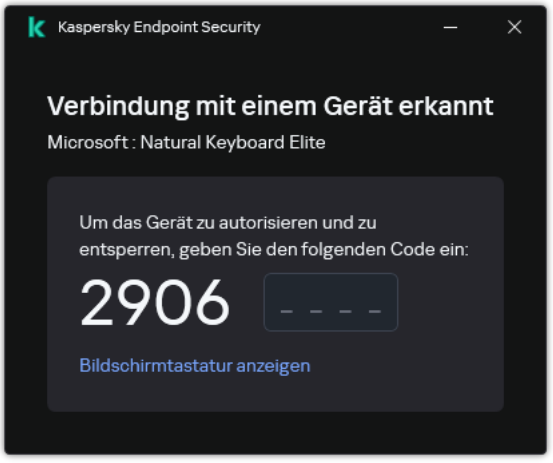
Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (sofern verfügbar) einen vom Programm generierten Code einzugeben (siehe folgende Abbildung). Dieser Vorgang 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.

Wurde der digitale Code falsch eingegeben, so generiert das Programm einen neuen Code. 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.



Autorisierung der Tastatur

Schutz vor modifizierten USB-Geräten aktivieren und deaktivieren

USB-Geräte, die vom Betriebssystem als Tastatur erkannt wurden und vor der Installation der Komponente „Schutz vor modifizierten USB-Geräten“ an den Computer angeschlossen wurden, werden nach der Installation der Komponente als autorisiert betrachtet.

So aktivieren und deaktivieren Sie die Komponente „Schutz vor modifizierten USB-Geräten“ (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor BadUSB-Angriffen** aus.
4. Verwenden Sie das Kontrollkästchen **Schutz vor BadUSB-Angriffen**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Passen Sie im Block **Autorisierung von USB-Geräten beim Anschließen** die Sicherheitseinstellungen für die Eingabe des Autorisierungscodes an:
   - **Maximale Anzahl der Autorisierungsversuche für USB-Geräte**. Automatisches Blockieren des USB-Gerätes, wenn der Autorisierungscode zu oft falsch eingegeben wird. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise fünf Eingabeversuche für den Autorisierungscode erlauben, sperrt das Programm das USB-Gerät nach dem fünften erfolglosen Versuch. Kaspersky Endpoint Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben.
   - **Timeout, wenn maximale Anzahl der Versuche erreicht wird (Minuten)**. Dauer, für die das USB-Gerät gesperrt wird, nachdem die festgelegte Anzahl erfolgloser Eingabeversuche für den Autorisierungscode erreicht wurde. Mögliche Werte: 1 bis 180 (Minuten).
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Schutz vor modifizierten USB-Geräten“ (in der Web Console und der Cloud Console)

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz → Schutz vor BadUSB-Angriffen**.
5. Verwenden Sie den Schalter **Schutz vor BadUSB-Angriffen AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Passen Sie im Block **Autorisierung von USB-Geräten** die Sicherheitseinstellungen für die Eingabe des Autorisierungscodes an:

   - **Maximale Anzahl der Autorisierungsversuche für USB-Geräte**. Automatisches Blockieren des USB-Gerätes, wenn der Autorisierungscode zu oft falsch eingegeben wird. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise fünf Eingabeversuche für den Autorisierungscode erlauben, sperrt das Programm das USB-Gerät nach dem fünften erfolglosen Versuch. Kaspersky Endpoint Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben.

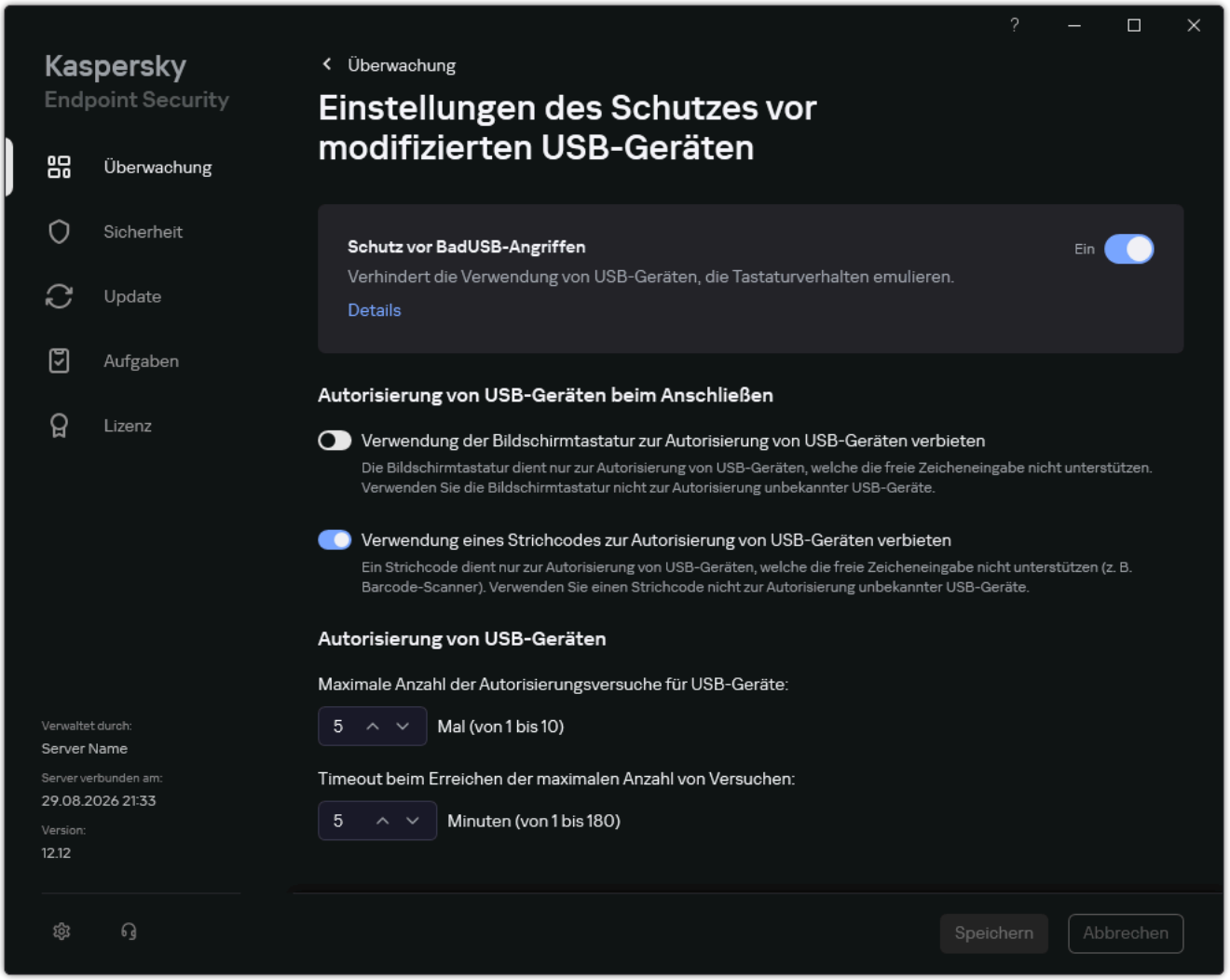
   - **Timeout beim Erreichen der maximalen Anzahl von Versuchen (Min.)**. Dauer, für die das USB-Gerät gesperrt wird, nachdem die festgelegte Anzahl erfolgloser Eingabeversuche für den Autorisierungscode erreicht wurde. Mögliche Werte: 1 bis 180 (Minuten).

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Schutz vor modifizierten USB-Geräten“ (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor BadUSB-Angriffen** aus.



Einstellungen für die Komponente „Schutz vor modifizierten USB-Geräten“

3. Verwenden Sie den Schalter **Schutz vor BadUSB-Angriffen**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Passen Sie im Block **Autorisierung von USB-Geräten beim Anschließen** die Sicherheitseinstellungen für die Eingabe des Autorisierungscodes an:

   - **Maximale Anzahl der Autorisierungsversuche für USB-Geräte**. Automatisches Blockieren des USB-Gerätes, wenn der Autorisierungscode zu oft falsch eingegeben wird. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise fünf Eingabeversuche für den Autorisierungscode erlauben, sperrt das Programm das USB-Gerät nach dem fünften erfolglosen Versuch. Kaspersky Endpoint Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben.

   - **Timeout beim Erreichen der maximalen Anzahl von Versuchen**. Dauer, für die das USB-Gerät gesperrt wird, nachdem die festgelegte Anzahl erfolgloser Eingabeversuche für den Autorisierungscode erreicht wurde. Mögliche Werte: 1 bis 180 (Minuten).

5. Speichern Sie die vorgenommenen Änderungen.

Wenn Schutz vor modifizierten USB-Geräten aktiviert ist, erfordert Kaspersky Endpoint Security daher die Autorisierung eines angeschlossenen USB-Geräts, das vom Betriebssystem als Tastatur identifiziert wird. Der Benutzer kann eine nicht autorisierte Tastatur erst verwenden, nachdem sie autorisiert wurde.

Verwenden der Bildschirmtastatur für die Autorisierung von USB-Geräten

Die Verwendung der Bildschirmtastatur ist nur für die Autorisierung von USB-Geräten vorgesehen, die die Eingabe beliebiger Zeichen nicht unterstützen (z. B. Barcode-Scanner). Es wird davon abgeraten, die Bildschirmtastatur für die Autorisierung unbekannter USB-Geräte zu verwenden.

So erlauben oder verbieten Sie die Verwendung der Bildschirmtastatur zu Autorisierungszwecken (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor BadUSB-Angriffen** aus.

4. Verwenden Sie das Kontrollkästchen **Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten**, um die Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten zu verbieten oder zuzulassen.

5. Speichern Sie die vorgenommenen Änderungen.

So erlauben oder verbieten Sie die Verwendung der Bildschirmtastatur zu Autorisierungszwecken (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz → Schutz vor BadUSB-Angriffen**.

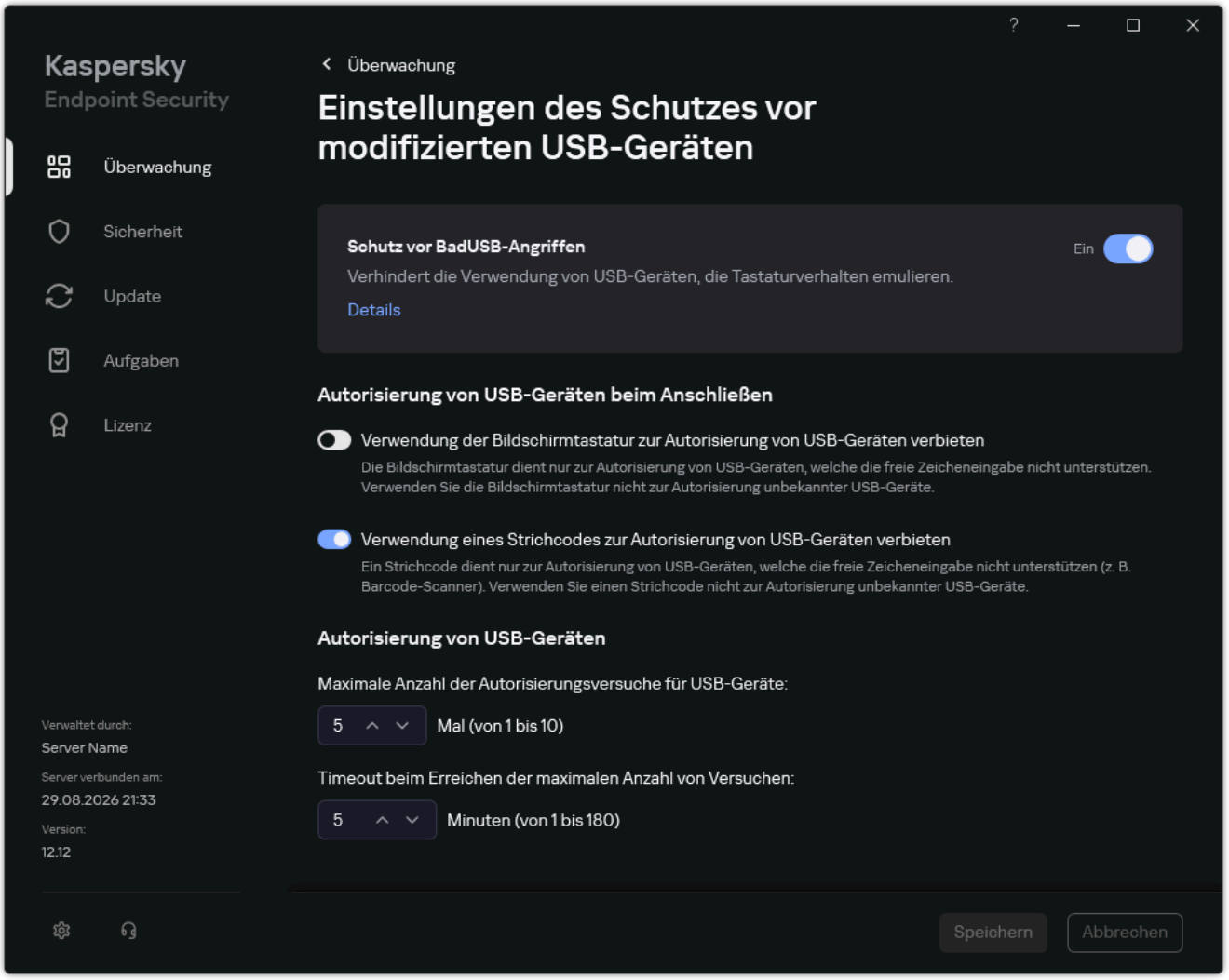
5. Verwenden Sie den Schalter **Verwendung der Bildschirmtastatur für die Autorisierung von USB-Geräten verbieten**, um die Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten zu verbieten oder zuzulassen.

6. Speichern Sie die vorgenommenen Änderungen.

So erlauben oder verbieten Sie die Verwendung der Bildschirmtastatur zu Autorisierungszwecken (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

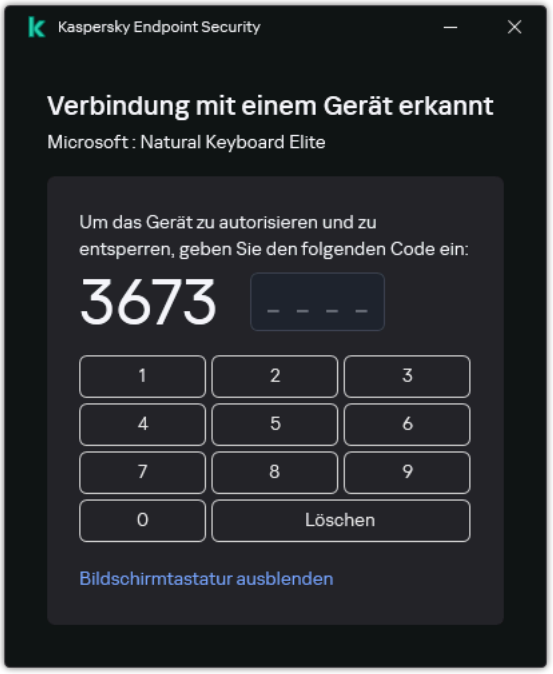
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor BadUSB-Angriffen** aus.



Einstellungen für die Komponente „Schutz vor modifizierten USB-Geräten"

3. Verwenden Sie den Schalter **Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten**, um die Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten zu verbieten oder zuzulassen.

4. Speichern Sie die vorgenommenen Änderungen.



Autorisierung von USB-Geräten

Autorisierung eines Barcode-Scanners

Wenn ein Barcode-Lesegerät an den Computer angeschlossen wird, identifiziert die Komponente „Schutz vor modifizierten USB-Geräten“ das Gerät als Eingabegerät und fordert Sie auf, das Gerät zu autorisieren. Um den Barcode-Scanner zu autorisieren, müssen Sie den Strichcode scannen, der auf dem Bildschirm angezeigt wird. Das Programm generiert einen Strichcode im Format Code39. Dieses Format wird von den meisten Barcode- und QR-Code-Scannern unterstützt.

Kaspersky Endpoint Security unterstützt noch eine weitere Autorisierungsmethode für Barcode-Scanner. Wenn Sie Geräte mit Touchscreen verwenden, können Sie über die Bildschirmtastatur einen Code eingeben. Dazu müssen Sie die Bildschirmtastatur genehmigen. Diese Methode ist beispielsweise bei stationären Barcode-Scannern praktisch, die in Kassengeräte eingebaut sind. Andere Autorisierungsmethoden für Barcode-Scanner sind nicht zulässig.

Zur Autorisierung von USB-Geräten verwendet das Programm standardmäßig keinen Strichcode.

So aktivieren Sie die Autorisierung von USB-Geräten per Strichcode (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.

3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

4. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor BadUSB-Angriffen** aus.

5. Verwenden Sie das Kontrollkästchen **Verwendung eines Strichcodes zur Autorisierung von USB-Geräten verbieten**, um die Verwendung von Strichcodes für die Autorisierung von USB-Geräten zu verbieten oder zuzulassen.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Autorisierung von USB-Geräten per Strichcode (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

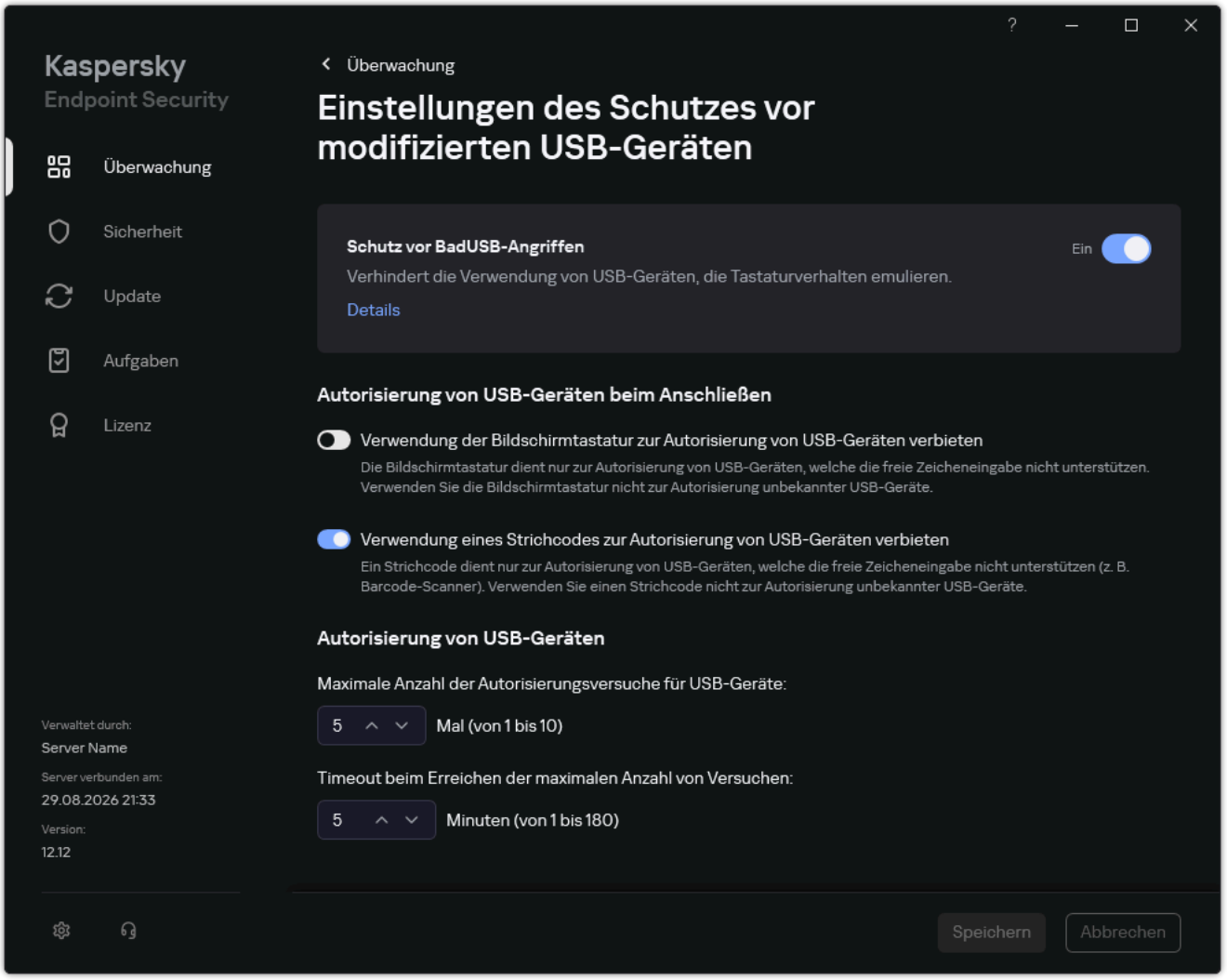
4. Gehen Sie zu **Host-Schutz** → **Schutz vor BadUSB-Angriffen**.

5. Verwenden Sie den Schalter **Verwendung eines Strichcodes für die Autorisierung von USB-Geräten verbieten**, um die Verwendung von Strichcodes zur Autorisierung von USB-Geräten zu verbieten oder zuzulassen.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

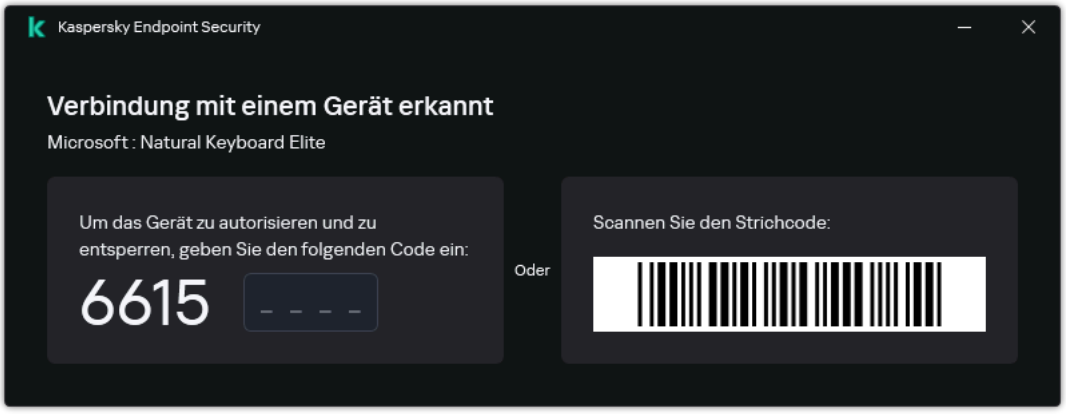
So aktivieren Sie die Autorisierung von USB-Geräten per Strichcode (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor BadUSB-Angriffen** aus.



Einstellungen für die Komponente „Schutz vor modifizierten USB-Geräten"

3. Verwenden Sie den Schalter **Verwendung eines Strichcodes zur Autorisierung von USB-Geräten verbieten**, um die Verwendung von Strichcodes zur Autorisierung von USB-Geräten zu verbieten oder zuzulassen.
4. Speichern Sie die vorgenommenen Änderungen.

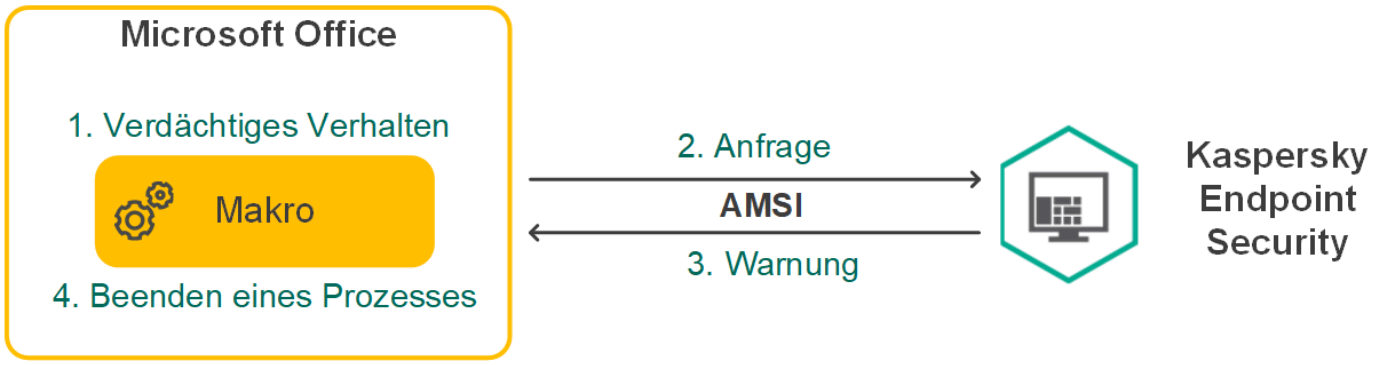


Autorisierung eines Barcode-Scanners

AMSI-Schutz

Die Komponente "AMSI-Schutz" dient der Unterstützung des Antimalware Scan Interface von Microsoft. Mithilfe *Schnittstelle für Antimalware Scan Interface (AMSI)* können Dritthersteller-Anwendungen, die AMSI unterstützen, Objekte (z. B. PowerShell-Skripte) für eine zusätzliche Untersuchung an Kaspersky Endpoint Security senden und Untersuchungsergebnisse für diese Objekte erhalten. Dritthersteller-Anwendungen können z. B. Microsoft-Office-Programme sein (siehe folgende Abb.). Details über die AMSI-Schnittstelle finden Sie in der Microsoft-Dokumentation.

Die Funktion von „AMSI-Schutz“ ist darauf beschränkt, eine Bedrohung zu erkennen und eine Drittanbieterprogramm über die gefundene Bedrohung zu benachrichtigen. Nachdem eine Dritthersteller-Anwendung über eine Bedrohung benachrichtigt wurde, verhindert diese die schädlichen Aktionen (z. B. beendet die Aktion).



Beispiel für die Funktionsweise von AMSI

Die Komponente „AMSI-Schutz“ kann die Anfrage eines Drittanbieterprogramms zurückweisen. Dies ist beispielsweise möglich, wenn dieses Programm die maximale Anzahl von Anfragen innerhalb des festgelegten Zeitraums erreicht hat. Kaspersky Endpoint Security sendet Informationen über die Ablehnung der Anfrage einer Dritthersteller-Anwendung an den Administrationsserver. Die Komponente „AMSI-Schutz“ weist Anfragen von Drittanbieter-Programmen nicht zurück, wenn für diese die kontinuierliche Integration mit der „AMSI-Schutz“-Komponente aktiviert ist.

„AMSI-Schutz“ ist für die folgenden Betriebssysteme für Workstations und Server verfügbar:

- Windows 10 Home / Pro / Pro für Workstations / Education / Enterprise / Enterprise Multi-Session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise Multi-Session
- Windows Server 2016 Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2019 Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (einschließlich Server Core-Modus)
- Windows Server 2025 Standard / Datacenter

AMSI-Schutz aktivieren und deaktivieren

Der AMSI-Schutz ist standardmäßig aktiviert und funktioniert im von Kaspersky empfohlenen Modus (siehe folgende Tabelle).

So aktivieren oder deaktivieren Sie den AMSI-Schutz (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **AMSI-Scanner** aus.
4. Verwenden Sie das Kontrollkästchen **AMSI-Scanner**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

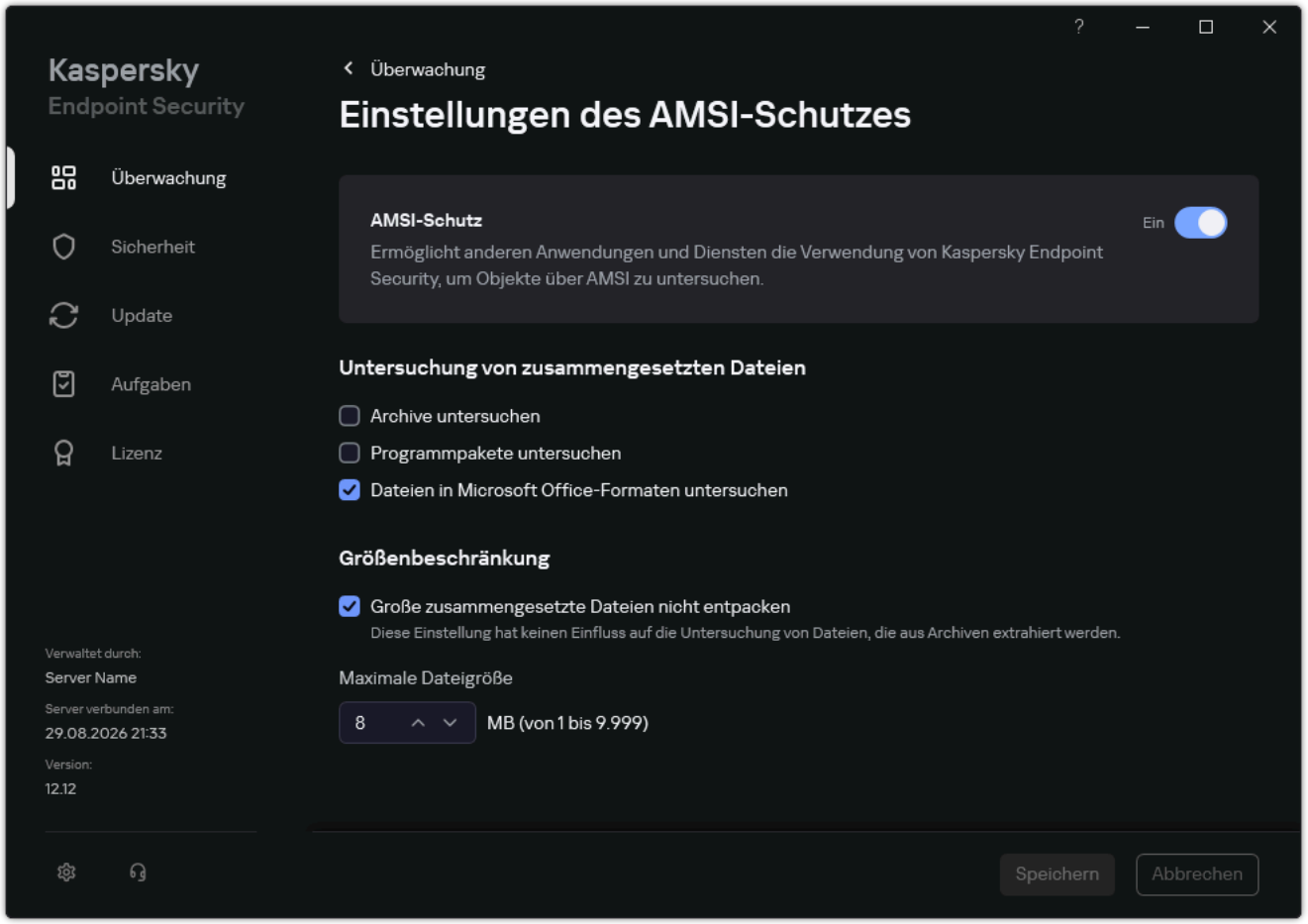
So aktivieren oder deaktivieren Sie den AMSI-Schutz (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **AMSI-Schutz**.
5. Verwenden Sie den Schalter **AMSI-Schutz AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren oder deaktivieren Sie den AMSI-Schutz (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **AMSI-Schutz** aus.



Einstellungen für den AMSI-Schutz

3. Verwenden Sie den Schalter **AMSI-Schutz**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

AMSI-Schutz-Einstellungen, die von Kaspersky-Experten empfohlen werden

Einstellung	Wert	Beschreibung
Archive untersuchen	**Aus**	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Programmpakete untersuchen	**Aus**	Verteilungspakete für Drittanbieter-Programme untersuchen.
Dateien in Microsoft Office-Formaten untersuchen	**Ein**	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Große zusammengesetzte Dateien nicht entpacken	**Maximale Dateigröße 8 MB**	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.

Dateiuntersuchung durch den AMSI-Schutz optimieren

Die Dateiuntersuchung lässt sich in folgender Hinsicht optimieren: Untersuchungsdauer verkürzen und Arbeitsgeschwindigkeit von Kaspersky Endpoint Security erhöhen. Sie können auswählen, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Verteilungspakete oder Dateien im Office-Format. Sie können auch festlegen, bis zu welcher Größe zusammengesetzte Dateien untersucht werden sollen. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Schutz“ nicht entpackt.

Eine häufige Methode, mit der Viren und andere bedrohliche Programme versteckt werden, ist die Einbettung der Schädlinge in zusammengesetzte Dateien wie beispielsweise Archive. Eine zusammengesetzte Datei muss entpackt werden, um Viren und sonstige Schadprogramme aufzuspüren, die auf diese Weise versteckt wurden. Dadurch kann die Untersuchungsgeschwindigkeit sinken. Sie können die Typen der zusammengesetzten Dateien, die untersucht werden sollen, beschränken und dadurch die Untersuchungsgeschwindigkeit erhöhen.

So optimieren Sie die Dateiuntersuchung durch den AMSI-Schutz (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **AMSI-Scanner** aus.
4. Geben Sie im Block **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Office-Format-Dateien.
5. Führen Sie im Block **Größenbeschränkung** eine der folgenden Aktionen aus:
   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie den entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Schutz“ nicht entpackt.
   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

   Die Komponente „AMSI-Schutz“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.
6. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So optimieren Sie die Dateiuntersuchung durch den AMSI-Schutz (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **AMSI-Schutz**.

5. Geben Sie im Block **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Office-Format-Dateien.

6. Führen Sie im Block **Untersuchung optimieren** eine der folgenden Aktionen aus:

   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Größenbeschränkung ist aktiviert** und geben Sie den entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Schutz“ nicht entpackt.

   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Größenbeschränkung ist aktiviert**.

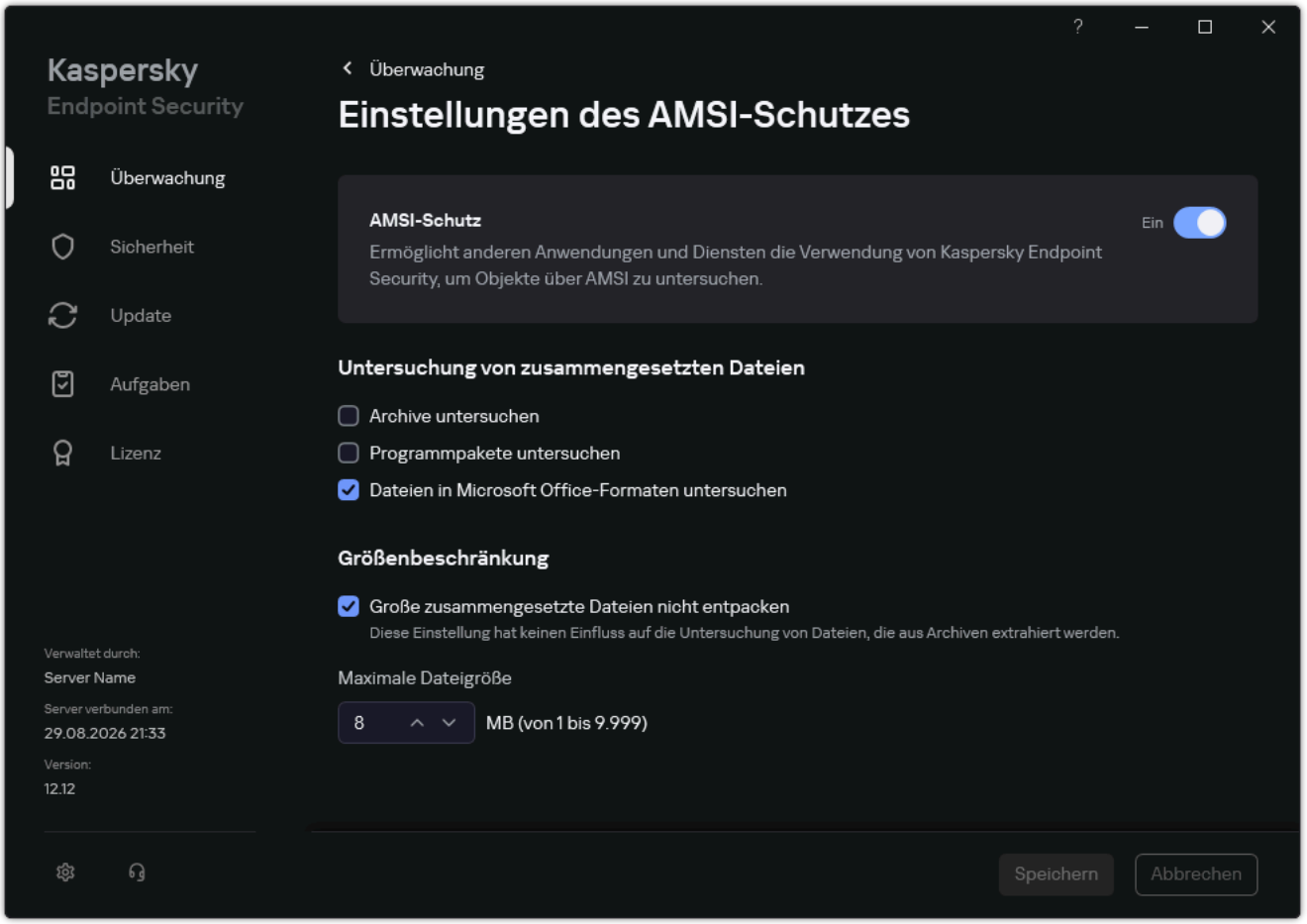
   Die Komponente „AMSI-Schutz“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Größenbeschränkung ist aktiviert** aktiviert ist.

7. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So optimieren Sie die Dateiuntersuchung durch den AMSI-Schutz (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **AMSI-Schutz** aus.



Einstellungen für den AMSI-Schutz

3. Geben Sie im Block **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Office-Format-Dateien.

4. Führen Sie im Block **Größenbeschränkung** eine der folgenden Aktionen aus:

   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie den entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Schutz“ nicht entpackt.

   - Wenn die Komponente „AMSI-Schutz“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

   Die Komponente „AMSI-Schutz“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

5. Speichern Sie die vorgenommenen Änderungen.

Schutz vor Web-Bedrohungen

Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert außerdem Verbindungen zu schädlichen Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Kaspersky Endpoint Security untersucht den HTTP-, HTTPS- und FTP-Datenverkehr. Kaspersky Endpoint Security untersucht URL- und IP-Adressen.

Um den Schutz vor Web-Bedrohungen zu verwenden, müssen Sie die Erstkonfiguration des Programms abschließen:

- Aktivieren Sie für die Kontrolle des HTTPS-Datenverkehrs die Untersuchung verschlüsselter Verbindungen (standardmäßig aktiviert).

- Wählen Sie die Ports aus, die Kaspersky Endpoint Security überwachen soll (standardmäßig überwacht das Programm alle Ports).

- Wählen Sie die Programme aus, deren Datenverkehr durch Kaspersky Endpoint Security überwacht werden soll. Die meisten Browser stehen bereits auf der Liste der von Kaspersky empfohlenen Programme. Wenn Ihr Browser nicht auf der Liste steht, fügen Sie ihn manuell hinzu.

- Wir empfehlen, ein Webseiten-Interaktionsskript in den Web-Datenverkehr einzubinden (die Skript-Injektion ist standardmäßig deaktiviert). Dieses Skript ermöglicht die Registrierung von Ereignissen des Schutzes vor Web-Bedrohungen im Ereignisprotokoll des Programms, im Ereignisprotokoll des Betriebssystems und in Berichten.

Wenn ein Benutzer versucht, eine schädliche Website oder eine Phishing-Website zu öffnen, blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an.

Schutz vor Web-Bedrohungen aktivieren und deaktivieren

Die Komponente „Schutz vor Web-Bedrohungen“ ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Für den „Schutz vor Web-Bedrohungen“ sind im Programm verschiedene Gruppen von Einstellungen (Einstellungssätze) verfügbar. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: **Hoch**, **Empfohlen**, **Niedrig**. Die Sicherheitsstufe **Empfohlen** für den Web-Datenverkehr gilt als optimal und wird von den Kaspersky-Spezialisten empfohlen (siehe Tabelle unten). Sie können eine der vordefinierten Sicherheitsstufen für den Web-Datenverkehr wählen, der mit den Protokollen HTTP und FTP empfangen oder übertragen wird, oder die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr selbstständig anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe für den Web-Datenverkehr geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Sie können die Sicherheitsstufe nur in der Verwaltungskonsole (MMC) oder der lokalen Programmoberfläche auswählen oder konfigurieren. Die Sicherheitsstufe kann nicht über die „Web Console“ oder „Cloud Console“ ausgewählt oder konfiguriert werden.

So aktivieren und deaktivieren Sie die Komponente „Schutz vor Web-Bedrohungen“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor Web-Bedrohungen** aus.
4. Verwenden Sie das Kontrollkästchen **Schutz vor Web-Bedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Wenn Sie die Komponente aktiviert haben, führen Sie im Block **Sicherheitsstufe** einen der folgenden Schritte aus:
   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:
     - **Hoch**. Auf dieser Sicherheitsstufe untersucht die Komponente „Schutz vor Web-Bedrohungen“ den Web-Datenverkehr, den ein Computer über HTTP und FTP empfängt, mit höchster Genauigkeit. Der Schutz vor Web-Bedrohungen untersucht alle Objekte des Web-Datenverkehrs ausführlich, verwendet die vollständigen Programm-Datenbanken und führt zusätzlich eine heuristische Analyse mit maximaler Tiefe aus.
     - **Empfohlen**. Diese Sicherheitsstufe bietet ein optimales Gleichgewicht zwischen der Leistung des Programms und der Sicherheit für den Web-Datenverkehr. Die Komponente „Schutz vor Web-Bedrohungen“ führt eine heuristische Analyse auf der mittleren Genauigkeitsebene aus. Diese Sicherheitsstufe für den Web-Datenverkehr wird von den Kaspersky-Experten empfohlen. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.
     - **Niedrig**. Diese Sicherheitsstufe für den Web-Datenverkehr gewährleistet maximale Geschwindigkeit bei der Untersuchung des Web-Datenverkehrs. Die Komponente „Schutz vor Web-Bedrohungen“ führt die heuristische Analyse auf der Stufe „Oberflächlich“ aus.

- Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Einstellungen** und legen Sie Ihre eigenen Komponenteneinstellungen fest (siehe Tabelle unten).

  Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen. Klicken Sie dazu auf die Schaltfläche **Standard**.

6. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn im Web-Datenverkehr ein schädliches Objekt gefunden wird:

   - **Blockieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.

   - **Informieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Komponente „Schutz vor Web-Bedrohungen“ in der Web Console

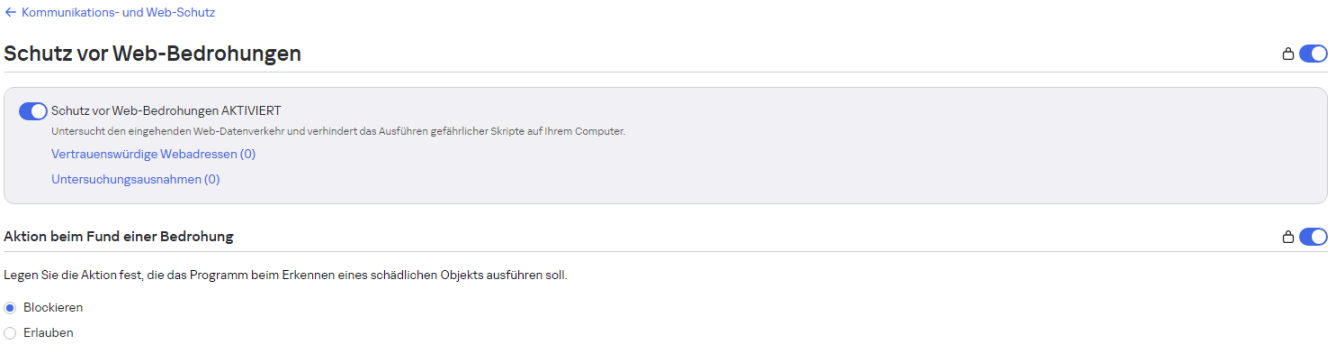
1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor Web-Bedrohungen**.



Einstellungen für den Schutz vor Web-Bedrohungen

5. Verwenden Sie den Schalter **Schutz vor Web-Bedrohungen AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn im Web-Datenverkehr ein schädliches Objekt gefunden wird:

   - **Blockieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.

   - **Erlauben, informieren oder Aktion erfragen (je nach Betriebssystem)**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.

7. Erstellen Sie bei Bedarf eine Liste mit vertrauenswürdigen Webadressen.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die Komponente „Schutz vor Web-Bedrohungen“

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Web-Bedrohungen** aus.

3. Verwenden Sie den Schalter **Schutz vor Web-Bedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Wenn Sie die Komponente aktiviert haben, führen Sie im Block **Sicherheitsstufe** einen der folgenden Schritte aus:

   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:

     - **Hoch**. Auf dieser Sicherheitsstufe untersucht die Komponente „Schutz vor Web-Bedrohungen“ den Web-Datenverkehr, den ein Computer über HTTP und FTP empfängt, mit höchster Genauigkeit. Der Schutz vor Web-Bedrohungen untersucht alle Objekte des Web-Datenverkehrs ausführlich, verwendet die vollständigen Programm-Datenbanken und führt zusätzlich eine heuristische Analyse mit maximaler Tiefe aus.

     - **Empfohlen**. Diese Sicherheitsstufe bietet ein optimales Gleichgewicht zwischen der Leistung des Programms und der Sicherheit für den Web-Datenverkehr. Die Komponente „Schutz vor Web-Bedrohungen“ führt eine heuristische Analyse auf der mittleren Genauigkeitsebene aus. Diese Sicherheitsstufe für den Web-Datenverkehr wird von den Kaspersky-Experten empfohlen. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.

     - **Niedrig**. Diese Sicherheitsstufe für den Web-Datenverkehr gewährleistet maximale Geschwindigkeit bei der Untersuchung des Web-Datenverkehrs. Die Komponente „Schutz vor Web-Bedrohungen“ führt die heuristische Analyse auf der Stufe „Oberflächlich“ aus.

   - Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Komponenteneinstellungen fest (siehe Tabelle unten).

     Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen. Klicken Sie dazu auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen**.

5. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security ausführen soll, wenn im Web-Datenverkehr ein schädliches Objekt gefunden wird:

   - **Blockieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen“ den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an.

   - **Informieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.

6. Speichern Sie die vorgenommenen Änderungen.

Von Kaspersky-Experten empfohlene Einstellungen zum Schutz vor Web-Bedrohungen (empfohlene Sicherheitsstufe)

Einstellung	Wert	Beschreibung
Webadresse mit der Datenbank für bösartige Webadressen untersuchen	**Ein**	Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Webadresse mit der Datenbank für Phishing-Webadressen untersuchen	**Ein**	Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Heuristische Analyse verwenden (Schutz vor Web-Bedrohungen)	**Mittel**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Heuristische Analyse verwenden (Anti-Phishing)	**Ein**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten.
Aktion beim Fund einer Bedrohung	**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.

Konfigurieren von Methoden zur Erkennung bösartiger Webadressen

Der „Schutz vor Web-Bedrohungen“ erkennt bösartige Webadressen mithilfe von Antiviren-Datenbanken, Cloud-Diensten von Kaspersky Security Network und heuristischer Analyse.

Die Methoden zur Erkennung bösartiger Webadressen können Sie nur in der Verwaltungskonsole (MMC) oder der lokalen Programmoberfläche auswählen. Die Methoden zur Erkennung bösartiger Webadressen können nicht in der „Web Console“ oder „Cloud Console“ ausgewählt werden. In der Grundeinstellung werden Webadressen anhand der Datenbank bösartiger Adressen mit der heuristischen Analyse (mittlere Stufe) überprüft.

Untersuchung mithilfe der Datenbank für bösartige Adressen

Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.

Kaspersky Endpoint Security untersucht alle Links, um zu überprüfen, ob sie in den Datenbanken für bösartige Webadressen aufgeführt sind. Die Programmeinstellungen für die Untersuchung sicherer Verbindungen haben keinen Einfluss auf die Link-Untersuchungsfunktion. Mit anderen Worten: Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, untersucht Kaspersky Endpoint Security die Links anhand der Datenbanken für bösartige Webadressen, selbst wenn der Netzwerkverkehr über eine verschlüsselte Verbindung übertragen wird.

So aktivieren oder deaktivieren Sie die Webadressen-Untersuchung anhand der Datenbank für bösartige Webadressen über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Web-Bedrohungen** aus.
4. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Aktivieren oder deaktivieren Sie im Block **Untersuchungsmethoden** das Kontrollkästchen **Webadresse mit der Datenbank für bösartige Webadressen untersuchen**, um die Untersuchung von Adressen anhand der Datenbank für bösartige Webadressen zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Webadressen-Untersuchung anhand der Datenbank für bösartige Adressen über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Web-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Wählen oder löschen Sie im Block **Untersuchungsmethoden** das Kontrollkästchen **Webadresse mit der Datenbank für bösartige Webadressen untersuchen**, um die Untersuchung von Adressen anhand der Datenbank für bösartige Webadressen zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

Heuristische Analyse

Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Programme im Betriebssystem zeigen. Die heuristische Analyse kann Bedrohungen erkennen, über die noch keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.

Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.

So aktivieren oder deaktivieren Sie die heuristische Analyse über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Web-Bedrohungen** aus.
4. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Aktivieren Sie im folgenden Fenster im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse verwenden**, wenn das Programm bei der Untersuchung des Web-Datenverkehrs auf Viren und andere Schadsoftware die heuristische Analyse verwenden soll.
6. Legen Sie mit dem Schieberegler die Ebene der heuristischen Analyse fest: **oberflächliche Stufe**, **mittlere Stufe** oder **tiefe Stufe**.

   Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die heuristische Analyse über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Web-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Aktivieren Sie im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse verwenden**, wenn das Programm beim Untersuchen des Web-Datenverkehrs auf Viren und andere Schadsoftware eine heuristische Analyse verwenden soll.

   Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
5. Speichern Sie die vorgenommenen Änderungen.

Anti-Phishing

Der „Schutz vor Web-Bedrohungen“ untersucht Links, um festzustellen, ob sie zu Phishing-Webadressen gehören. Dadurch können *Phishing-Angriffe* verhindert werden. Ein häufiges Beispiel für Phishing-Angriffe ist eine E-Mail-Nachricht, die scheinbar von Ihrer Bank stammt und einen Link zur offiziellen Website der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Website, die eine exakte Kopie der Bankseite darstellt und für die im Browser sogar deren Webadresse angezeigt wird, obwohl Sie sich in Wirklichkeit auf einer fiktiven Website befinden. Alle Aktionen, die Sie auf dieser Website ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Phishing-Links können sich nicht nur in E-Mail-Nachrichten befinden, sondern beispielsweise auch in Messengern. Darum überwacht die Komponente „Schutz vor Web-Bedrohungen“ alle Versuche zum Öffnen einer Phishing-Website auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Websites. Listen mit Phishing-Webadressen gehören zum Lieferumfang von Kaspersky Endpoint Security.

Sie können „Anti-Phishing“ nur in der Verwaltungskonsole (MMC) oder auf der lokalen Programmoberfläche konfigurieren. „Anti-Phishing“ kann nicht in der „Web Console“ oder „Cloud Console“ konfiguriert werden. „Anti-Phishing“ ist standardmäßig mit der heuristischen Analyse aktiviert.

So aktivieren oder deaktivieren Sie „Anti-Phishing“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Web-Bedrohungen** aus.
4. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.

5. Wählen oder löschen Sie in dem sich öffnenden Fenster im Block **Anti-Phishing-Einstellungen** das Kontrollkästchen **Webadresse mit der Datenbank für Phishing-Webadressen untersuchen** zum Aktivieren oder Deaktivieren von Anti-Phishing.

   Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.

6. Aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**, damit das Programm die heuristische Analyse verwendet, wenn Webseiten auf Phishing-Links untersucht werden.

   Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Programme im Betriebssystem zeigen. Die heuristische Analyse kann Bedrohungen erkennen, über die noch keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.

   Zur Link-Untersuchung können Sie neben den Antiviren-Datenbanken und der heuristischen Analyse auch die Reputationsdatenbanken von Kaspersky Security Network nutzen.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie „Anti-Phishing“ über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Web-Bedrohungen** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Damit die Komponente „Schutz vor Web-Bedrohungen“ Links mithilfe der Datenbanken für Phishing-Webadressen untersucht, aktivieren Sie im Block **Anti-Phishing** das Kontrollkästchen **Webadresse mit der Datenbank für Phishing-Webadressen untersuchen**. Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.

5. Aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**, damit das Programm die heuristische Analyse verwendet, wenn Webseiten auf Phishing-Links untersucht werden.

   Bei der heuristischen Analyse analysiert Kaspersky Endpoint Security die Aktivität, die Programme im Betriebssystem zeigen. Die heuristische Analyse kann Bedrohungen erkennen, über die noch keine Einträge in den Datenbanken von Kaspersky Endpoint Security vorliegen.

   Zur Link-Untersuchung können Sie neben den Antiviren-Datenbanken und der heuristischen Analyse auch die Reputationsdatenbanken von Kaspersky Security Network nutzen.

6. Speichern Sie die vorgenommenen Änderungen.

Liste mit vertrauenswürdigen Webadressen erstellen

Der „Schutz vor Web-Bedrohungen“ kann nicht nur bösartige Websites und Phishing-Websites blockieren. Beispielsweise blockiert der „Schutz vor Web-Bedrohungen“ auch HTTP-Datenverkehr, der nicht den RFC-Standards entspricht. Sie können eine Liste der Webadressen anlegen, deren Inhalt Sie vertrauen. Informationen, die von vertrauenswürdigen Webadressen stammen, werden von der Komponente „Schutz vor Web-Bedrohungen“ nicht auf Viren und andere gefährliche Programme analysiert. Diese Option kann beispielsweise nützlich sein, wenn die Komponente „Schutz vor Web-Bedrohungen“ den Download einer Datei von einer Ihnen bekannten Website verhindert.

Der Begriff Webadresse bezieht sich sowohl auf eine bestimmte Webseite, als auch auf eine Website.

Hinzufügen oder Löschen einer vertrauenswürdigen Ressource über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor Web-Bedrohungen** aus.
5. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.
6. Wählen Sie im folgenden Fenster die Registerkarte **Vertrauenswürdige Webadressen** aus.
7. Aktivieren Sie das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen**.

   Ist diese Option ausgewählt, so untersucht die Komponente „Schutz vor Web-Bedrohungen“ den Inhalt von Webseiten/Websites nicht, deren Adressen auf der Liste der vertrauenswürdigen Webadressen stehen. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website.
8. Erstellen Sie eine Liste mit Adressen der Websites / Webseiten, deren Inhalt Sie vertrauen.

   Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

   Außerdem können Sie eine Liste mit vertrauenswürdigen Webadressen aus einer XML-Datei importieren.
9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie in der Web Console eine vertrauenswürdige Webadresse hinzu

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.

5. Klicken Sie im folgenden Fenster auf den Link **Webadressen**.

   Dies öffnet ein Fenster mit einer Liste vertrauenswürdiger Webadressen.

6. Erstellen Sie eine Liste mit Adressen der Websites / Webseiten, deren Inhalt Sie vertrauen.

   Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

   Außerdem können Sie eine Liste mit vertrauenswürdigen Webadressen aus einer JSON-Datei importieren.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie eine vertrauenswürdige Webadresse über die Programmoberfläche hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Web-Bedrohungen** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Aktivieren Sie das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen**.

   Ist diese Option ausgewählt, so untersucht die Komponente „Schutz vor Web-Bedrohungen“ den Inhalt von Webseiten/Websites nicht, deren Adressen auf der Liste der vertrauenswürdigen Webadressen stehen. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website.

5. Erstellen Sie eine Liste mit Adressen der Websites / Webseiten, deren Inhalt Sie vertrauen.

   Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

   Außerdem können Sie eine Liste mit vertrauenswürdigen Webadressen aus einer XML-Datei importieren.

6. Speichern Sie die vorgenommenen Änderungen.

Nun wird der Datenverkehr von vertrauenswürdigen Webadressen nicht mehr vom „Schutz vor Web-Bedrohungen“ untersucht. Der Benutzer kann eine vertrauenswürdige Website jederzeit öffnen und eine Datei von dieser Website herunterladen. Wenn Sie keinen Zugriff auf die Website erhalten, überprüfen Sie die Einstellungen der Komponenten Untersuchung verschlüsselter Verbindungen, Web-Kontrolle und Überwachung von Netzwerkports. Wenn Kaspersky Endpoint Security eine Datei, die von einer vertrauenswürdigen Website heruntergeladen wurde, als bösartig einstuft, können Sie diese Datei den Ausnahmen hinzufügen.

Außerdem können Sie eine allgemeine Liste mit Ausnahmen für verschlüsselte Verbindungen erstellen. 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.

Exportieren und importieren der Liste vertrauenswürdiger Webadressen

Sie können die Liste der vertrauenswürdigen Webadressen in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Webadressen desselben Typs hinzuzufügen. Sie können die Export-/Import-Funktion auch verwenden, um ein Backup für die Liste der vertrauenswürdigen Webadressen anzulegen oder die Liste auf einen anderen Server zu migrieren.

So exportieren und importieren Sie eine Liste vertrauenswürdiger Webadressen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Web-Bedrohungen** aus.
4. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Wählen Sie im folgenden Fenster die Registerkarte **Vertrauenswürdige Webadressen** aus.
6. So exportieren Sie eine Liste mit vertrauenswürdigen Webadressen:
   a. Wählen Sie die vertrauenswürdigen Webadressen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keine vertrauenswürdige Webadresse ausgewählt haben, exportiert Kaspersky Endpoint Security alle Webadressen.

   b. Klicken Sie auf den Link **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der vertrauenswürdigen Adressen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die gesamte Liste der vertrauenswürdigen Webadressen in die XLM-Datei.
7. So importieren Sie die Liste der vertrauenswürdigen Adressen:
   a. Klicken Sie auf den Link **Importieren**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdigen Adressen importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste vertrauenswürdiger Webadressen in die Web Console und die Cloud-Konsole

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kommunikations- und Web-Schutz → Schutz vor Web-Bedrohungen**.

5. So exportieren Sie die Liste der Ausnahmen im Block **Regelliste**:

   a. Wählen Sie die vertrauenswürdigen Webadressen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

   Kaspersky Endpoint Security exportiert die Liste der vertrauenswürdigen Webadressen in eine json-Datei im standardmäßigen Download-Ordner.

6. So importieren Sie die Ausnahmeliste im Block **Regelliste**:

   a. Klicken Sie auf die Schaltfläche → **Import**.

   Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der vertrauenswürdigen Adressen importieren möchten.

   b. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

Schutz vor E-Mail-Bedrohungen

Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. 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. Die Anwendung unterstützt POP3, SMTP, IMAP und NNTP in den folgenden E-Mail-Clients:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Um den Datenverkehr in den E-Mail-Clients Mozilla Thunderbird, MyOffice Mail und R7-Office Organizer zu untersuchen, müssen Sie ein Kaspersky-Zertifikat zum Zertifikatspeicher hinzufügen und den Speicher für eigene Zertifikate auswählen.

Der „Schutz vor E-Mail-Bedrohungen“ unterstützt keine anderen Protokolle und E-Mail-Clients.

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 bietet der „Schutz vor E-Mail-Bedrohungen“ eine Erweiterung für Microsoft Office Outlook. Mit dieser Erweiterung können Nachrichten auf der *Ebene des E-Mail-Clients* untersucht werden. Die Erweiterung für den Schutz vor E-Mail-Bedrohungen unterstützt die 32-Bit- und 64-Bit-Versionen von Outlook 2010, 2013, 2016, 2019, 2021, 2024 und 365. Auf Arm-basierten Computern unterstützt die Erweiterung für den Schutz vor E-Mail-Bedrohungen die 32-Bit- und 64-Bit-Versionen von Outlook 2016, Outlook 2021, Outlook 2024 und Outlook 365 für Arm64.

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>*.

Schutz vor E-Mail-Bedrohungen aktivieren und deaktivieren

Die Komponente „Schutz vor E-Mail-Bedrohungen“ ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Für den Schutz vor E-Mail-Bedrohungen sind im Programm verschiedene Gruppen von Einstellungen verfügbar. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: **Hoch**, **Empfohlen**, **Niedrig**. Die E-Mail-Sicherheitsstufe **Empfohlen** gilt als optimal und wird von den Kaspersky-Spezialisten empfohlen (siehe Tabelle unten). Sie können eine der vordefinierten Sicherheitsstufen für den E-Mail-Schutz wählen oder die Einstellungen einer Sicherheitsstufe anpassen. Nachdem Sie die Einstellungen einer Sicherheitsstufe für den E-Mail-Schutz geändert haben, können Sie die empfohlenen Einstellungen der Sicherheitsstufe jederzeit wiederherstellen.

Bei Verwendung des E-Mail-Clients „Mozilla Thunderbird“ werden Nachrichten, die mit dem IMAP-Protokoll übertragen werden, von der Komponente „Schutz vor E-Mail-Bedrohungen“ nicht auf Viren und andere bedrohliche Programme untersucht, falls Filter verwendet werden, die Nachrichten aus dem Ordner „Posteingang“ verschieben.

So aktivieren und deaktivieren Sie die Komponente Schutz vor E-Mail-Bedrohungen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.
4. Verwenden Sie das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.

5. Wenn Sie die Komponente aktiviert haben, führen Sie im Block **Sicherheitsstufe** einen der folgenden Schritte aus:

   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:

     - **Hoch**. Auf dieser E-Mail-Sicherheitsstufe kontrolliert die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten mit höchster Genauigkeit. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mails und führt eine tiefe heuristische Analyse durch. Die E-Mail-Sicherheitsstufe „Hoch“ wird für Umgebungen mit hohem Risiko empfohlen. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk ohne zentralisierten E-Mail-Schutz erfolgt.

     - **Empfohlen**. Diese E-Mail-Sicherheitsstufe bietet ein optimales Gleichgewicht zwischen der Leistung des Programms und der Sicherheit für E-Mails. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mail-Nachrichten und führt eine heuristische Analyse mit mittlerer Tiefe aus. Diese E-Mail-Sicherheitsstufe wird von den Kaspersky-Experten empfohlen. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.

     - **Niedrig**. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ nur eingehende E-Mail-Nachrichten, führt eine oberflächliche heuristische Analyse aus und scannt die an Nachrichten angehängten Archive nicht. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ E-Mail-Nachrichten mit maximaler Geschwindigkeit und beansprucht die Betriebssystemressourcen minimal. Die E-Mail-Sicherheitsstufe „Niedrig“ ist für die Arbeit in einer gut geschützten Umgebung geeignet. Ein Beispiel für eine solche Umgebung ist ein LAN eines Unternehmens mit zentralisiertem E-Mail-Schutz.

   - Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Einstellungen** und legen Sie Ihre eigenen Komponenteneinstellungen fest (siehe Tabelle unten).

     Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen. Klicken Sie dazu auf die Schaltfläche **Standard**.

6. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security mit schädlichen Objekten ausführen soll:

   - **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 Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, wird das infizierte Objekt gelöscht. Das Programm fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

   - **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. 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.

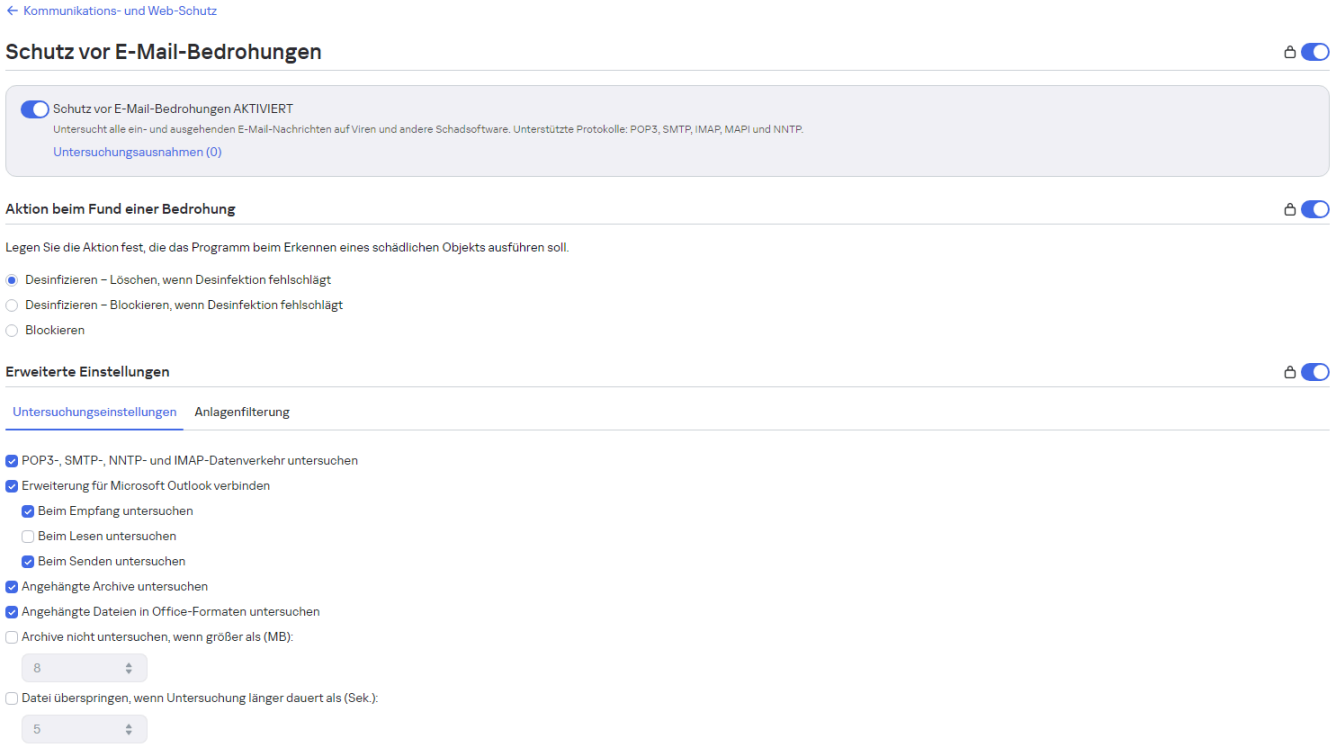
   - **Blockieren**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, blockiert das Programm das Senden der Nachricht und der Mail-Client meldet einen Fehler.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die Komponente „Schutz vor E-Mail-Bedrohungen“ in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor E-Mail-Bedrohungen**.



Einstellungen für den Schutz vor E-Mail-Bedrohungen

5. Verwenden Sie den Schalter **Schutz vor E-Mail-Bedrohungen AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security mit schädlichen Objekten ausführen soll:

   - **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 Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, wird das infizierte Objekt gelöscht. Das Programm fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

   - **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. 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**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, blockiert das Programm das Senden der Nachricht und der Mail-Client meldet einen Fehler.

7. Bearbeiten Sie bei Bedarf die erweiterten Einstellungen des Schutzes vor E-Mail-Bedrohungen.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die Komponente Schutz vor E-Mail-Bedrohungen in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.

3. Verwenden Sie den Schalter **Schutz vor E-Mail-Bedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Wenn Sie die Komponente aktiviert haben, führen Sie im Block **Sicherheitsstufe** einen der folgenden Schritte aus:

   - Um eine der vordefinierten Sicherheitsstufen zu übernehmen, verwenden Sie den Schieberegler:

     - **Hoch**. Auf dieser E-Mail-Sicherheitsstufe kontrolliert die Komponente „Schutz vor E-Mail-Bedrohungen" die Nachrichten mit höchster Genauigkeit. Die Komponente „Schutz vor E-Mail-Bedrohungen" untersucht ein- und ausgehende E-Mails und führt eine tiefe heuristische Analyse durch. Die E-Mail-Sicherheitsstufe „Hoch" wird für Umgebungen mit hohem Risiko empfohlen. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk ohne zentralisierten E-Mail-Schutz erfolgt.

     - **Empfohlen**. Diese E-Mail-Sicherheitsstufe bietet ein optimales Gleichgewicht zwischen der Leistung des Programms und der Sicherheit für E-Mails. Die Komponente „Schutz vor E-Mail-Bedrohungen" untersucht ein- und ausgehende E-Mail-Nachrichten und führt eine heuristische Analyse mit mittlerer Tiefe aus. Diese E-Mail-Sicherheitsstufe wird von den Kaspersky-Experten empfohlen. Die Werte der Einstellungen für die empfohlene Sicherheitsstufe sind in der nachstehenden Tabelle aufgeführt.

     - **Niedrig**. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen" nur eingehende E-Mail-Nachrichten, führt eine oberflächliche heuristische Analyse aus und scannt die an Nachrichten angehängten Archive nicht. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen" E-Mail-Nachrichten mit maximaler Geschwindigkeit und beansprucht die Betriebssystemressourcen minimal. Die E-Mail-Sicherheitsstufe „Niedrig" ist für die Arbeit in einer gut geschützten Umgebung geeignet. Ein Beispiel für eine solche Umgebung ist ein LAN eines Unternehmens mit zentralisiertem E-Mail-Schutz.

   - Wenn Sie eine benutzerdefinierte Sicherheitsstufe konfigurieren möchten, klicken Sie auf **Erweiterte Einstellungen** und legen Sie Ihre eigenen Komponenteneinstellungen fest (siehe Tabelle unten).

     Sie können die Werte der voreingestellten Sicherheitsstufen wiederherstellen. Klicken Sie dazu auf die Schaltfläche **Empfohlene Sicherheitsstufe wiederherstellen**.

5. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Aktion aus, die Kaspersky Endpoint Security mit schädlichen Objekten ausführen soll:

   - **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 Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, wird das infizierte Objekt gelöscht. Das Programm fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

   - **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. 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**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, blockiert das Programm das Senden der Nachricht und der Mail-Client meldet einen Fehler.

6. Speichern Sie die vorgenommenen Änderungen.

Von Kaspersky-Experten empfohlene Einstellungen zum Schutz vor E-Mail-Bedrohungen (empfohlene Sicherheitsstufe)

Einstellung	Wert	Beschreibung
Schutzbereich	**Eingehende und ausgehende Nachrichten**	Der *Schutzbereich* umfasst die Objekte, welche die Komponente während ihrer Ausführung untersucht: ein- und ausgehende Nachrichten oder nur eingehende Nachrichten. Um den Schutz Ihrer Computer sicherzustellen, müssen Sie nur die eingehenden Nachrichten untersuchen. Die Untersuchung ausgehender Nachrichten kann aktiviert werden, um zu verhindern, dass infizierte Dateien in Form von Archiven versendet werden. Außerdem kann die Untersuchung ausgehender Nachrichten aktiviert werden, um zu verhindern, dass Dateien bestimmter Formate wie Audio- und Videodateien versendet werden.
Erweiterung für Microsoft Outlook verbinden	**Ein**	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. Erfolgt die E-Mail-Untersuchung mithilfe der Erweiterung für Microsoft Outlook, so wird empfohlen, den Exchange-Cache-Modus zu verwenden (Use Cached Exchange Mode). Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.
Angehängte Archive untersuchen	**Ein**	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Angehängte Dateien in Microsoft Office-Formaten untersuchen	**Ein**	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Anlagenfilterung	**Anlagen der ausgewählten Typen umbenennen**	Wenn Sie diese Option auswählen, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Erweiterung angehängter Dateien bestimmter Typen mit einem Unterstrich (z. B. attachment.doc_). Der Benutzer muss die Datei dann zunächst umbenennen, um sie öffnen zu können.
Heuristische Analyse	**Mittel**	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Aktion beim Fund einer Bedrohung	**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 Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, wird das infizierte Objekt gelöscht. Das Programm fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

Aktion für infizierte E-Mail-Nachrichten ändern

Die Komponente „Schutz vor E-Mail-Bedrohungen“ versucht standardmäßig, alle gefundenen infizierten E-Mail-Nachrichten automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden infizierte E-Mail-Nachrichten von der Komponente „Schutz vor E-Mail-Bedrohungen“ gelöscht.

Um die Aktion für infizierte E-Mail-Nachrichten zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.

3. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** eine Aktion, die Kaspersky Endpoint Security beim Fund einer infizierten Nachricht ausführen soll:

   - **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 Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, wird das infizierte Objekt gelöscht. Das Programm fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*.

   - **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. 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**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, blockiert das Programm das Senden der Nachricht und der Mail-Client meldet einen Fehler.

4. Speichern Sie die vorgenommenen Änderungen.

Schutzbereich für die Komponente „Schutz vor E-Mail-Bedrohungen“

Schutzbereich bezieht sich auf die Objekte, die von einer Komponente während der Ausführung untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften. Der Schutzbereich für die Komponente „Schutz vor E-Mail-Bedrohungen“ wird durch folgende Eigenschaften definiert: Einstellungen für die Integration der Komponente „Schutz vor E-Mail-Bedrohungen“ in die Mail-Clients, Typ der E-Mail-Nachrichten und der E-Mail-Protokolle, deren Datenverkehr von der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht wird. Kaspersky Endpoint Security untersucht standardmäßig ein- und ausgehende E-Mail-Nachrichten sowie den Datenverkehr der Mailprotokolle POP3, SMTP, NNTP und IMAP und wird in den Mail-Client Microsoft Office Outlook integriert.

Um den Schutzbereich für die Komponente „Schutz vor E-Mail-Bedrohungen“ zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor E-Mail-Bedrohungen** aus.

3. Klicken Sie auf **Erweiterte Einstellungen**.

4. Wählen Sie im Block **Schutzbereich** die zu untersuchenden Nachrichten aus:

   - **Eingehende und ausgehende Nachrichten**.

   - **Nur eingehende Nachrichten**.

Um den Schutz Ihrer Computer sicherzustellen, müssen Sie nur die eingehenden Nachrichten untersuchen. Die Untersuchung ausgehender Nachrichten kann aktiviert werden, um zu verhindern, dass infizierte Dateien in Form von Archiven versendet werden. Außerdem kann die Untersuchung ausgehender Nachrichten aktiviert werden, um zu verhindern, dass Dateien bestimmter Formate wie Audio- und Videodateien versendet werden.

Wenn Sie nur die Untersuchung eingehender Nachrichten wählen, wird empfohlen, eine einmalige Untersuchung aller ausgehenden Nachrichten vorzunehmen, da sich auf Ihrem Computer Mail-Würmer befinden können, die sich mithilfe von E-Mails ausbreiten. Dadurch lassen sich Probleme vermeiden, die durch unkontrolliertes Versenden infizierter Nachrichten von Ihrem Computer auftreten können.

5. Gehen Sie im Block **Konnektivität** wie folgt vor:

- Aktivieren Sie das Kontrollkästchen **POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten untersucht, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden. Die Untersuchung erfolgt, bevor die Nachrichten auf dem Benutzercomputer empfangen werden.

  Deaktivieren Sie das Kontrollkästchen **POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen**, damit die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht untersucht, die mit den Protokollen POP3, SMTP, NNTP und IMAP übertragen werden, bevor die Nachrichten auf dem Benutzercomputer eintreffen. In diesem Fall werden die Nachrichten von der Erweiterung der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht, die in den Mail-Client Microsoft Office Outlook integriert ist, wenn das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden** aktiviert ist. Die Untersuchung erfolgt, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  Wenn Sie einen anderen E-Mail-Client als Microsoft Office Outlook verwenden, untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht, die über die Protokolle POP3, SMTP, NNTP und IMAP übertragen werden, wenn das Kontrollkästchen **POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen** deaktiviert ist.

- Aktivieren Sie das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden**, um den Zugriff auf die Einstellungen für die Komponente „Schutz vor E-Mail-Bedrohungen“ aus dem Programm Microsoft Office Outlook zu ermöglichen und die Untersuchung von Nachrichten zu aktivieren, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Diese Untersuchung erfolgt mithilfe der Erweiterung, die in das Programm Microsoft Office Outlook integriert ist, und wird ausgeführt, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  Deaktivieren Sie das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden**, um den Zugriff auf die Einstellungen für die Komponente „Schutz vor E-Mail-Bedrohungen“ aus dem Programm Microsoft Office Outlook zu untersagen und die Untersuchung von Nachrichten zu deaktivieren, die mit den Protokollen POP3, SMTP, NNTP, IMAP und MAPI übertragen werden. Diese Option bezieht sich auf die Untersuchung mithilfe der Erweiterung, die in das Programm Microsoft Office Outlook integriert ist, und ausgeführt werden kann, nachdem die Nachrichten auf den Benutzercomputer heruntergeladen wurden.

  Die Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ wird bei der Installation von Kaspersky Endpoint Security in den Mail-Client Microsoft Office Outlook integriert.

6. Speichern Sie die vorgenommenen Änderungen.

Untersuchung zusammengesetzter Dateien, die an E-Mail-Nachrichten angehängt sind

Sie können die Untersuchung von Objekten, die an Nachrichten angehängt sind, aktivieren oder deaktivieren, und für zu untersuchende Objekte, die an Nachrichten angehängt sind, eine maximale Größe und eine maximale Untersuchungsdauer festlegen.

Um die Untersuchung von zusammengesetzten Dateien anzupassen, die an E-Mail-Nachrichten angehängt sind, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Konfigurieren Sie im Block **Untersuchung von zusammengesetzten Dateien** die Untersuchungseinstellungen:
   - **Angehängte Dateien in Microsoft Office-Formaten untersuchen**. Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
   - **Angehängte Archive untersuchen**. Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).

     Falls das Programm während der Untersuchung im Nachrichtentext ein Kennwort für ein Archiv findet, wird dieses Kennwort verwendet, um den Inhalt des Archivs auf Schadsoftware zu untersuchen. Das Kennwort wird in diesem Fall nicht gespeichert. Ein Archiv wird während der Untersuchung entpackt. Wenn während des Entpackungsvorgangs ein Anwendungsfehler auftritt, können Sie die unter dem folgenden Pfad gespeicherten entpackten Dateien manuell löschen: %systemroot%\temp. Diese Dateien besitzen das Präfix PR.

   - **Archive nicht untersuchen, wenn größer als n MB (von 1 bis 9.999)**. Ist das Kontrollkästchen aktiviert, so schließt die Komponente „Schutz vor E-Mail-Bedrohungen“ die Archive, die an E-Mail-Nachrichten angehängt sind, von der Untersuchung aus, falls sie die festgelegte Größe überschreiten. Ist das Kontrollkästchen deaktiviert, so untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die an E-Mail-Nachrichten angehängten Archive unabhängig von deren Größe.
   - **Untersuchungsdauer für Archive beschränken auf n Sek. (von 1 bis 9.999)**. Wenn dieses Kontrollkästchen aktiviert ist, wird die Untersuchungsdauer für Archive, die an E-Mail-Nachrichten angehängt sind, auf die festgelegte Dauer beschränkt.
5. Speichern Sie die vorgenommenen Änderungen.

Filterung von E-Mail-Anlagen

Die Anlagenfilterung funktioniert nicht für ausgehende E-Mail-Nachrichten.

Schädliche Programme können sich in Form von den Anlagen für E-Mail-Nachrichten verbreiten. Sie können eine Filterung nach dem Typ der Nachrichtenanhänge einrichten, damit Dateien der festgelegten Typen automatisch umbenannt oder gelöscht werden. Durch das Umbenennen bestimmter Typen kann Kaspersky Endpoint Security Ihren Computer vor dem automatischen Start von schädlichen Programmen schützen.

Gehen Sie folgendermaßen vor, um die Anlagenfilterung anzupassen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.
3. Klicken Sie auf **Erweiterte Einstellungen**.
4. Führen Sie im Block **Anlagenfilterung** eine der folgenden Aktionen aus:
   - **Filterung deaktivieren**. Bei Auswahl dieser Variante werden Dateien, die an E-Mail-Nachrichten angehängt sind, von der Komponente „Schutz vor E-Mail-Bedrohungen“ nicht gefiltert.
   - **Anlagen der ausgewählten Typen umbenennen**. Wenn Sie diese Option auswählen, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Erweiterung angehängter Dateien bestimmter Typen mit einem Unterstrich (z. B. attachment.doc_). Der Benutzer muss die Datei dann zunächst umbenennen, um sie öffnen zu können.
   - **Anlagen der ausgewählten Typen löschen**. Bei Auswahl dieser Variante löscht die Komponente „Schutz vor E-Mail-Bedrohungen“ aus E-Mail-Nachrichten die angehängten Dateien der angegebenen Typen.
5. Wenn Sie beim vorherigen Schritt der Anleitung die Variante **Anlagen der ausgewählten Typen umbenennen** oder die Variante **Anlagen der ausgewählten Typen löschen** gewählt haben, aktivieren Sie die Kontrollkästchen für die erforderlichen Dateitypen.
6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Erweiterungen für die Anlagenfilterung

Sie können die Liste der Erweiterungen für Anlagenfilterung in eine XML-Datei exportieren. Mit der Export-/Importfunktion können Sie ein Backup für die Liste der Regeln der Erweiterungen anlegen oder die Liste auf einen anderen Server migrieren.

So exportieren und importieren Sie eine Liste von Erweiterungen der Anlagenfilterung in der Verwaltungskonsole (MMC)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor E-Mail-Bedrohungen**.
5. So exportieren Sie die Liste der Erweiterungen im Block **Anlagenfilterung**:

   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten.

   b. Klicken Sie auf den Link **Export**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Erweiterungen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.
6. So importieren Sie die Liste der Erweiterungen im Block **Anlagenfilterung**:

   a. Klicken Sie auf den Link **Import**.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Erweiterungen möchten.

   c. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit Erweiterungen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.
4. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Anlagenfilterung**-Registerkarte aus.
6. So exportieren Sie die Liste der Erweiterungen:

   a. Wählen Sie die Erweiterungen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

   b. Klicken Sie auf den Link **Export**.

c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Erweiterungen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

d. Speichern Sie die Datei.

Kaspersky Endpoint Security exportiert die gesamte Liste der Erweiterungen in die XLM-Datei.

7. So importieren Sie die Liste der Erweiterungen:

a. Klicken Sie auf den Link **Import**.

b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Erweiterungen möchten.

c. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Erweiterungen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

E-Mail-Untersuchung in Microsoft Office Outlook

Bei der Installation von Kaspersky Endpoint Security wird eine Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ in das Programm Microsoft Office Outlook (im Folgenden „Outlook“ genannt) integriert. Die Erweiterung ermöglicht die Untersuchung von Nachrichten auf der Ebene eines E-Mail-Clients statt auf Protokollebene. Zusätzlich zu Nachrichten können Sie mit der Erweiterung auch Objekte untersuchen, die über die MAPI-Schnittstelle von Microsoft Exchange-Repositorys empfangen werden (z. B. Objekte im Kalender). Diese Untersuchung erfolgt im Mail-Client.

Sie können aus Outlook zu den Einstellungen der Komponente „Schutz vor E-Mail-Bedrohungen“ wechseln und festlegen, zu welchem Zeitpunkt E-Mail-Nachrichten auf Viren und andere bedrohliche Programme untersucht werden sollen.

Die Erweiterung für den Schutz vor E-Mail-Bedrohungen unterstützt die 32-Bit- und 64-Bit-Versionen von Outlook 2010, 2013, 2016, 2019, 2021, 2024 und 365.

Auf Arm-basierten Computern unterstützt die Erweiterung für den Schutz vor E-Mail-Bedrohungen die 32-Bit- und 64-Bit-Versionen von Outlook 2016, Outlook 2021, Outlook 2024 und Outlook 365 für Arm64.

In Outlook werden eingehende E-Mail-Nachrichten zuerst von der Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht (sofern auf der Programmoberfläche von Kaspersky Endpoint Security das Kontrollkästchen POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen aktiviert ist). Anschließend werden eingehende E-Mail-Nachrichten von der Outlook-Erweiterung für „Schutz vor E-Mail-Bedrohungen“ gescannt. Findet die Komponente „Schutz vor E-Mail-Bedrohungen“ in einer E-Mail-Nachricht ein schädliches Objekt, so werden Sie darüber informiert.

Die Einstellungen der Komponente „Schutz vor E-Mail-Bedrohungen“ können direkt in Outlook angepasst werden, wenn die Microsoft Outlook-Erweiterung auf der Programmoberfläche von Kaspersky Endpoint Security aktiviert ist (siehe Bild unten).



Einstellungen der Komponente „Schutz vor E-Mail-Bedrohungen“ in Outlook

Ausgehende Nachrichten werden zuerst von der Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht und anschließend von der Komponente „Schutz vor E-Mail-Bedrohungen“ gescannt.

Für die Untersuchung von E-Mails mit der Outlook-Erweiterung zum Schutz vor E-Mail-Bedrohungen wird empfohlen, den Cache-Modus von Exchange Server zu verwenden (Exchange-Cache-Modus verwenden). Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.

So konfigurieren Sie den Funktionsmodus der Outlook-Erweiterung für den Schutz vor E-Mail-Bedrohungen in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor E-Mail-Bedrohungen** aus.
5. Klicken Sie im Block **Sicherheitsstufe** auf **Einstellungen**.
6. Aktivieren Sie im angezeigten Fenster im Block **Konnektivität** das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden**.
7. Klicken Sie auf **Einstellungen**.

8. Gehen Sie Fenster **E-Mail-Schutz** wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Beim Empfang untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die eingehenden Nachrichten untersucht, wenn sie im E-Mail-Postfach eintreffen.

   - Aktivieren Sie das Kontrollkästchen **Beim Lesen untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die eingehenden Nachrichten untersucht, wenn der Benutzer sie zum Lesen öffnen möchte.

   - Aktivieren Sie das Kontrollkästchen **Beim Senden untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die ausgehenden Nachrichten beim Senden untersucht.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Funktionsmodus der Outlook-Erweiterung für den Schutz vor E-Mail-Bedrohungen in der Web Console

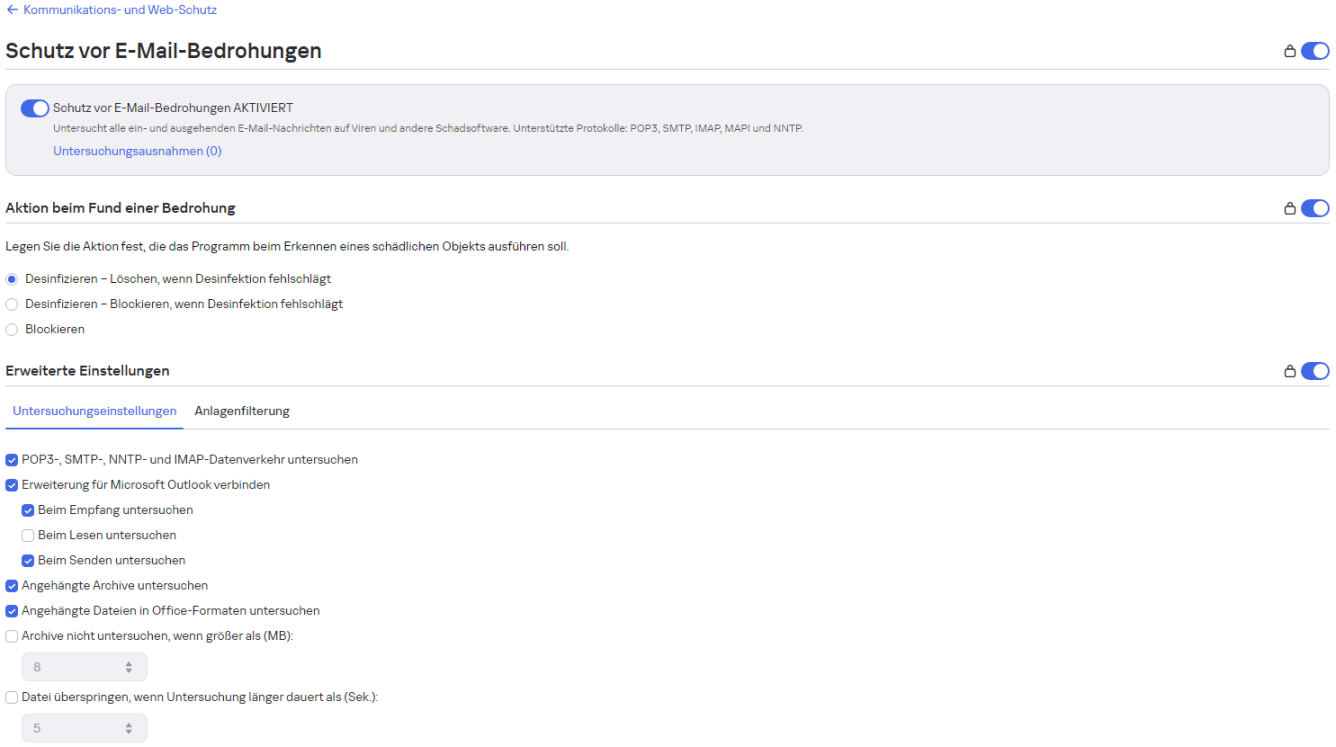
1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor E-Mail-Bedrohungen**.



Einstellungen für den Schutz vor E-Mail-Bedrohungen

5. Wählen Sie unter **Erweiterte Einstellungen** die Registerkarte **Untersuchungseinstellungen** aus.

6. Aktivieren Sie das Kontrollkästchen **Erweiterung für Microsoft Outlook verbinden**.

7. Konfigurieren Sie den Funktionsmodus der Erweiterung:

   - Aktivieren Sie das Kontrollkästchen **Beim Empfang untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die eingehenden Nachrichten untersucht, wenn sie im E-Mail-Postfach eintreffen.

   - Aktivieren Sie das Kontrollkästchen **Beim Lesen untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die eingehenden Nachrichten untersucht, wenn der Benutzer sie zum Lesen öffnen möchte.

   - Aktivieren Sie das Kontrollkästchen **Beim Senden untersuchen**, damit die Outlook-Erweiterung für die Komponente „Schutz vor E-Mail-Bedrohungen“ die ausgehenden Nachrichten beim Senden untersucht.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Untersuchung von E-Mails in Thunderbird, MyOffice, R7-Office

Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. Bei den Mail-Clients Mozilla Thunderbird, MyOffice Mail und R7-Office Organizer erhält das Programm nur auf *Protokollebene* (POP3, SMTP, IMAP, NNTP) Zugriff auf Nachrichten.

Um den Datenverkehr in den E-Mail-Clients Mozilla Thunderbird, MyOffice Mail und R7-Office Organizer zu untersuchen, müssen Sie ein Kaspersky-Zertifikat zum Zertifikatspeicher hinzufügen und den Speicher für eigene Zertifikate auswählen.

Wenn ein Mail-Client in einem Browser geöffnet ist, untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten nicht.

Echtzeitschutz vor E-Mail-Bedrohungen

Der Schutz vor E-Mail-Bedrohungen kann sowohl eingehende als auch ausgehende Nachrichten untersuchen. Die Komponente „Schutz vor E-Mail-Bedrohungen“ versucht standardmäßig, alle gefundenen infizierten E-Mail-Nachrichten automatisch zu desinfizieren. Wenn eine Desinfektion nicht möglich ist, werden infizierte E-Mail-Nachrichten von der Komponente „Schutz vor E-Mail-Bedrohungen“ gelöscht. 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>*.

Bei Verwendung des E-Mail-Clients „Mozilla Thunderbird“ werden Nachrichten, die mit dem IMAP-Protokoll übertragen werden, von der Komponente „Schutz vor E-Mail-Bedrohungen“ nicht auf Viren und andere bedrohliche Programme untersucht, falls Filter verwendet werden, die Nachrichten aus dem Ordner „Posteingang“ verschieben.

Schadsoftware-Untersuchung in E-Mail-Datenbanken

Der Schutz vor E-Mail-Bedrohungen verhindert eine Infektion des Computers auf Protokollebene. War der Computer jedoch schon infiziert, bevor Kaspersky Endpoint Security installiert wurde, kann das Programm die Bedrohung mithilfe der Aufgabe *Schadsoftware-Untersuchung* in den E-Mail-Datenbanken erkennen. Das Programm desinfiziert oder löscht infizierte Dateien in E-Mail-Datenbanken nicht, unabhängig von den Aufgabeneinstellungen. Dies liegt daran, dass Kaspersky Endpoint Security Nachrichten aus Thunderbird, MyOffice und P7-Office nicht auf dieselbe Weise in ihre Bestandteile (Kopfzeile, Nachrichtentext, Anhänge) zerlegt wie Nachrichten aus Microsoft Office Outlook. Das Programm fügt nur Informationen über erkannte Objekte zur Liste der aktiven Bedrohungen hinzu.

So beseitigen Sie aktive Bedrohungen:

1. Suchen Sie die Nachricht mit dem gefundenen Objekt über die Benutzeroberfläche des E-Mail-Clients und löschen Sie sie manuell.

   Das Programm zeigt Informationen über die erkannten Objekte in der Liste für aktive Bedrohungen an.

   Beispiel für eine Karte mit einem erkannten Objekt:

   HEUR:Trojan.PDF.Phish.gen
   Objekt: `C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. Komprimieren Sie die Datenbank.

   Wenn eine Nachricht über die Benutzeroberfläche gelöscht wird, fügt der E-Mail-Client nur eine Löschmarkierung hinzu. Der Mail-Client löscht die Nachricht erst dann tatsächlich, nachdem die Datenbank komprimiert wurde. Einzelheiten zur Datenbankkomprimierung finden Sie in der Hilfe Ihres E-Mail-Programms (z. B. Mozilla Thunderbird).

3. Führen Sie die Aufgabe *Schadsoftware-Untersuchung* erneut aus und vergewissern Sie sich, dass die Bedrohung nicht mehr vorhanden ist.

Wenn Nachrichten mit infizierten Dateien aus irgendeinem Grund momentan nicht gelöscht werden können, können Sie solche Bedrohungen in der Benutzeroberfläche von Kaspersky Endpoint Security verarbeiten. Für Dateien von E-Mail-Clients stehen Ihnen zwei Möglichkeiten zur Verarbeitung einer Bedrohung zur Verfügung: **Ignorieren** und **Zu Ausnahmen hinzufügen**. Um zu verhindern, dass das Programm diese Objekte bei einer erneuten Untersuchung zur Liste der aktiven Bedrohungen hinzufügt, fügen Sie sie zur Liste der Untersuchungsausnahmen hinzu.

Schutz vor Netzwerkbedrohungen

Die Komponente *Schutz vor Netzwerkbedrohungen* (auch Intrusion Detection System oder IDS genannt) überwacht den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe charakteristisch sind. Wenn das Programm einen Netzwerkangriff auf den Benutzercomputer erkennt, sperrt es die Netzwerkverbindung mit dem angreifenden Computer. Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Programm-Datenbanken enthalten. Die Liste der Netzwerkangriffe, die von der Komponente „Schutz vor Netzwerkbedrohungen“ erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert.

Schutz vor Netzwerkbedrohungen aktivieren und deaktivieren

Der Schutz vor Netzwerkbedrohungen ist standardmäßig aktiviert und läuft im optimalen Modus. Kaspersky Endpoint Security überwacht den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe charakteristisch sind, und blockiert die Angriffe.

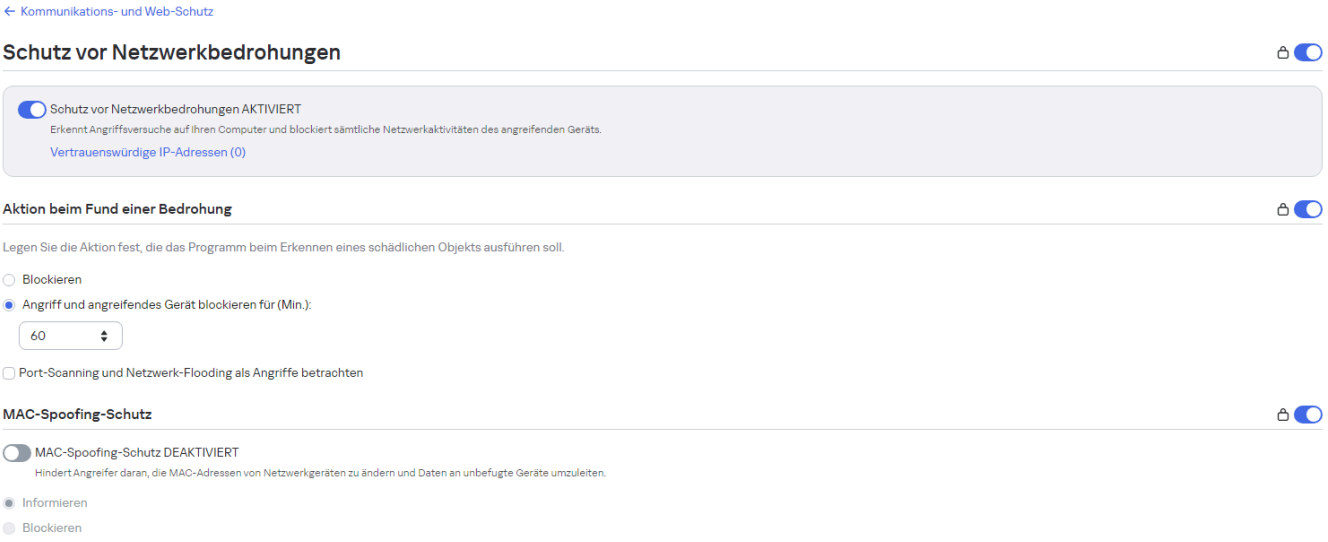
So aktivieren oder deaktivieren Sie den „Schutzes vor Netzwerkbedrohungen“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Schutz vor Netzwerkbedrohungen** aus.
4. Verwenden Sie das Kontrollkästchen **Schutz vor Netzwerkbedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Schutz vor Netzwerkbedrohungen in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Schutz vor Netzwerkbedrohungen**.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

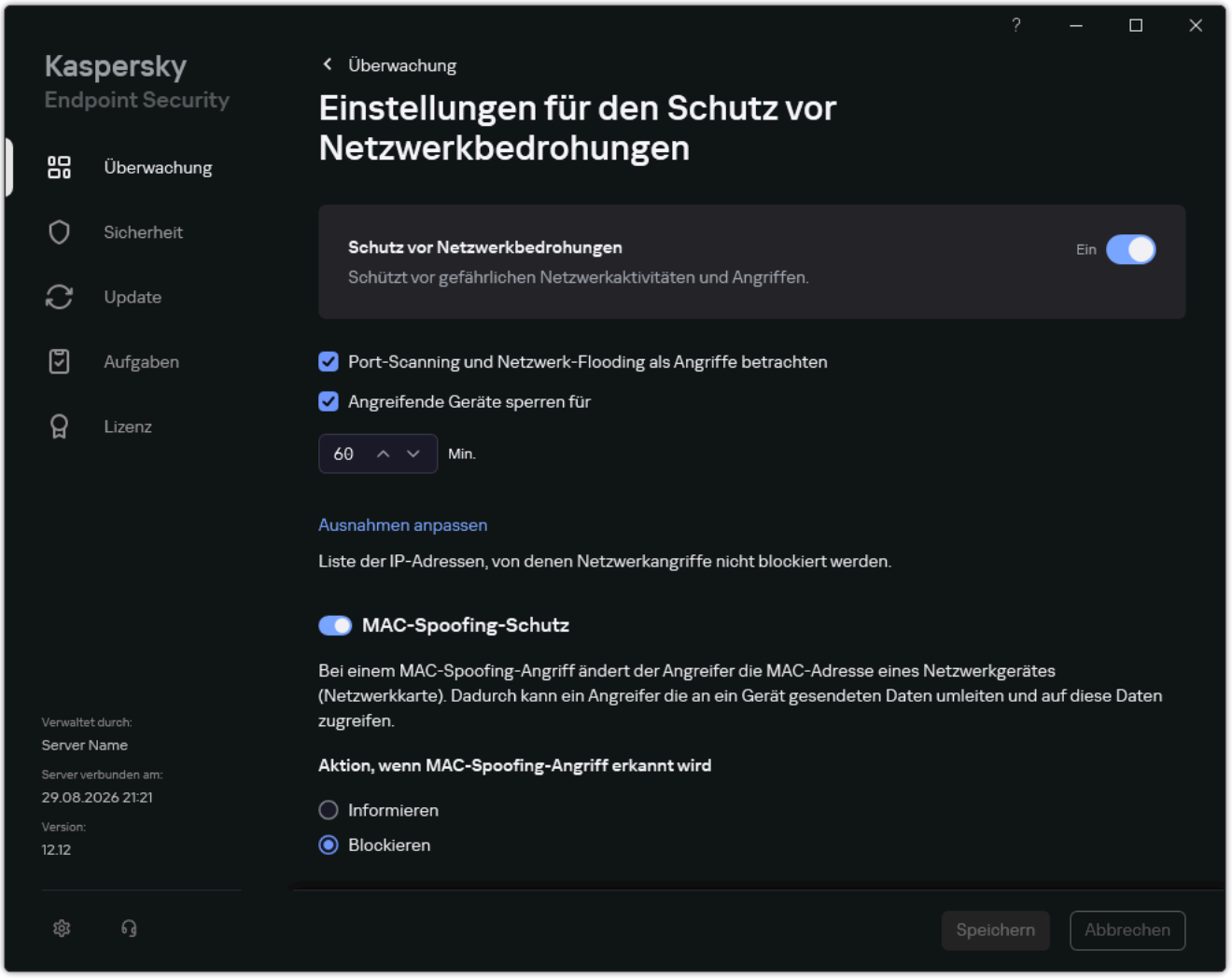
5. Verwenden Sie den Schalter **Schutz vor Netzwerkbedrohungen AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie den „Schutzes vor Netzwerkbedrohungen“ über die App-Oberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

3. Verwenden Sie den Schalter **Schutz vor Netzwerkbedrohungen**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Angreifenden Computer blockieren

Wenn die Komponente „Schutzes vor Netzwerkbedrohungen“ aktiviert ist, werden Netzwerkbedrohungen automatisch durch Kaspersky Endpoint Security blockiert. Darüber hinaus kann die App den angreifenden Computer blockieren und das Senden von Netzwerkpaketen für einen bestimmten Zeitraum einschränken. Standardmäßig blockiert Kaspersky Endpoint Security den Computer für eine Stunde.

So blockieren Sie einen angreifenden Computer über die Verwaltungskonsole (MMC)

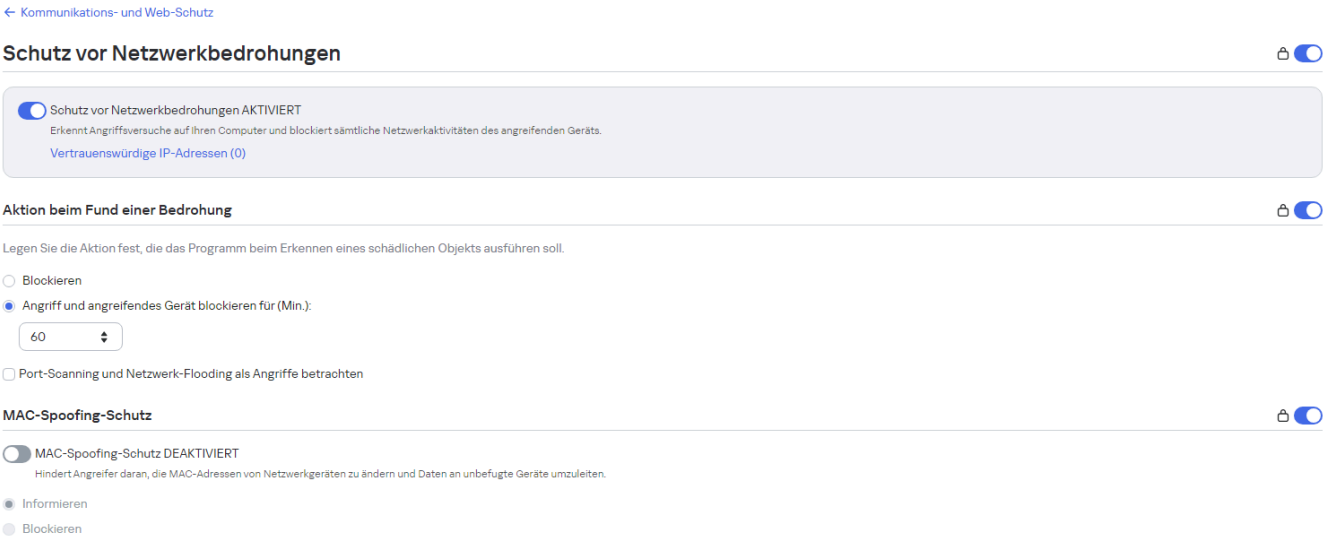
1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.
4. Aktivieren Sie unter **Einstellungen für den Schutz vor Netzwerkbedrohungen** das Kontrollkästchen **Angreifende Geräte sperren für n 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.
5. Sie können auch eine andere Sperrdauer für einen angreifenden Computer festlegen. Verwenden Sie dazu das Feld rechts neben dem Kontrollkästchen **Angreifende Geräte sperren für n Min**.
6. Speichern Sie die vorgenommenen Änderungen.

So blockieren Sie einen angreifenden Computer über die Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz → Schutz vor Netzwerkbedrohungen**.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

5. Aktivieren Sie im Block **Aktion beim Fund einer Bedrohung** das Kontrollkästchen **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.

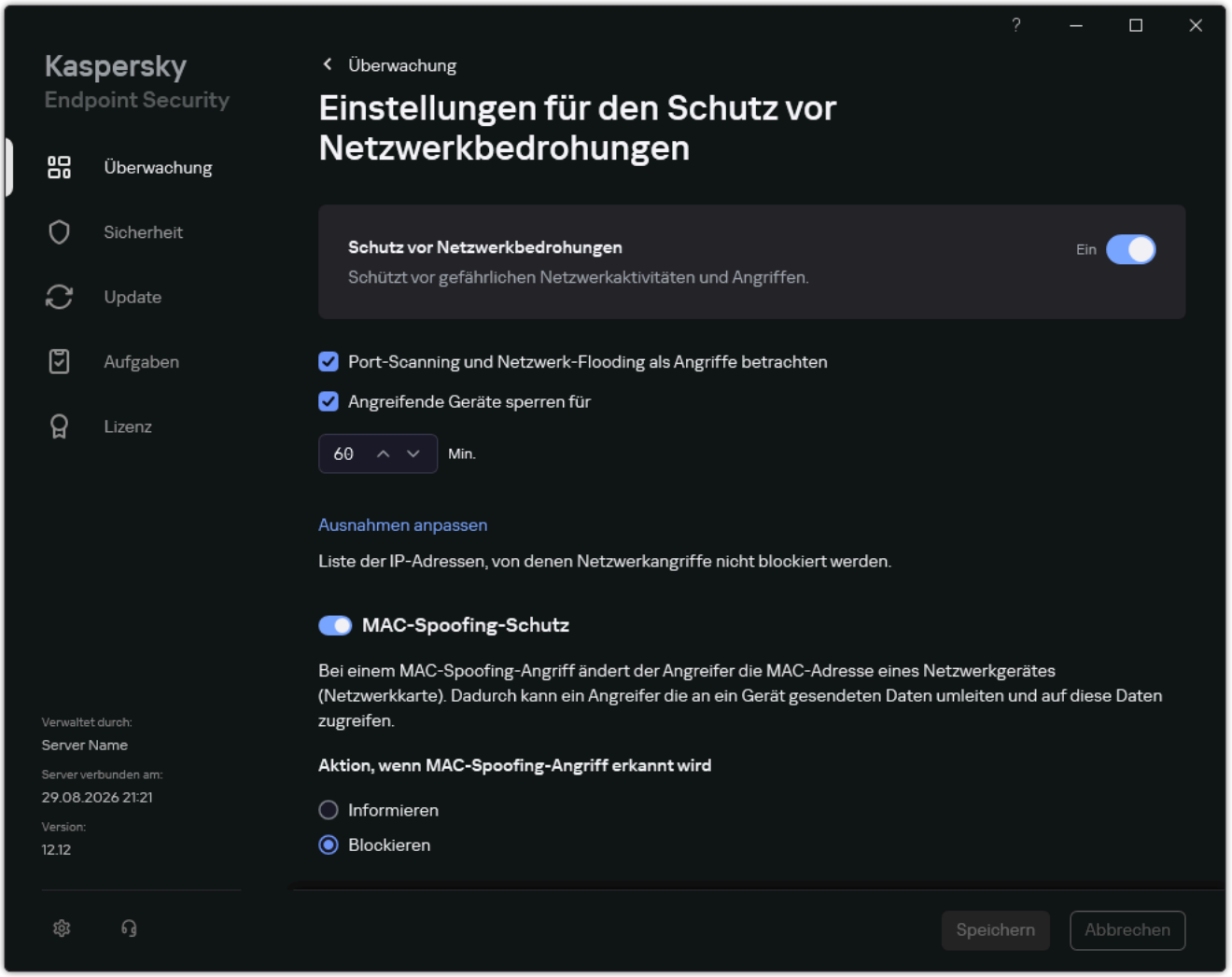
6. Ändern Sie die Dauer, für die der angreifende Computer gesperrt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

So blockieren Sie einen angreifenden Computer über die App-Oberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

3. Aktivieren Sie den Schalter **Angreifende Geräte sperren für n Min**.

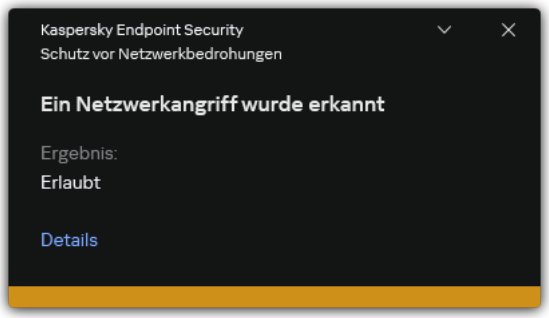
   Ist diese Option aktiviert, so fügt die Komponente „Schutz vor Netzwerkbedrohungen“ den angreifenden Computer zur Sperrliste hinzu. Das bedeutet, dass die Komponente „Schutz vor Netzwerkbedrohungen“ die Netzwerkverbindung mit dem angreifenden Computer nach dem ersten Netzwerkangriffsversuch für die angegebene 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.

4. Sie können auch eine andere Sperrdauer für einen angreifenden Computer festlegen. Verwenden Sie dazu das Feld unter dem Schalter **Angreifende Geräte sperren für n Min**.

5. Speichern Sie die vorgenommenen Änderungen.

Wenn Kaspersky Endpoint Security einen versuchten Netzwerkangriff auf einen Benutzercomputer erkennt, blockiert es daher alle Verbindungen mit dem angreifenden Computer. Kaspersky Endpoint Security erstellt das Ereignis *Netzwerkangriff erkannt*. Das Ereignis enthält Informationen über den angreifenden Computer: IP- und MAC-Adresse.

Sie können die MAC-Adresse des angreifenden Computers in der App-Benutzeroberfläche oder in der Kaspersky Security Center-Konsole Version 15.1 oder höher anzeigen.



Benachrichtigung über einen erkannten Netzwerkangriff

Kaspersky Endpoint Security entsperrt den Computer nach Ablauf der angegebenen Dauer. Zur Überwachung blockierter Computer bietet die Kaspersky Security Center-Konsole keine speziellen Tools, sondern nur die Ereignisse *Netzwerkangriff erkannt* im Bericht. Eine Liste der blockierenden Computer können Sie nur in der Benutzeroberfläche des Programms einsehen. Diese Funktionalität wird vom Tool *Netzwerkmonitor* bereitgestellt. Sie können das Tool „Netzwerkmonitor“ auch verwenden, um die Blockierung eines Computers aufzuheben.

So entsperren Sie einen Computer:

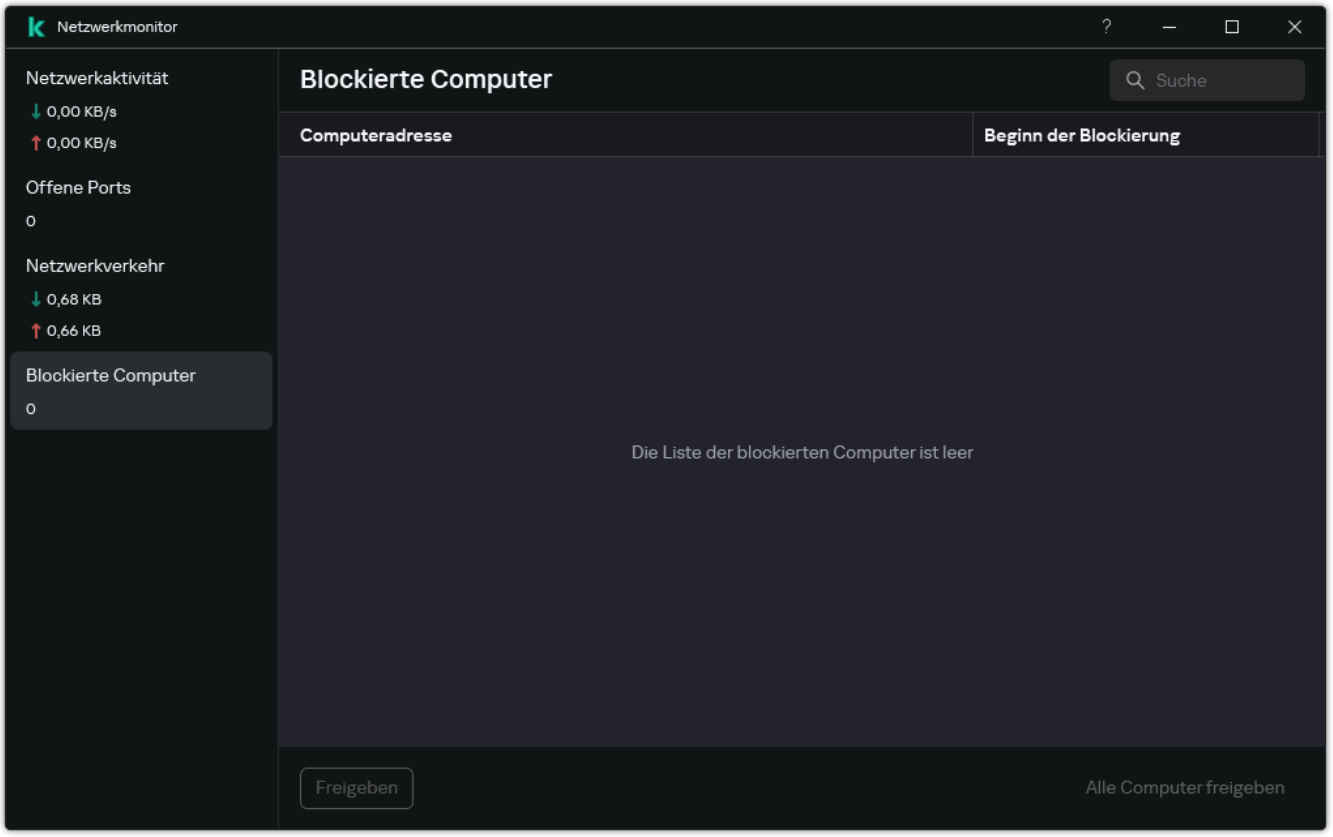
1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Netzwerkmonitor**.

2. Gehen Sie zur Registerkarte **Blockierte Computer**.

   Dadurch wird eine Liste der blockierten Computer geöffnet (siehe Abbildung unten).

   Kaspersky Endpoint Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ geändert werden.

3. Wählen Sie den Computer aus, den Sie entsperren möchten, und klicken Sie auf **Freigeben**.



Liste der blockierten Computer

Adressen anpassen, die bei der Sperrung als Ausnahmen gelten sollen

Kaspersky Endpoint Security kann einen Netzwerkangriff erkennen und eine ungesicherte Netzwerkverbindung blockieren, die eine große Anzahl von Paketen (z. B. von Überwachungskameras) überträgt. Um mit vertrauenswürdigen Geräten zu arbeiten, können Sie die IP-Adressen dieser Geräte zu der Liste der Ausnahmen hinzufügen. Außerdem können Sie das Protokoll und den Port auswählen, die für die Kommunikation verwendet werden, und bestimmte Netzwerkaktivitäten zulassen.

So konfigurieren Sie Adressen von Sperr-Ausnahmen über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.
5. Klicken Sie im Block **Einstellungen für den Schutz vor Netzwerkbedrohungen** auf **Ausnahmen**.
6. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

7. Geben Sie die IP-Adresse des Computers ein, der blockiert werden soll, wenn Netzwerkangriffe von ihm ausgehen.

   Wählen Sie bei Bedarf das Protokoll und die Ports aus, über die die Daten übertragen werden.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie in der Web Console Adressen, die von der Blockierung ausgeschlossen sind

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.
5. Klicken Sie im folgenden Fenster auf den Link **IP-Adressen**.

   Dies öffnet ein Fenster mit einer Liste vertrauenswürdiger IP-Adressen.

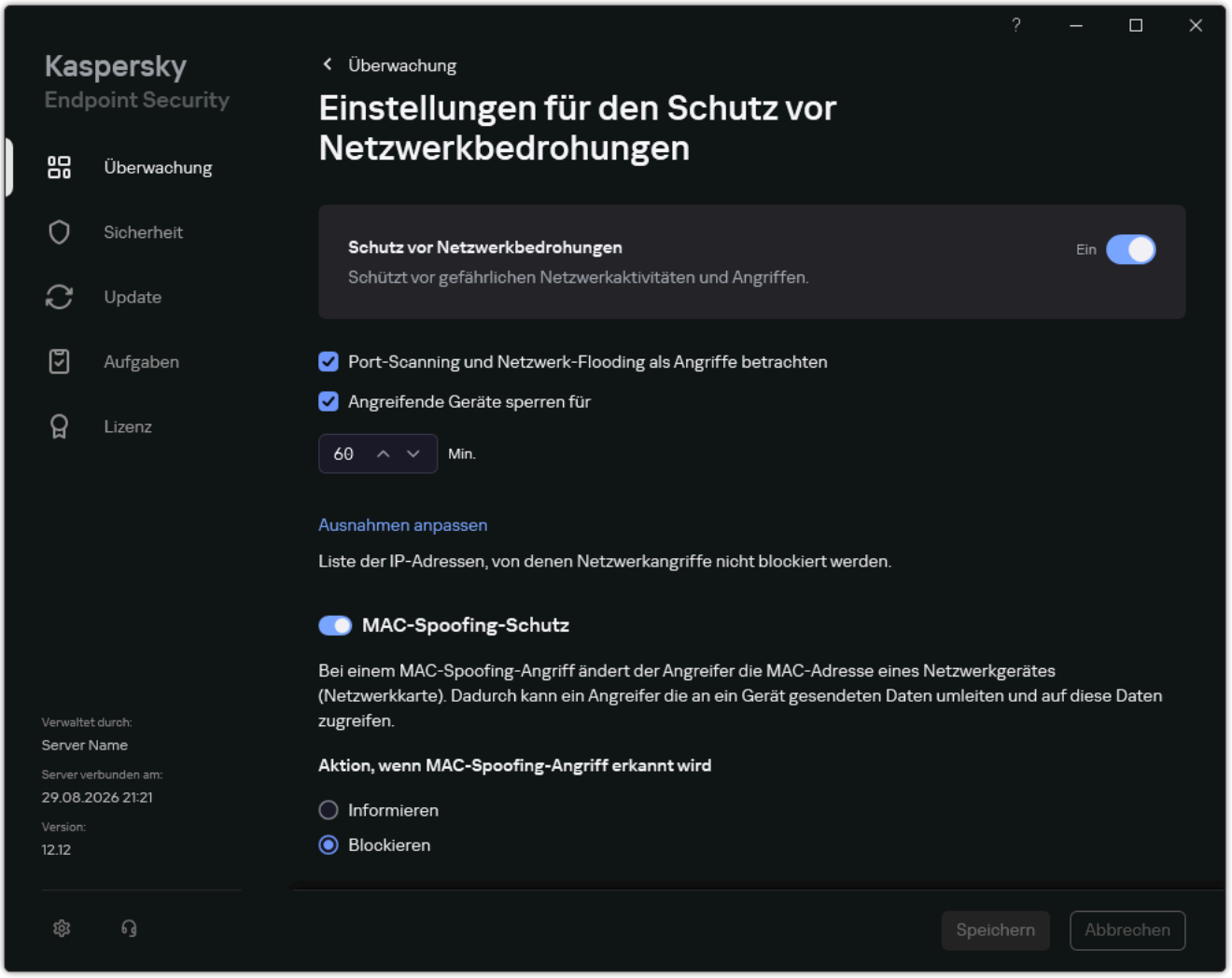
6. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
7. Geben Sie die IP-Adresse des Computers ein, der blockiert werden soll, wenn Netzwerkangriffe von ihm ausgehen.

   Geben Sie bei Bedarf das Subnetz an.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie Adressen von Sperr-Ausnahmen über die App-Oberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

3. Klicken Sie auf den Link **Ausnahmen anpassen**.
4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
5. Geben Sie die IP-Adresse des Computers ein, der blockiert werden soll, wenn Netzwerkangriffe von ihm ausgehen.

   Wählen Sie bei Bedarf das Protokoll und die Ports aus, über die die Daten übertragen werden.
6. Speichern Sie die vorgenommenen Änderungen.

Liste der Sperr-Ausnahmen exportieren und importieren

Sie können die Liste der Ausnahmen in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Adressen desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup für die Listen der Erweiterungen anzulegen oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Ausnahmen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.
4. Klicken Sie im Block **Einstellungen für den Schutz vor Netzwerkbedrohungen** auf **Ausnahmen**.
5. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.
   b. Klicken Sie auf die Schaltfläche → **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Speichern Sie die Datei.
      Kaspersky Endpoint Security exportiert die gesamte Liste der Ausnahmen in die XML-Datei.
6. So importieren Sie die Ausnahmeliste:
   a. Klicken Sie auf die Schaltfläche → **Importieren**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Öffnen Sie die Datei.
      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste der Ausnahmen in der Kaspersky Security Center Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz → Schutz vor Netzwerkbedrohungen**.
5. Klicken Sie im oberen Fensterbereich auf den Link **Vertrauenswürdige IP-Adressen**.
   Die Liste der Ausnahmen öffnet sich.

6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

      Kaspersky Endpoint Security exportiert die Liste der Ausnahmen in eine json-Datei im standardmäßigen Download-Ordner.

7. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der JSON-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

Schutz vor Netzwerkbedrohungen nach Typ konfigurieren

Mit Kaspersky Endpoint Security können Sie den Schutz vor den folgenden Arten von Netzwerkangriffen verwalten:

- *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.

- 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.

- 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

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.

Standardmäßig überwacht Kaspersky Endpoint Security keine Angriffe vom Typ „Network Flooding“, „Port Scanning“ und „MAC-Spoofing“.

Für diese Arten von Angriffen können Sie keine separaten Ausnahmen konfigurieren. Das bedeutet, dass Kaspersky Endpoint Security den angreifenden Computer beim Erkennen eines solchen Angriffs blockiert, selbst wenn einzelne IP-Adressen zur vertrauenswürdigen Zone hinzugefügt wurden. Sie können die Erkennung solcher Angriffe aktivieren oder deaktivieren.

Es wird nicht empfohlen, den MAC-Spoofing-Schutz auf virtuellen Maschinen in der Microsoft Hyper-V-Infrastruktur zu aktivieren. Aufgrund von Besonderheiten der Microsoft Hyper-V-Plattform können Fehlalarme dazu führen, dass Kaspersky Industrial CyberSecurity for Nodes den Hypervisor blockiert.

So konfigurieren Sie den Schutz vor Netzwerkbedrohungen nach Typ (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.
4. Mit dem Kontrollkästchen **Port-Scanning und Netzwerk-Flooding als Angriffe betrachten** können Sie die Erkennung dieser Angriffe aktivieren oder deaktivieren.

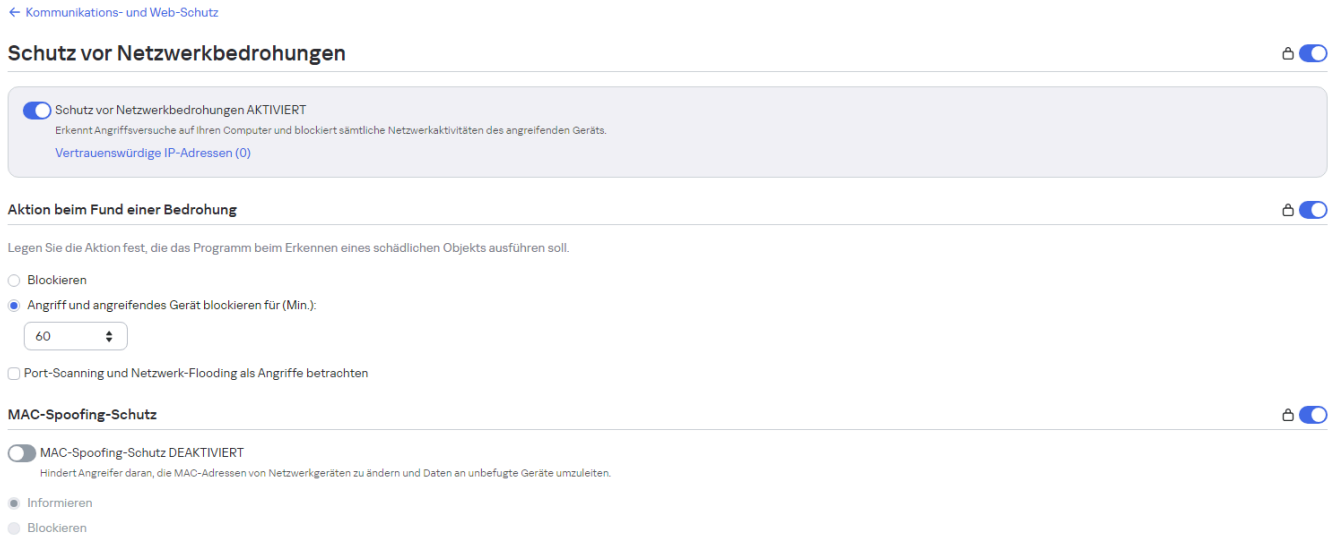
   Wenn diese Funktionalität aktiviert ist, überwacht Kaspersky Endpoint Security den Netzwerkverkehr auf Port-Scanning und Network-Flooding. Wenn ein solches Verhalten erkannt wird, benachrichtigt die App den Benutzer und sendet ein entsprechendes Ereignis an Kaspersky Security Center. Die App stellt Informationen über den Computer bereit, der die Anfragen stellt. Diese Informationen sind für eine zeitnahe Reaktion erforderlich. Allerdings wird der Computer, von dem die Anfragen stammen, nicht durch Kaspersky Endpoint Security blockiert, da dieser Datenverkehr im Unternehmensnetzwerk normal sein kann.
5. Wählen Sie im Block **Modus für MAC-Spoofing-Schutz** eine der folgenden Optionen aus:
   - **MAC-Spoofing nicht überwachen**.
   - **Informieren**.
   - **Blockieren**.
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Schutz vor Netzwerkbedrohungen nach Typ in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kommunikations- und Web-Schutz → Schutz vor Netzwerkbedrohungen**.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

5. Mit dem Kontrollkästchen **Port-Scanning und Netzwerk-Flooding als Angriffe betrachten** können Sie die Erkennung dieser Angriffe aktivieren oder deaktivieren.

   Wenn diese Funktionalität aktiviert ist, überwacht Kaspersky Endpoint Security den Netzwerkverkehr auf Port-Scanning und Network-Flooding. Wenn ein solches Verhalten erkannt wird, benachrichtigt die App den Benutzer und sendet ein entsprechendes Ereignis an Kaspersky Security Center. Die App stellt Informationen über den Computer bereit, der die Anfragen stellt. Diese Informationen sind für eine zeitnahe Reaktion erforderlich. Allerdings wird der Computer, von dem die Anfragen stammen, nicht durch Kaspersky Endpoint Security blockiert, da dieser Datenverkehr im Unternehmensnetzwerk normal sein kann.

6. Konfigurieren Sie unter **MAC-Spoofing-Schutz** die Erkennung von MAC-Spoofing-Angriffen:

   a. Mit dem Schalter **MAC-Spoofing-Schutz AKTIVIERT** können Sie die Erkennung dieser Angriffe aktivieren oder deaktivieren.

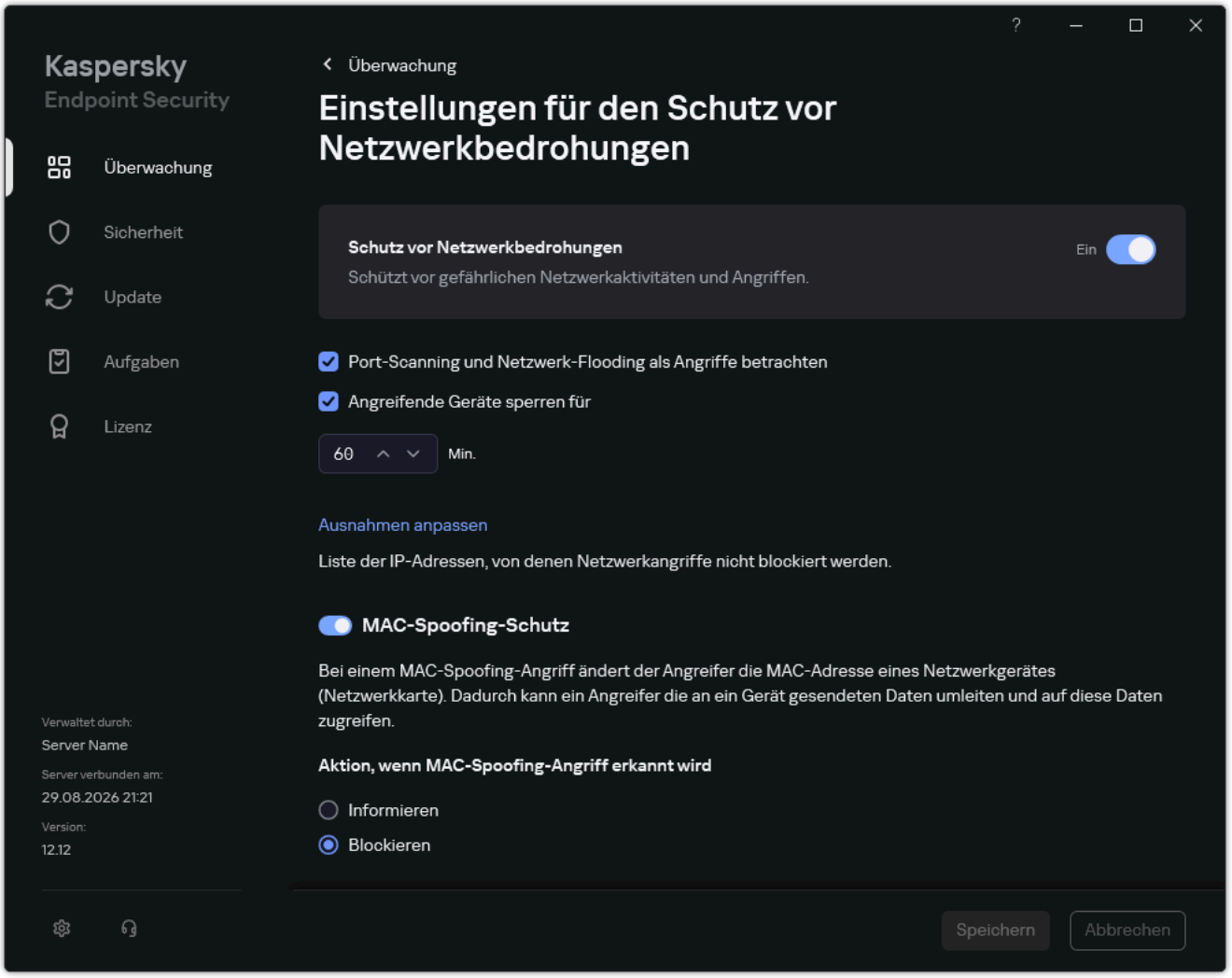
   b. Wählen Sie die Aktion aus, die beim Erkennen eines MAC-Spoofing-Angriffs ausgeführt werden soll:

   - **Informieren**.
   - **Blockieren**.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Schutz vor Netzwerkbedrohungen nach Typ (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Schutz vor Netzwerkbedrohungen** aus.



Einstellungen für den „Schutz vor Netzwerkbedrohungen“

3. Mit dem Schalter **Port-Scanning und Netzwerk-Flooding als Angriffe betrachten** können Sie die Erkennung dieser Angriffe aktivieren oder deaktivieren.

   Wenn diese Funktionalität aktiviert ist, überwacht Kaspersky Endpoint Security den Netzwerkverkehr auf Port-Scanning und Network-Flooding. Wenn ein solches Verhalten erkannt wird, benachrichtigt die App den Benutzer und sendet ein entsprechendes Ereignis an Kaspersky Security Center. Die App stellt Informationen über den Computer bereit, der die Anfragen stellt. Diese Informationen sind für eine zeitnahe Reaktion erforderlich. Allerdings wird der Computer, von dem die Anfragen stammen, nicht durch Kaspersky Endpoint Security blockiert, da dieser Datenverkehr im Unternehmensnetzwerk normal sein kann.

4. Mit dem Schalter **MAC-Spoofing-Schutz** können Sie die Erkennung dieser Angriffe aktivieren oder deaktivieren.

5. Wählen Sie im Block **Aktion, wenn MAC-Spoofing-Angriff erkannt wird** eine der folgenden Optionen aus:

   - **Informieren**.
   - **Blockieren**.

6. Speichern Sie die vorgenommenen Änderungen.

Firewall

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*.

Der Administrationsagent wird für die Interaktion mit Kaspersky Security Center verwendet. Die Firewall erstellt automatisch Netzwerkregeln, die für die ordnungsgemäße Funktion des Programms und des Administrationsagenten erforderlich sind. Dadurch bedingt öffnet die Firewall bestimmte Ports auf dem Computer. Welche Ports geöffnet werden, hängt von der Rolle des Computers ab (z. B. Verteilungspunkt). Weitere Informationen zu den Ports, die auf dem Computer geöffnet werden, finden Sie in der Hilfe zu Kaspersky Security Center.

Netzwerkregeln

Sie können die Netzwerkregeln auf folgenden Ebenen anpassen:

- *Regeln für Netzwerkpakete*. Sie dienen zur Definition von Beschränkungen für die Netzwerkpakete, wobei das Programm keine Rolle spielt. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Kaspersky Endpoint Security hat vordefinierte Netzwerkregeln für Pakete mit Lösungen, die von den Kaspersky-Experten empfohlen werden.

- *Netzwerkregeln für das Programm*. Sie dienen zur Definition von Beschränkungen der Netzwerkaktivität eines konkreten Programms. Dabei werden nicht nur die Merkmale des Netzwerkpakets berücksichtigt, sondern auch das konkrete Programm, an das dieses Netzwerkpaket adressiert ist oder welches das Senden dieses Netzwerkpakets initiiert hat.

Die Komponente „Programm-Überwachung“ kontrolliert mithilfe von *Programmrechten* den Zugriff auf Betriebssystemressourcen, Prozesse und persönliche Daten.

Wenn ein Programm zum ersten Mal gestartet wird, führt die „Firewall“ folgende Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.

2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Firewall“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Platziert das Programm in einer der Vertrauensgruppen: *Vertrauenswürdig*, *Schwach beschränkt*, *Stark beschränkt*, *Nicht vertrauenswürdig*.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung“ aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Netzwerkaktivität des Programms. Für Programme aus der Sicherheitsgruppe „*Stark beschränkt*“ sind beispielsweise alle Netzwerkverbindungen verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde das Programm nicht verändert, so wendet die Komponente die aktuellen Netzwerkregeln darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Prioritäten der Netzwerkregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Netzwerkaktivität in mehreren Regeln vorkommt, reguliert die „Firewall“ die Netzwerkaktivität nach der Regel mit der höchsten Priorität.

Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme. Sind für eine Art der Netzwerkaktivität gleichzeitig Netzwerkregeln für Pakete und Netzwerkregeln für Programme vorhanden, wird diese Netzwerkaktivität nach den Netzwerkregeln für Pakete verarbeitet.

Netzwerkregeln für Programme funktionieren auf besondere Weise. Die Netzwerkregel für Programme enthält Zugriffsregeln basierend auf dem Netzwerkstatus: *Öffentliches Netzwerk*, *Lokales Netzwerk*, *Vertrauenswürdiges Netzwerk*. Zum Beispiel ist für die Sicherheitsgruppe „*Stark beschränkt*“ standardmäßig jede Netzwerkaktivität eines Programms in Netzwerken mit beliebigem Status verboten. Wenn für ein bestimmtes Programm (übergeordnetes Programm) eine Netzwerkregel vorliegt, werden die untergeordneten Prozesse anderer Programme gemäß der Netzwerkregel des übergeordneten Programms ausgeführt. Gibt es keine Netzwerkregel für ein Programm, so werden die untergeordneten Prozesse gemäß der Regel für den Zugriff auf Netzwerke der Sicherheitsgruppe des Programms ausgeführt.

Beispiel: Sie haben jede Netzwerkaktivität aller Programme für Netzwerke mit beliebigem Status verboten, unter Ausnahme von Browser X. Wenn Browser X (übergeordnetes Programm) die Installation von Browser Y startet (untergeordneter Prozess), erhält Browser Y Zugriff auf das Netzwerk und lädt die erforderlichen Dateien herunter. Nach der Installation sind für Browser Y alle Netzwerkverbindungen verboten, wobei die Einstellungen der Firewall gelten. Um dem Installationsprogramm von Browser Y die Netzwerkaktivität als untergeordneter Prozess zu verbieten, muss eine Netzwerkregel für das Installationsprogramm von Browser Y hinzugefügt werden.

Arten von Netzwerkverbindungen

Bei der Kontrolle der Netzwerkaktivität kann die „Firewall“ den Typ einer Netzwerkverbindung berücksichtigen. Den Typ der Netzwerkverbindung erhält Kaspersky Endpoint Security vom Betriebssystem des Computers. Den Typ einer Netzwerkverbindung im Betriebssystem legt der Benutzer beim Einrichten der Verbindung fest. Sie können den Typ der Netzwerkverbindung in den Einstellungen von Kaspersky Endpoint Security ändern. Dann kontrolliert die Firewall die Netzwerkaktivität anhand des Netzwerktyps, der in den Einstellungen von Kaspersky Endpoint Security angegeben ist, nicht anhand des Typs aus dem Betriebssystem.

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.

  Das Internet erhält von der Firewall standardmäßig den Typ *Öffentliches Netzwerk*. Der Typ des Internets kann nicht geändert werden.

- **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 im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.

Kompatibilität mit der Windows Defender Firewall

Das Betriebssystem verfügt über eine eigene integrierte Firewall, die *Windows Defender Firewall*. Das Programm verhält sich je nach Betriebssystemtyp unterschiedlich:

- **Workstation**. Die parallele Verwendung der Kaspersky Firewall und der Windows Defender Firewall kann zu Fehlfunktionen des Betriebssystems führen. Daher verfügt Kaspersky Endpoint Security über einen Mechanismus, der die gleichzeitige Verwendung beider Firewalls verhindert. Wenn Sie die Kaspersky Firewall aktivieren, deaktiviert das Betriebssystem automatisch die Windows Defender Firewall. Wenn Sie die Kaspersky Firewall deaktivieren, aktiviert das Betriebssystem die Windows Defender Firewall automatisch wieder, damit der Computer geschützt bleibt.

- **Server**. Die Kaspersky Firewall und die Windows Defender Firewall sind nicht miteinander kompatibel. Das Installationsprogramm von Kaspersky Endpoint Security entfernt die Windows Defender Firewall automatisch bei der Installation des Programms.

Firewall aktivieren und deaktivieren

Die Firewall ist standardmäßig aktiviert und arbeitet im optimalen Modus.

So aktivieren oder deaktivieren Sie die Firewall über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz → Firewall**.
4. Verwenden Sie das Kontrollkästchen **Firewall**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Firewall in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie **Kommunikations- und Web-Schutz → Firewall**.
5. Verwenden Sie den Schalter **Firewall AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Firewall über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz → Firewall** aus.
3. Verwenden Sie den Schalter **Firewall**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Wenn die Firewall aktiviert ist, kontrolliert Kaspersky Endpoint Security daher die Netzwerkaktivität und blockiert nicht autorisierte Netzwerkverbindungen zu Ihrem Computer sowie die nicht autorisierte Netzwerkaktivität von Programmen auf Ihrem Computer. Die Netzwerkaktivität wird auch von der Komponente zum Schutz vor Netzwerkbedrohungen gesteuert. Die Komponente „Schutz vor Netzwerkbedrohungen" (auch Intrusion Detection System oder IDS genannt) überwacht den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe charakteristisch sind.

Kaspersky Endpoint Security protokolliert Netzwerkangriffsereignisse in seinen Berichten unabhängig von den Firewall-Einstellungen. Auch wenn die Firewall die Netzwerkverbindung anhand von Regeln blockiert und so einen Netzwerkangriff verhindert, registriert die Komponente Schutz vor Netzwerkbedrohungen Netzwerkangriffsereignisse. Das ist erforderlich, um statistische Informationen über Netzwerkangriffe auf die Computer in Ihrer Organisation zu generieren.

Typ einer Netzwerkverbindung ändern

Das Internet erhält von der Firewall standardmäßig den Typ *Öffentliches Netzwerk*. Der Typ des Internets kann nicht geändert werden.

Um den Netzwerkverbindungstyp zu ändern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Verfügbare Netzwerke**.
4. Wählen Sie die Netzwerkverbindung, deren Typ Sie ändern möchten.
5. Wählen Sie in der Spalte **Netzwerktyp** den Typ der Netzwerkverbindung aus:
   - **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 im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.
6. Speichern Sie die vorgenommenen Änderungen.

Arbeit mit Netzwerkregeln für Pakete

Bei der Arbeit mit Netzwerkregeln für Pakete können Sie folgende Aktionen ausführen:

- Erstellen einer neuen Netzwerkregel für Pakete

  Sie können eine neue Netzwerkregel für Pakete erstellen. Dazu wird eine Kombination von Bedingungen und Aktionen für Netzwerkpakete und Datenströme festgelegt.

- Aktivieren und Deaktivieren einer Netzwerkregel für Pakete

  Alle Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt werden, besitzen den Status *Aktiv*. Ist eine Netzwerkregel für Pakete aktiviert, wendet die Firewall diese Regel an.

  Sie können eine beliebige Netzwerkregel für Pakete deaktivieren, die auf der Liste der Netzwerkregeln für Pakete steht. Ist eine Netzwerkregel für Pakete deaktiviert, wird diese Regel vorübergehend nicht von der Firewall verwendet.

Eine neue Netzwerkregel für Pakete, die vom Benutzer erstellt wurde, wird standardmäßig mit dem Status *Aktiv* zur Liste Netzwerkregeln für Pakete hinzugefügt.

- Ändern der Einstellungen einer vorhandenen Netzwerkregel für Pakete

  Nach Erstellung einer neuen Netzwerkregel für Pakete können Sie ihre Einstellungen jederzeit ändern.

- Ändern der Firewall-Aktion für eine Netzwerkregel für Pakete

  In der Liste der Netzwerkregeln für Pakete können Sie die Aktion ändern, die von der Firewall ausgeführt wird, wenn eine Netzwerkaktivität erkannt wird, die der angegebenen Netzwerkregel für Pakete entspricht.

- Ändern der Priorität einer Netzwerkregel für Pakete

  Sie können die Priorität einer in der Liste markierten Netzwerkregel für Pakete ändern.

- Löschen einer Netzwerkregel für Pakete

  Sie können eine Netzwerkregel für Pakete löschen, wenn Sie nicht möchten, dass diese Regel beim Fund einer Netzwerkaktivität von der Firewall angewendet wird und dass die Regel mit dem Status *Deaktiviert* in der Liste der Netzwerkregeln für Pakete erscheint.

Eine Netzwerkpaketregel erstellen

Die Firewall filtert alle Netzwerkaktivitäten auf dem Computer anhand von Regeln für Netzwerkpakete. Regeln für Netzwerkpakete enthalten Bedingungen (z. B. Richtung und Protokoll), nach denen die Firewall die Netzwerkverbindungen des Computers kontrolliert. Regeln für Netzwerkpakete legen auch fest, welche Aktion die Firewall mit einer Verbindung ausführt, die der Regel entspricht (Verbindung erlauben oder blockieren).

Empfehlungen zum Erstellen von Regeln für Netzwerkpakete

Sie können eine IP-Adresse oder einen Bereich von IP-Adressen angeben, um die Netzwerkaktivität zu filtern. Sie können auch einen DNS-Namen angeben.

Wenn in einer Regel ein DNS-Name verwendet wird, löst Kaspersky Endpoint Security diesen DNS-Namen in eine IP-Adresse auf und verarbeitet die Regel anschließend so, als wäre diese IP-Adresse darin angegeben.

Kaspersky Endpoint Security kann DNS-Namen in den folgenden Fällen auflösen:

- Programmstart
- Ändern der Firewall-Einstellungen

Wenn das Programm DNS-Namen von dem Computer auflöst, auf dem es installiert ist, kann eine große Anzahl von Anfragen an den DNS-Server gesendet werden. Um dies zu vermeiden, wird empfohlen, beim Erstellen von Regeln IP-Adressen anstelle von DNS-Namen zu verwenden.

In einigen Fällen kann die Verwendung von DNS-Namen in den Namen von Netzwerkpaketen unsicher sein, da der Besitzer des DNS-Servers die Parameter des DNS-Eintrags ändern kann. Außerdem könnte ein böswilliger Akteur DNS-Nachrichten fälschen und Firewall-Regeln umgehen.

Mithilfe von Regeln der Web-Kontrolle können Sie Netzwerkverbindungen nach DNS-Namen kontrollieren. Sollte es erforderlich sein, in Firewall-Regeln einen DNS-Namen anzugeben:

- Sorgen Sie für die Sicherheit des Unternehmens-LANs.
- Gewährleisten Sie die Sicherheit von Caching- und autoritativen DNS-Servern.
- Schützen Sie den DNS-Eintrag vor Änderungen.

Bei der Erstellung von Regeln für Netzwerkpakete ist zu beachten, dass diesen Vorrang vor den Netzwerkregeln für Programme eingeräumt wird.

Methoden zum Erstellen von Regeln für Netzwerkpakete

Eine Netzwerkpaketregel kann auf folgende Arten erstellt werden:

- Verwenden Sie das Tool Netzwerkmonitor.

  Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen. Das ist praktisch, da Sie so nicht alle Regeleinstellungen konfigurieren müssen. Einige Firewall-Einstellungen werden automatisch aus den Daten des Netzwerkmonitors eingefügt. Der Netzwerkmonitor ist nur in der Programmoberfläche verfügbar.

- Konfigurieren Sie die Firewall-Einstellungen.

  Auf diese Weise können Sie die einzelnen Firewall-Einstellungen flexibel anpassen. Sie können Regeln für jede Netzwerkaktivität erstellen, selbst wenn derzeit keine Netzwerkaktivität vorhanden ist.

Verwendung des Netzwerkmonitors zum Erstellen einer Netzwerkpaketregel in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Netzwerkmonitor**.
2. Gehen Sie zur Registerkarte **Netzwerkaktivität**.

   Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt.
3. Wählen Sie im Kontextmenü einer Netzwerkverbindung den Punkt **Regel für Netzwerkpakete erstellen**.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.
4. Setzen Sie den Status **Aktiv** für die Paketregel.
5. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
6. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
7. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

8. Klicken Sie auf **Speichern**.

   Die neue Netzwerkregel wird der Liste hinzugefügt.

9. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

10. Speichern Sie die vorgenommenen Änderungen.

Verwendung der Firewall-Einstellungen zum Erstellen einer Netzwerkpaketregel in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.

4. Wählen Sie in der Dropdown-Liste **Hinzufügen** die Position der Regel in der Liste aus: am Anfang der Liste, am Ende der Liste oder neben der ausgewählten Regel.

   Die Position, die eine Regel in der Liste einnimmt, bestimmt die Priorität der Regel. Die oberste Regel in der Liste hat die höchste Priorität.

5. Setzen Sie den Status **Aktiv** für die Paketregel.

6. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.

7. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

8. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

9. Klicken Sie auf **Speichern**.

   Die neue Netzwerkregel wird der Liste hinzugefügt.

10. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

11. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Netzwerkpaketregel in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Firewall**.

4. Klicken Sie im Block **Firewall-Einstellungen** auf **Einstellungen**.

   Eine Liste mit Netzwerkpaketregeln und eine Liste mit Netzwerkregeln für Programme werden geöffnet.

5. Gehen Sie zur Registerkarte **Regeln für Netzwerkpakete**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.

6. Wählen Sie in der Dropdown-Liste **Hinzufügen** die Position der Regel in der Liste aus: am Anfang der Liste, am Ende der Liste oder neben der ausgewählten Regel.

   Die Position, die eine Regel in der Liste einnimmt, bestimmt die Priorität der Regel. Die oberste Regel in der Liste hat die höchste Priorität.

7. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.

8. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf die Schaltfläche klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

9. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

10. Speichern Sie die Netzwerkregel.

11. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

12. Speichern Sie die vorgenommenen Änderungen.

Die Firewall wird Netzwerkpakete gemäß dieser Regel überwachen. Eine Paketregel kann in der Firewall deaktiviert werden, ohne dass sie aus der Liste gelöscht werden muss. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

So erstellen Sie eine Regel für Netzwerkpakete in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie **Kommunikations- und Web-Schutz** → **Firewall**.

5. Wählen Sie die Registerkarte **Regeln für Netzwerkpakete** aus.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.

6. Klicken Sie auf **Hinzufügen**.

   Dadurch wird das Formular für eine neue Netzwerkregel geöffnet.

7. Geben Sie im Feld **Regelname** manuell den Namen des Netzwerkdienstes ein.

8. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Regelvorlage auswählen** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

9. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

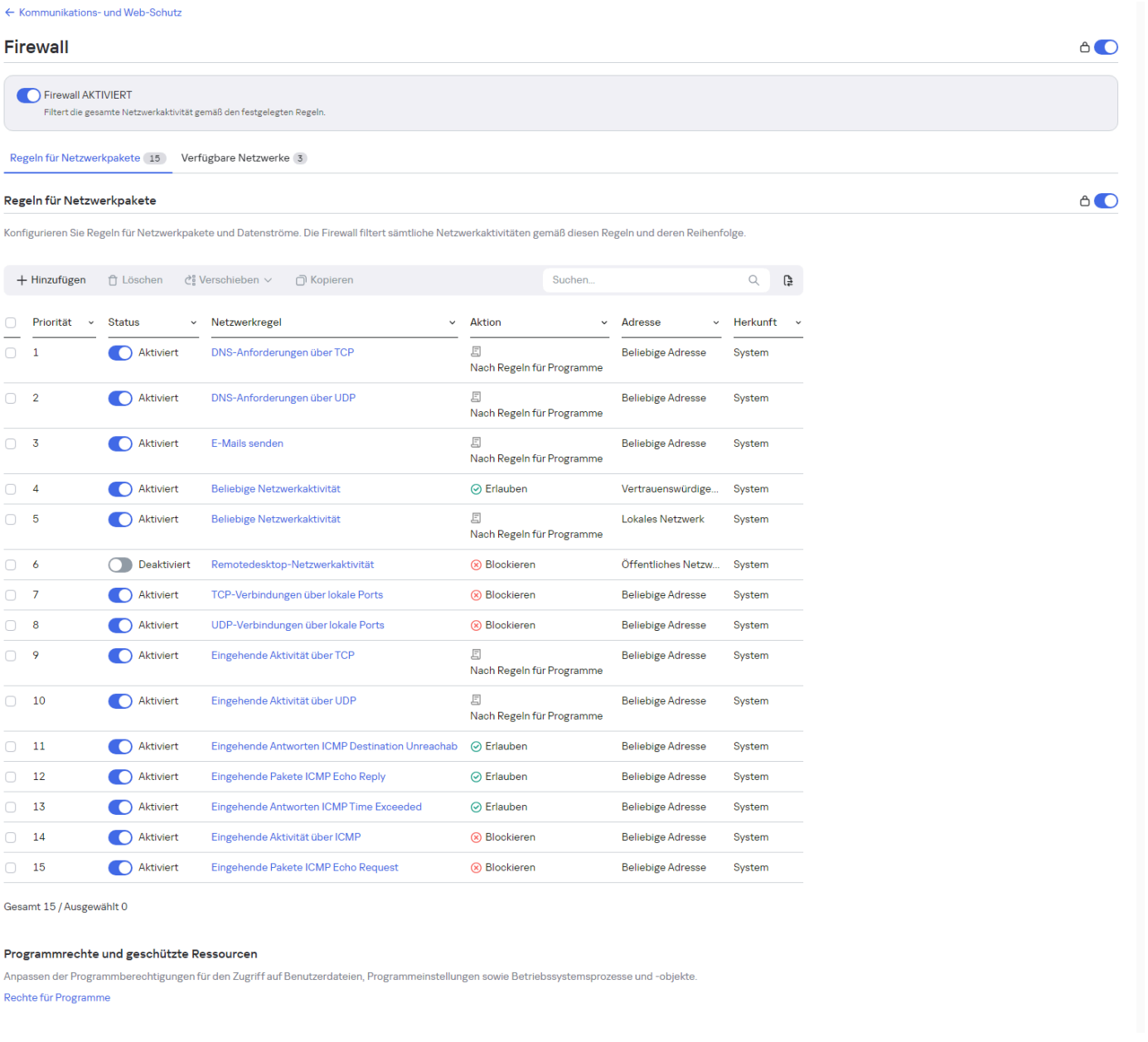
10. Speichern Sie die Netzwerkregel.

    Die neue Netzwerkregel wird der Liste hinzugefügt.

11. Verwenden Sie die Schaltfläche **Verschieben**, um die Priorität der Netzwerkregel festzulegen.

12. Speichern Sie die vorgenommenen Änderungen.

Die Firewall wird Netzwerkpakete gemäß dieser Regel überwachen. Eine Paketregel kann in der Firewall deaktiviert werden, ohne dass sie aus der Liste gelöscht werden muss. Verwenden Sie den Schalter in der Spalte **Status**, um die Paketregel zu aktivieren oder zu deaktivieren.



Firewall-Paketregeln

Einstellungen der Netzwerkpaketregel

Einstellung	Beschreibung
Aktion	**Erlauben**. **Blockieren**. **Nach Regeln des Programms**. Bei Auswahl dieser Variante wendet die Firewall die Netzwerkregeln des Programms auf die Netzwerkverbindung an.

Einstellung	Beschreibung
Protokoll	Überwachen Sie die Netzwerkaktivität über das ausgewählte Protokoll: TCP, UDP, ICMP, ICMPv6, IGMP und GRE. Wurde ICMP oder ICMPv6 als Protokoll gewählt, können Sie Typ und Code des ICMP-Pakets festlegen. Wurde TCP oder UDP als Protokolltyp ausgewählt, können Sie die Portnummern des lokalen Computers und des Remote-Computers angeben, zwischen denen die Verbindung überwacht werden soll. Bereich der möglichen Werte für die Portnummern: 0 bis 65535. Sie können in jedes Feld mehrere, durch `,` getrennte Werte eingeben oder mit `-` einen Wertebereich festlegen. Beispielsweise: • `100,101` • `100-130` • `100,110-130`
Richtung	**Eingehend (Paket)**. Die Firewall wendet die Netzwerkregel auf alle eingehenden Netzwerkpakete an. **Eingehend**. Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine von einem Remote-Computer initiierte Verbindung gesendet werden. **Eingehend/Ausgehend**. Die Firewall wendet die Netzwerkregel auf alle eingehenden und ausgehenden Netzwerkpakete an. **Ausgehend (Paket)**. Die Firewall wendet die Netzwerkregel auf alle ausgehenden Netzwerkpakete an. **Ausgehend**. Die Firewall wendet die Netzwerkregel auf alle Netzwerkpakete an, die über eine vom Benutzercomputer initiierte Verbindung gesendet werden.
Netzwerkadapter	Netzwerkadapter, die Netzwerkpakete senden und/oder empfangen können. Das Festlegen der Einstellungen für Netzwerkadapter erlaubt das Unterscheiden von Netzwerkpaketen, die von den Netzwerkadaptern mit denselben IP-Adressen gesendet oder empfangen wurden.
Lebensdauer (TTL)	Begrenzung der Kontrolle von Netzwerkpaketen nach ihrer Lebensdauer (Time to Live, TTL).
Remote-Adressen	Netzwerkadressen der Remote-Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegebenen Bereich von Remote-Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen, eine separate Liste mit IP-Adressen erstellen, einen IP-Adressbereich angeben oder ein Subnetz auswählen (Vertrauenswürdige Netzwerke, Lokale Netzwerke, Öffentliche Netzwerke). Anstelle der IP-Adresse können Sie auch den DNS-Namen eines Computers angeben. DNS-Namen sollten nur für LAN-Computer oder interne Dienste verwendet werden. Die Interaktion mit Cloud-Diensten (z. B. Microsoft Azure) und anderen Internetressourcen sollte von der Komponente „Web Control“ abgewickelt werden. Wenn Sie in der Netzwerkpaketregel einen DNS-Namen hinzugefügt haben, für den keine IP-Adresse ermittelt werden konnte, zeigt Kaspersky Endpoint Security eine Warnung an. Web Console: Zur Liste der Regeln für Netzwerkpakete wurde eine Spalte mit einer Fehlerbeschreibung hinzugefügt. In der Verwaltungskonsole (MMC) ist die Fehlerbeschreibung nicht verfügbar. Solche Paketregeln werden farblich hervorgehoben.
Lokale Adressen	Netzwerkadressen der Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegeben Bereich von lokalen Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen, eine separate Liste mit IP-Adressen erstellen oder einen IP-Adressbereich angeben. Das Programm speichert lokale Adressen nur dann, wenn eine Liste mit Remote-Adressen angegeben ist. Das heißt, der Wert **Adressen aus der Liste** wurde für **Remote-Adressen** ausgewählt und mindestens eine Adresse wurde hinzugefügt. Es ist für Anwendungen nicht immer möglich, die lokale Adresse zu bekommen. In diesem Fall wird diese Einstellung ignoriert.

Netzwerkregel für Pakete aktivieren und deaktivieren

Gehen Sie folgendermaßen vor, um eine Regel für Netzwerkpakete zu aktivieren oder zu deaktivieren:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.

4. Wählen Sie in der Liste die erforderliche Regel für Netzwerkpakete.

5. Verwenden Sie den Schalter in der Spalte **Status**, um die Regel zu aktivieren oder zu deaktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

Verhalten der Firewall in Bezug auf Netzwerkregeln für Pakete ändern

Gehen Sie folgendermaßen vor, um die Firewall-Aktion für die Regel für Netzwerkpakete zu ändern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.

4. Wählen Sie aus der Liste der Netzwerkregeln für Pakete eine Regel und klicken Sie auf **Ändern**, um sie zu ändern.

5. Wählen Sie in der Dropdown-Liste **Aktion** die Aktion aus, welche die Firewall bei Erkennen der entsprechenden Art von Netzwerkaktivität ausführen soll:

   - **Erlauben**.
   - **Blockieren**.
   - **Nach Regeln des Programms**. Bei Auswahl dieser Variante wendet die Firewall die Netzwerkregeln des Programms auf die Netzwerkverbindung an.

6. Speichern Sie die vorgenommenen Änderungen.

Priorität einer Netzwerkregel für Pakete ändern

Die Ausführungspriorität einer Regel für Netzwerkpakete wird durch ihre Position in der Liste der Regeln für Netzwerkpakete bestimmt. Die Netzwerkregel, die in der Liste der Regeln für Netzwerkpakete an erster Stelle steht, besitzt die höchste Priorität.

Jede Regel für Netzwerkpakete, die Sie manuell erstellen, wird am Ende der Liste der Regeln für Netzwerkpakete hinzugefügt und besitzt die niedrigste Priorität.

Die Firewall führt die Regeln in der Reihenfolge aus, in der sie auf der Liste der Regeln für Netzwerkpakete stehen (von oben nach unten). Entsprechend jeder Regel für Netzwerkpakete, die verarbeitet und auf eine bestimmte Netzwerkverbindung angewendet wurde, erlaubt oder verbietet die Firewall den Netzwerkzugriff auf die Adressen und Ports, die in den Einstellungen dieser Netzwerkverbindung angegeben sind.

Gehen Sie folgendermaßen vor, um die Priorität einer Regel für Netzwerkpakete zu ändern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Paketregeln**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln für Pakete, die standardmäßig von der Firewall erstellt wurden.
4. Wählen Sie in der Liste die Regel für Netzwerkpakete, deren Priorität Sie ändern möchten.
5. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Netzwerkpaketregeln

Sie können die Liste der Regeln für Netzwerkpakete in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Regeln desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie ein Backup für die Liste der Regeln für Netzwerkpakete anlegen oder die Liste auf einen anderen Server migrieren.

Exportieren und Importieren einer Liste von Regeln für Netzwerkpakete in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Firewall**.
4. Klicken Sie im Block **Firewall-Einstellungen** auf **Einstellungen**.

   Eine Liste mit Netzwerkpaketregeln und eine Liste mit Netzwerkregeln für Programme werden geöffnet.
5. Gehen Sie zur Registerkarte **Regeln für Netzwerkpakete**.
6. So exportieren Sie die Liste der Regeln für Netzwerkpakete:

   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

   Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.

   b. Klicken Sie auf den Link **Exportieren**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.

7. So importieren Sie eine Liste der Regeln für Netzwerkpakete:

   a. Klicken Sie auf den Link **Importieren**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste von Regeln für Netzwerkpakete in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie **Kommunikations- und Web-Schutz** → **Firewall**.
5. Um die Liste der Regeln zu exportieren, gehen Sie im Block **Regeln für Netzwerkpakete** wie folgt vor:

   a. Wählen Sie die Regeln, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine json-Datei im standardmäßigen Download-Ordner.
6. Zum Importieren der Liste der Regeln gehen Sie im Block **Regeln für Netzwerkpakete** wie folgt vor:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

Regeln für Netzwerkpakete in XML definieren

In der „Firewall" können auch Regeln für Netzwerkpakete im XML-Format exportiert werden. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Regeln desselben Typs hinzuzufügen.

Die XML-Datei enthält die zwei Hauptknoten `Rules` und `Resources`. Der Knoten `Rules` enthält Regeln für Netzwerkpakete. Dieser Knoten enthält die standardmäßig konfigurierten Regeln (*vordefinierte Regeln*) und die vom Benutzer hinzugefügten Regeln (*benutzerdefinierte Regeln*).

Markup für Netzwerkpaketregeln

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

Einstellungen für Netzwerkpaketregeln im XML-Format

Einstellung	Beschreibung	Wert
`<key name="0000">`	Priorität der Regel. Je niedriger der Wert, desto höher ist die Priorität.	Ganze Zahl Der Prioritätswert muss aus 4 Ziffern bestehen. Die Knoten in der XML-Datei müssen nach Prioritätswert angeordnet sein, beginnend mit `0000`.
`RuleId`	ID der Regel.	**Vorkonfigurierte Regeln** `100` – **DNS-Anforderungen über TCP**. `101` – **DNS-Anforderungen über UDP**. `102` – **E-Mail-Nachrichten senden**. `110` – **Jede Netzwerkaktivität** (Vertrauenswürdige Netzwerke). `125` – **Jede Netzwerkaktivität** (Lokale Netzwerke). `130` – **Remotedesktop-Netzwerkaktivität**. `131` – **TCP-Verbindungen über lokale Ports**. `132` – **UDP-Verbindungen über lokale Ports**. `133` – **Eingehende Aktivität über TCP**. `134` – **Eingehende Aktivität über UDP**. `137` – **Eingehende Antworten ICMP Destination Unreachable**. `138` – **Eingehende Pakete ICMP Echo Reply**. `140` – **Eingehende Antworten ICMP Time Exceeded**. `142` – **Eingehende Aktivität über ICMP**. `266` – **Eingehende Pakete ICMPv6 Echo Request**.
`RuleState`	Status der Regel.	`0` – vordefinierte Regel ist deaktiviert `1` – vordefinierte Regel ist aktiviert `2` – benutzerdefinierte Regel ist deaktiviert `3` – benutzerdefinierte Regel ist aktiviert
`RuleTypeId`	ID der Regeltyps.	`4` – Regel für Netzwerkpakete.
`AppIdEx`	ID der App, zu der die Regel für Netzwerkpakete gehört.	Wenn die Regel nicht zu einer App gehört, ist der Wert `0`.
`ResIdEx`	Haupt-ID der Ressource mit den Regeleinstellungen. Diese ID können Sie verwenden, um einen Block mit Regeleinstellungen im Knoten `Resources` zu suchen.	Ganze Zahl
`ResIdEx2`	ID des Netzwerktyps.	`0` – **Beliebige Adresse**. `50` – **Vertrauenswürdige Netzwerke**. `51` – **Lokale Netzwerke**. `52` – **Öffentliche Netzwerke**. `<Network Identifier>` – **Adressen aus der Liste** (Adressen werden manuell definiert).

Einstellung	Beschreibung	Wert
`AccessFlag`	Wert des Parameters **Aktion**.	`0` – **Erlauben**. `2` – **Nach Regeln des Programms**. `3` – **Verbieten**. `4` – **Erlauben** und **Protokollieren**. `6` – **Nach Regeln des Programms** und **Protokollieren**. `7` – **Verbieten** und **Protokollieren**.
`</key>`		

Der Knoten `Resources` enthält Einstellungen für Netzwerkpaketregeln. Einstellungen einer benutzerdefinierten Regel für Netzwerkpakete sind im Block `<key name="0004">` enthalten.

Benutzerdefiniertes Markup für Netzwerkpaketregeln

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

Benutzerdefinierte Einstellungen der Netzwerkpaketregel

Einstellung	Beschreibung	Wert
`<key name="Data">`	ID des Parameterblocks.	Ganze Zahl
`RemotePorts`	Wert des Parameters **Remote-Ports**.	Liste der Remote-Portbereiche.
`LocalPorts`	Wert des Parameters **Lokale Ports**.	Liste der lokalen Portbereiche.

Einstellung	Beschreibung	Wert
`AdapterBindings`	Wert des Parameters **Netzwerkadapter**.	`IpAddresses` – Wert des Parameters **IP-Adressen**. `MacAddresses` – Wert des Parameters **MAC-Adressen**. `AdapterName` – Name des Netzwerkadapters. `InterfaceType` – Wert des Parameters **Schnittstellentyp**: • `0` – **Andere**. • `1` – **LoopBack**. • `2` – **Kabelgebundenes Netzwerk (Ethernet)**. • `3` – **Drahtlosnetzwerk (WLAN)**. • `4` – **Tunnel**. • `5` – **PPP-Verbindung**. • `6` – **PPPoE-Verbindung**. • `7` – **VPN-Verbindung**. • `8` – **Modemverbindung**.
`unique`	Interne ID der Struktur.	Ganze Zahl Es wird empfohlen, diesen Parameter nicht zu verändern.
`Proto`	Wert des Parameters **Protokoll**.	`0` – deaktiviert. `1` – **ICMP**. `2` – **IGMP**. `6` – **TCP**. `17` – **UDP**. `47` – **GRE**. `58` – **ICMPv6**.
`Direction`	Wert des Parameters **Richtung**.	`1` – **Eingehend (Paket)**. `2` – **Ausgehend (Paket)**. `3` – **Eingehend/Ausgehend**. `4` – **Eingehend**. `5` – **Ausgehend**.

Einstellung	Beschreibung	Wert
`IcmpType`	Wert des Parameters **ICMP-Typ**.	**ICMP-Protokoll** `0` – **Echo Reply** (ICMP) oder deaktiviert. `3` – **Destination Unreachable** (ICMP). `4` – **Source Quench**. `5` – **Redirect**. `6` – **Alternate Host Address**. `8` – **Echo Request**. `9` – **Router Advertisement**. `10` – **Router Solicitation**. `11` – **Time Exceeded**. `12` – **Parameter Problem**. `13` – **Timestamp**. `14` – **Timestamp Reply**. `15` – **Information Request**. `16` – **Information Reply**. `17` – **Address Mask Request**. `18` – **Address Mask Reply**. `30` – **Traceroute**. `31` – **Datagram Conversion Error**. `32` – **Mobile Host Redirect**. `33` – **IPv6 Where-Are-You**. `34` – **IPv6 I-Am-Here**. `35` – **Mobile Registration Request**. `36` – **Mobile Registration Reply**. `37` – **Domain Name Request**. `38` – **Domain Name Reply**. `40` – **Photuris**. **ICMPv6-Protokoll** `1` – **Destination Unreachable**. `2` – **Packet Too Big**. `3` – **Time Exceeded**. `4` – **Parameter Problem**. `128` – **Echo Request**. `129` – **Echo Reply**. `130` – **Multicast Listener Query**. `131` – **Multicast Listener Report**. `132` – **Multicast Listener Done**. `133` – **Router Solicitation**. `134` – **Router Advertisement**. `135` – **Neighbor Solicitation**. `136` – **Neighbor Advertisement**. `137` – **Redirect Message**. `138` – **Router Renumbering**. `139` – **ICMP Node Information Query**. `141` – **Inverse Neighbor Discovery Solicitation Message**. `142` – **Inverse Neighbor Discovery Advertisement Message**. `143` – **Version 2 Multicast Listener Report**.

Einstellung	Beschreibung	Wert
		`144` – **Home Agent Address Discovery Request Message**. `145` – **Home Agent Address Discovery Reply Message**. `146` – **Mobile Prefix Solicitation**. `147` – **Mobile Prefix Advertisement**. `148` – **Certification Path Solicitation Message**. `149` – **Certification Path Advertisement Message**. `151` – **Multicast Router Advertisement**. `152` – **Multicast Router Solicitation**. `153` – **Multicast Router Termination**.
`IcmpCode`	Wert des Parameters **ICMP-Code**.	`0` – **Code 0** oder deaktiviert. `1` – **Code 1**. `2` – **Code 2**.
`Flags`	Attributzeiger der Struktur.	Ganze Zahl Es wird empfohlen, diesen Parameter nicht zu verändern.
`TTL`	Wert des Parameters **Lebensdauer (TTL)**.	Wert in Sekunden. Wenn deaktiviert, ist der Wert `0`.
`</key>`		
`Id`	Haupt-ID der Ressource (siehe Knoten `Rules`).	Ganze Zahl
`ParentID`	ID der übergeordneten Gruppe.	Ganze Zahl Es wird empfohlen, diesen Parameter nicht zu verändern.
`Flags`	Status der Regel.	`6` – die Regel ist deaktiviert. `38` – die Regel ist aktiviert.
`Name`	Name der Regel für Netzwerkpakete.	Suchbegriff

Verwendung von Netzwerkregeln für Programme

Kaspersky Endpoint Security ordnet standardmäßig alle Programme, die auf dem Benutzercomputer installiert sind, nach dem Herstellernamen der Programme an, deren Datei- und Netzwerkaktivität kontrolliert wird. Programmgruppen werden nach Sicherheitsgruppen angeordnet. Alle Programme und Programmgruppen erben folgende Eigenschaften der jeweiligen übergeordneten Gruppe: Kontrollregeln für Programme, Netzwerkregeln für das Programm, sowie Ausführungspriorität.

Die Komponenten Programm-Überwachung und Firewall verwenden standardmäßig die Netzwerkregeln für eine Programmgruppe zur Filterung der Netzwerkaktivität aller Programme dieser Gruppe. Die Netzwerkregeln für eine Programmgruppe legen fest, welche Rechte die Programme, die dieser Gruppe angehören, für den Zugriff auf unterschiedliche Netzwerkverbindungen besitzen.

Die Firewall erstellt standardmäßig eine Auswahl von Netzwerkregeln für jede Gruppe von Programmen, die von Kaspersky Endpoint Security auf dem Computer gefunden wurden. Sie können die Firewall-Aktion für die standardmäßig erstellten Netzwerkregeln für eine Programmgruppe ändern. Standardmäßig erstellte Netzwerkregeln für eine Programmgruppe können nicht geändert, gelöscht oder deaktiviert werden. Außerdem ist ihre Priorität unveränderlich.

Sie können eine Netzwerkregel für ein bestimmtes Programm erstellen. Eine solche Regel besitzt eine höhere Priorität als die Netzwerkregel der Gruppe, zu welcher dieses Programm gehört.

Eine Netzwerkregel für das Programm erstellen

Standardmäßig erfolgt die Aktivitätskontrolle für Programme mittels Netzwerkregeln. Diese Regeln werden für die Sicherheitsgruppe angelegt, in die das Programm bei seinem ersten Start von Kaspersky Endpoint Security verschoben wurde. Bei Bedarf können Sie Netzwerkregeln für eine gesamte Sicherheitsgruppe, für ein einzelnes Programm oder für eine Programmgruppe innerhalb einer Sicherheitsgruppe erstellen.

Manuell angelegte Netzwerkregeln haben eine höhere Priorität als Netzwerkregeln, die für eine Sicherheitsgruppe festgelegt wurden. Mit anderen Worten: Wenn manuell angelegte Programmregeln sich von den für die Sicherheitsgruppe festgelegten Programmregeln unterscheiden, überwacht die Firewall die Programmaktivität gemäß den manuell angelegten Programmregeln.

Standardmäßig erstellt die Firewall für jedes Programm die folgenden Netzwerkregeln:

- Jede Netzwerkaktivität in vertrauenswürdigen Netzwerken
- Jede Netzwerkaktivität in lokalen Netzwerken
- Jede Netzwerkaktivität in öffentlichen Netzwerken

Kaspersky Endpoint Security überwacht die Netzwerkaktivität von Programmen wie folgt gemäß vordefinierten Netzwerkregeln:

- „Vertrauenswürdig“ und „Schwach beschränkt“: Alle Netzwerkaktivitäten sind zulässig.
- „Stark beschränkt“ und „Nicht vertrauenswürdig“: Alle Netzwerkaktivitäten sind blockiert.

Vordefinierte Programmregeln können nicht bearbeitet oder gelöscht werden.

Eine Netzwerkregel für das Programm kann auf folgende Arten erstellt werden:

- Verwenden Sie das Tool Netzwerkmonitor.

  Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen. Das ist praktisch, da Sie so nicht alle Regeleinstellungen konfigurieren müssen. Einige Firewall-Einstellungen werden automatisch aus den Daten des Netzwerkmonitors eingefügt. Der Netzwerkmonitor ist nur in der Programmoberfläche verfügbar.

- Konfigurieren Sie die Firewall-Einstellungen.

  Auf diese Weise können Sie die einzelnen Firewall-Einstellungen flexibel anpassen. Sie können Regeln für jede Netzwerkaktivität erstellen, selbst wenn derzeit keine Netzwerkaktivität vorhanden ist.

Beachten Sie beim Erstellen von Netzwerkregeln für Programme, dass Netzwerkpaketregeln Vorrang vor Netzwerkregeln für Programme haben.

Verwendung des Netzwerkmonitors zum Erstellen einer Netzwerkregeln für Programme in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Netzwerkmonitor**.
2. Gehen Sie zur Registerkarte **Netzwerkaktivität** oder **Offene Ports**.

   Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt.

   Auf der Registerkarte **Offene Ports** sind alle geöffneten Ports des Computers aufgelistet.
3. Wählen Sie im Kontextmenü einer Netzwerkverbindung den Punkt **Netzwerkregel für das Programm erstellen**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
4. Wählen Sie die Registerkarte **Netzwerkregeln** aus.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.
5. Klicken Sie auf **Hinzufügen**.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.
6. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.
7. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.
8. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.
9. Klicken Sie auf **Speichern**.

   Die neue Netzwerkregel wird der Liste hinzugefügt.
10. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.
11. Speichern Sie die vorgenommenen Änderungen.

Verwendung der Firewall-Einstellungen zum Erstellen einer Netzwerkregeln für Programme in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.

3. Klicken Sie auf **Regeln für Programme**.

   Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.

4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für die eine Netzwerkregel erstellt werden soll.

5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.

6. Wählen Sie die Registerkarte **Netzwerkregeln** aus.

7. Klicken Sie auf **Hinzufügen**.

   Die Eigenschaften von Netzwerkregeln werden geöffnet.

8. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.

9. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

   Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Vorlage für Netzwerkregel** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

   Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

10. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

11. Klicken Sie auf **Speichern**.

    Die neue Netzwerkregel wird der Liste hinzugefügt.

12. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

13. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Netzwerkregel für Programme in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Basisschutz** → **Firewall**.

4. Klicken Sie im Block **Firewall-Einstellungen** auf **Einstellungen**.

   Eine Liste mit Netzwerkpaketregeln und eine Liste mit Netzwerkregeln für Programme werden geöffnet.

5. Gehen Sie zur Registerkarte **Netzwerkregeln für Programme**.

6. Klicken Sie auf **Hinzufügen**.

7. Geben Sie im angezeigten Fenster die Suchkriterien für das Programm ein, für das eine Netzwerkregel erstellt werden soll.

   Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

8. Klicken Sie auf **Aktualisieren**.

   Kaspersky Endpoint Security sucht in der konsolidierten Liste der auf den verwalteten Computern installierten Programme nach dem Programm. Kaspersky Endpoint Security zeigt eine Liste der Programme an, die Ihren Suchkriterien entsprechen.

9. Wählen Sie das erforderliche Programm.

10. Wählen Sie in der Dropdown-Liste **Ausgewähltes Programm zur Sicherheitsgruppe hinzufügen** den Punkt **Ursprüngliche Gruppen** aus und klicken Sie auf **OK**.

    Das Programm wird der Standardgruppe hinzugefügt.

11. Wählen Sie das gewünschte Programm aus und klicken Sie dann auf **Rechte für Programme** im Kontextmenü des Programms.

    Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.

12. Wählen Sie die Registerkarte **Netzwerkregeln** aus.

    Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.

13. Klicken Sie auf **Hinzufügen**.

    Die Eigenschaften von Netzwerkregeln werden geöffnet.

14. Geben Sie im Feld **Name** manuell den Namen des Netzwerkdienstes ein.

15. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

    Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf die Schaltfläche klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

    Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

16. Aktivieren Sie das Kontrollkästchen **Protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

17. Speichern Sie die Netzwerkregel.

18. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

19. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Netzwerkregel für Programme in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie **Kommunikations- und Web-Schutz** → **Firewall**.

5. Klicken Sie im Block **Programmrechte und geschützte Ressourcen** auf den Link **Rechte für Programme**.

   Das Konfigurationsfenster für Programmrechte mit einer Liste der geschützten Ressourcen wird geöffnet.

6. Gehen Sie zur Registerkarte **Rechte für Programme**.

   Im linken Bereich des Fensters sehen Sie eine Liste mit Sicherheitsgruppen. Im rechten Bereich werden deren Eigenschaften angezeigt.

7. Klicken Sie im Block **Programme** auf **Hinzufügen**.

   Der Assistent zum Hinzufügen eines Programms zu einer Sicherheitsgruppe wird gestartet.

8. Wählen Sie die entsprechende Sicherheitsgruppe für das Programm.

9. Wählen Sie den Typ **Programm** aus. Weiter zum nächsten Schritt

   Wenn Sie eine Netzwerkregel für mehrere Programme erstellen möchten, wählen Sie den Typ der **Gruppe** aus und legen Sie den Namen der Programmgruppe fest.

10. Wählen Sie in der geöffneten Liste mit Programmen die Programme aus, für die eine Netzwerkregel erstellt werden soll.

    Verwenden Sie einen Filter. Sie können den Namen des Programms oder den Namen des Anbieters eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

11. Schließen Sie den Assistenten ab.

    Das Programm wird der Sicherheitsgruppe hinzugefügt.

12. Klicken Sie im linken Fensterbereich auf das gewünschte Programm.

13. Wählen Sie im rechten Fensterbereich in der Dropdown-Liste den Punkt **Netzwerkregeln** aus.

    Diese Registerkarte öffnet eine Liste mit Netzwerkregeln, die standardmäßig von der Firewall erstellt wurden.

14. Klicken Sie auf **Hinzufügen**.

    Die Eigenschaften von Programmregeln werden geöffnet.

15. Geben Sie im Feld **Regelname** manuell den Namen des Netzwerkdienstes ein.

16. Passen Sie die Einstellungen der Netzwerkregel an (s. folgende Tabelle).

    Sie können eine vordefinierte Regelvorlage auswählen, indem Sie auf den Link **Regelvorlage auswählen** klicken. Regelvorlagen beschreiben die am häufigsten verwendeten Netzwerkverbindungen.

    Alle Netzwerkregel-Einstellungen werden automatisch ausgefüllt.

17. Aktivieren Sie das Kontrollkästchen **Ereignisse protokollieren**, damit die Aktion der Netzwerkregel im Bericht aufgezeichnet wird.

18. Speichern Sie die Netzwerkregel.

    Die neue Netzwerkregel wird der Liste hinzugefügt.

19. Verwenden Sie die Schaltfläche **Verschieben**, um die Priorität der Netzwerkregel festzulegen.

20. Speichern Sie die vorgenommenen Änderungen.

Einstellung	Beschreibung
Aktion	**Erlauben**. **Blockieren**.
Protokoll	Überwachen Sie die Netzwerkaktivität über das ausgewählte Protokoll: TCP, UDP, ICMP, ICMPv6, IGMP und GRE. Wurde ICMP oder ICMPv6 als Protokoll gewählt, können Sie Typ und Code des ICMP-Pakets festlegen. Wurde TCP oder UDP als Protokolltyp ausgewählt, können Sie die Portnummern des lokalen Computers und des Remote-Computers angeben, zwischen denen die Verbindung überwacht werden soll. Bereich der möglichen Werte für die Portnummern: 0 bis 65535. Sie können in jedes Feld mehrere, durch `,` getrennte Werte eingeben oder mit `-` einen Wertebereich festlegen. Beispielsweise: • `100,101` • `100-130` • `100,110-130`
Richtung	**Eingehend**. **Eingehend/Ausgehend**. **Ausgehend**.
Remote-Adressen	Netzwerkadressen der Remote-Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegebenen Bereich von Remote-Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen, eine separate Liste mit IP-Adressen erstellen, einen IP-Adressbereich angeben oder ein Subnetz auswählen (Vertrauenswürdige Netzwerke, Lokale Netzwerke, Öffentliche Netzwerke). Anstelle der IP-Adresse können Sie auch den DNS-Namen eines Computers angeben. DNS-Namen sollten nur für LAN-Computer oder interne Dienste verwendet werden. Die Interaktion mit Cloud-Diensten (z. B. Microsoft Azure) und anderen Internetressourcen sollte von der Komponente „Web Control“ abgewickelt werden. Wenn Sie in der Netzwerkpaketregel einen DNS-Namen hinzugefügt haben, für den keine IP-Adresse ermittelt werden konnte, zeigt Kaspersky Endpoint Security eine Warnung an. Web Console: Zur Liste der Regeln für Netzwerkpakete wurde eine Spalte mit einer Fehlerbeschreibung hinzugefügt. In der Verwaltungskonsole (MMC) ist die Fehlerbeschreibung nicht verfügbar. Solche Paketregeln werden farblich hervorgehoben.
Lokale Adressen	Netzwerkadressen der Computer, die Netzwerkpakete senden und/oder empfangen können. Die Firewall wendet diese Netzwerkregel auf den angegeben Bereich von lokalen Netzwerkadressen an. Sie können alle IP-Adressen in eine Netzwerkregel aufnehmen, eine separate Liste mit IP-Adressen erstellen oder einen IP-Adressbereich angeben. Das Programm speichert lokale Adressen nur dann, wenn eine Liste mit Remote-Adressen angegeben ist. Das heißt, der Wert **Adressen aus der Liste** wurde für **Remote-Adressen** ausgewählt und mindestens eine Adresse wurde hinzugefügt. Es ist für Anwendungen nicht immer möglich, die lokale Adresse zu bekommen. In diesem Fall wird diese Einstellung ignoriert.

Netzwerkregel für Programme aktivieren und deaktivieren

Um eine Netzwerkregel für Programme zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.
4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für die eine Netzwerkregel erstellt oder geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.

6. Wählen Sie die Registerkarte **Netzwerkregeln** aus.
7. Wählen Sie in der Liste der Netzwerkregeln dieser Gruppe die entsprechende Netzwerkregel.

   Das Fenster mit den Eigenschaften für Netzwerkregeln wird geöffnet.
8. Legen Sie den Status **Aktiv** oder **Inaktiv** für die Netzwerkregel fest.

   Sie können eine Netzwerkregel für Programmgruppen nicht deaktivieren, wenn sie standardmäßig von der Firewall erstellt wurde.
9. Speichern Sie die vorgenommenen Änderungen.

Firewall-Aktion für die Netzwerkregel für Programme ändern

Sie können die Firewall-Aktion für alle standardmäßig erstellten Netzwerkregeln eines Programms oder einer Programmgruppe ändern, und Sie können die Firewall-Aktion für eine bestimmte manuell erstellte Netzwerkregel eines Programms oder einer Programmgruppe ändern.

Um die Firewall-Aktion für alle Netzwerkregeln eines Programms oder einer Programmgruppe zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.
4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, wenn Sie die Firewall-Aktion für alle entsprechenden standardmäßig erstellten Netzwerkregeln ändern möchten. Manuell erstellte Netzwerkregeln bleiben unverändert.
5. Klicken Sie mit der rechten Maustaste, um das Kontextmenü zu öffnen, wählen Sie **Netzwerkregeln** und dann die Aktion, die Sie zuordnen möchten:
   - **Erben**.
   - **Erlauben**.
   - **Blockieren**.
6. Speichern Sie die vorgenommenen Änderungen.

Um die Firewall-Aktion für eine Netzwerkregel eines Programms oder einer Programmgruppe zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.

4. Wählen Sie in der Liste ein Programm oder eine Programmgruppe, für welche die Aktion einer Netzwerkregel geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
6. Wählen Sie die Registerkarte **Netzwerkregeln** aus.
7. Wählen Sie die Netzwerkregel, für welche Sie die Firewall-Aktion ändern möchten.
8. Klicken Sie mit der rechten Maustaste auf die Spalte **Erlaubnis** und wählen Sie die gewünschte Aktion:
   - **Erben**.
   - **Erlauben**.
   - **Verbieten**.
   - **Ereignisse protokollieren**.
9. Speichern Sie die vorgenommenen Änderungen.

Priorität der Netzwerkregel für Programme ändern

Die Ausführungspriorität einer Netzwerkregel wird durch ihre Position in der Liste der Netzwerkregeln bestimmt. Die Firewall führt die Regeln in der Reihenfolge aus, in der sie auf der Liste der Netzwerkregeln stehen (von oben nach unten). Entsprechend jeder Netzwerkregel, die verarbeitet und auf eine bestimmte Netzwerkverbindung angewendet wurde, erlaubt oder verbietet die Firewall den Netzwerkzugriff auf die Adressen und Ports, die in den Einstellungen dieser Netzwerkverbindung angegeben sind.

Manuell erstellte Netzwerkregeln besitzen eine höhere Priorität als standardmäßig erstellte Netzwerkregeln.

Sie können die Priorität von manuell erstellten Netzwerkregeln für Programmgruppen nicht ändern.

Um die Priorität einer Netzwerkregel zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Basisschutz** → **Firewall** aus.
3. Klicken Sie auf **Regeln für Programme**.

   Dies öffnet die Liste der Regeln für Programme.
4. Wählen Sie in der Programmliste ein Programm oder eine Programmgruppe, für welche die Priorität der Netzwerkregel geändert werden soll.
5. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie den Punkt **Details und Regeln**.

   Das Fenster mit den Regeln und Eigenschaften für Programme wird geöffnet.
6. Wählen Sie die Registerkarte **Netzwerkregeln** aus.
7. Wählen Sie die Netzwerkregel, deren Priorität Sie ändern möchten.

8. Verwenden Sie die Schaltflächen **Aufwärts**/**Abwärts**, um die Priorität der Netzwerkregel festzulegen.

9. Speichern Sie die vorgenommenen Änderungen.

Netzwerkmonitor

Der *Netzwerkmonitor* dient dazu, in Echtzeit Informationen über die Netzwerkaktivität des Benutzercomputers anzuzeigen.

Gehen Sie folgendermaßen vor, um den Netzwerkmonitor zu starten:

Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Netzwerkmonitor**.

Das Fenster „Netzwerkmonitor“ wird geöffnet. Dieses Fenster bietet vier Registerkarten mit Informationen zu den Netzwerkaktivitäten des Benutzercomputers:

- Auf der Registerkarte **Netzwerkaktivität** werden alle momentan aktiven Netzverbindungen des Computers angezeigt. Es werden sowohl eingehende als auch ausgehende, vom Benutzercomputer initiierte Netzverbindungen dargestellt. Auf dieser Registerkarte können Sie auch Netzwerkpaketregeln für den Firewall-Betrieb erstellen.
- Auf der Registerkarte **Offene Ports** sind alle geöffneten Ports des Computers aufgelistet. Auf dieser Registerkarte können Sie auch Netzwerkpaketregeln und Programmregeln für den Firewall-Betrieb erstellen.
- Auf der Registerkarte **Netzwerkverkehr** wird das Volumen des ein- und ausgehenden Netzwerkverkehrs zwischen dem lokalen Computer und anderen Computern des Netzwerks angezeigt, in dem der Computer momentan arbeitet.
- Auf der Registerkarte **Blockierte Computer** sind die IP-Adressen jener Remote-Computer aufgelistet, von deren IP-Adresse versuchte Netzwerkangriffe erkannt wurden und deren Netzwerkaktivität deshalb von der Komponente „Schutzes vor Netzwerkbedrohungen“ blockiert wurde.

Exploit-Prävention

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.

Exploit-Prävention aktivieren und deaktivieren

Die „Exploit-Prävention“ ist standardmäßig aktiviert und verwendet den optimalen Modus. Kaspersky Endpoint Security überwacht ausführbare Dateien, die von verwundbaren Anwendungen ausgeführt werden. Wenn Kaspersky Endpoint Security erkennt, dass eine ausführbare Datei aus einem verwundbaren Programm nicht vom Benutzer gestartet wurde, führt Kaspersky Endpoint Security die ausgewählte Aktion aus (beispielsweise wird der Vorgang blockiert).

So aktivieren oder deaktivieren Sie die „Exploit-Prävention“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Exploit-Prävention** aus.
4. Verwenden Sie das Kontrollkästchen **Exploit-Prävention**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Wählen Sie die entsprechende Aktion im Block **Wenn ein Exploit erkannt wird**:
   - **Verbieten**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält.
   - **Informieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über den Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die „Exploit-Prävention“ über die Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Exploit-Prävention**.
5. Verwenden Sie den Schalter **Exploit-Prävention**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Wählen Sie die entsprechende Aktion im Block **Aktion beim Fund einer Bedrohung**:

   - **Blockieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält.

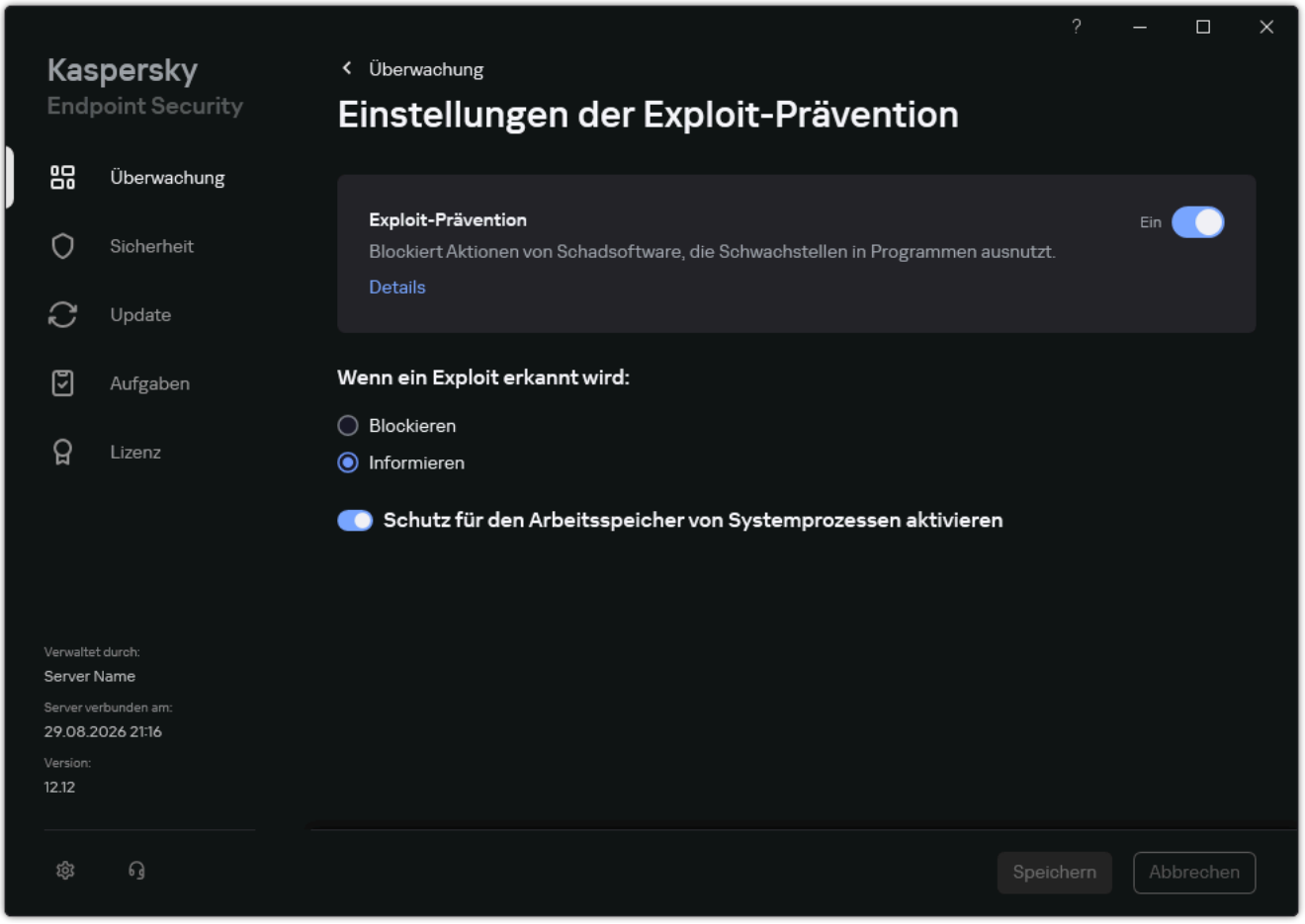
   - **Informieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über den Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die „Exploit-Prävention“ über die App-Oberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Exploit-Prävention** aus.



Einstellungen zur Exploit-Prävention

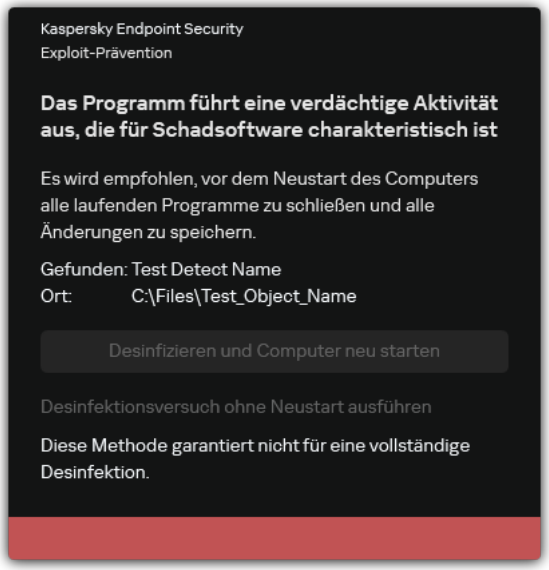
3. Verwenden Sie den Schalter **Exploit-Prävention**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Wählen Sie die entsprechende Aktion im Block **Wenn ein Exploit erkannt wird**:

   - **Blockieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält.

   - **Informieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über den Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.

5. Speichern Sie die vorgenommenen Änderungen.



Benachrichtigung über eine aktive Bedrohung

Schutz für den Arbeitsspeicher von Systemprozessen

Der Schutz für den Arbeitsspeicher von Systemprozessen ist standardmäßig aktiviert. Kaspersky Endpoint Security blockiert externe Prozesse, die versuchen, Zugriff auf Systemprozesse zu erhalten.

So aktivieren oder deaktivieren Sie über die Verwaltungskonsole (MMC) den Schutz für den Arbeitsspeicher von Systemprozessen

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Exploit-Prävention** aus.

4. Verwenden Sie das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**, um die Option zu aktivieren oder deaktivieren.

5. Speichern Sie die vorgenommenen Änderungen.

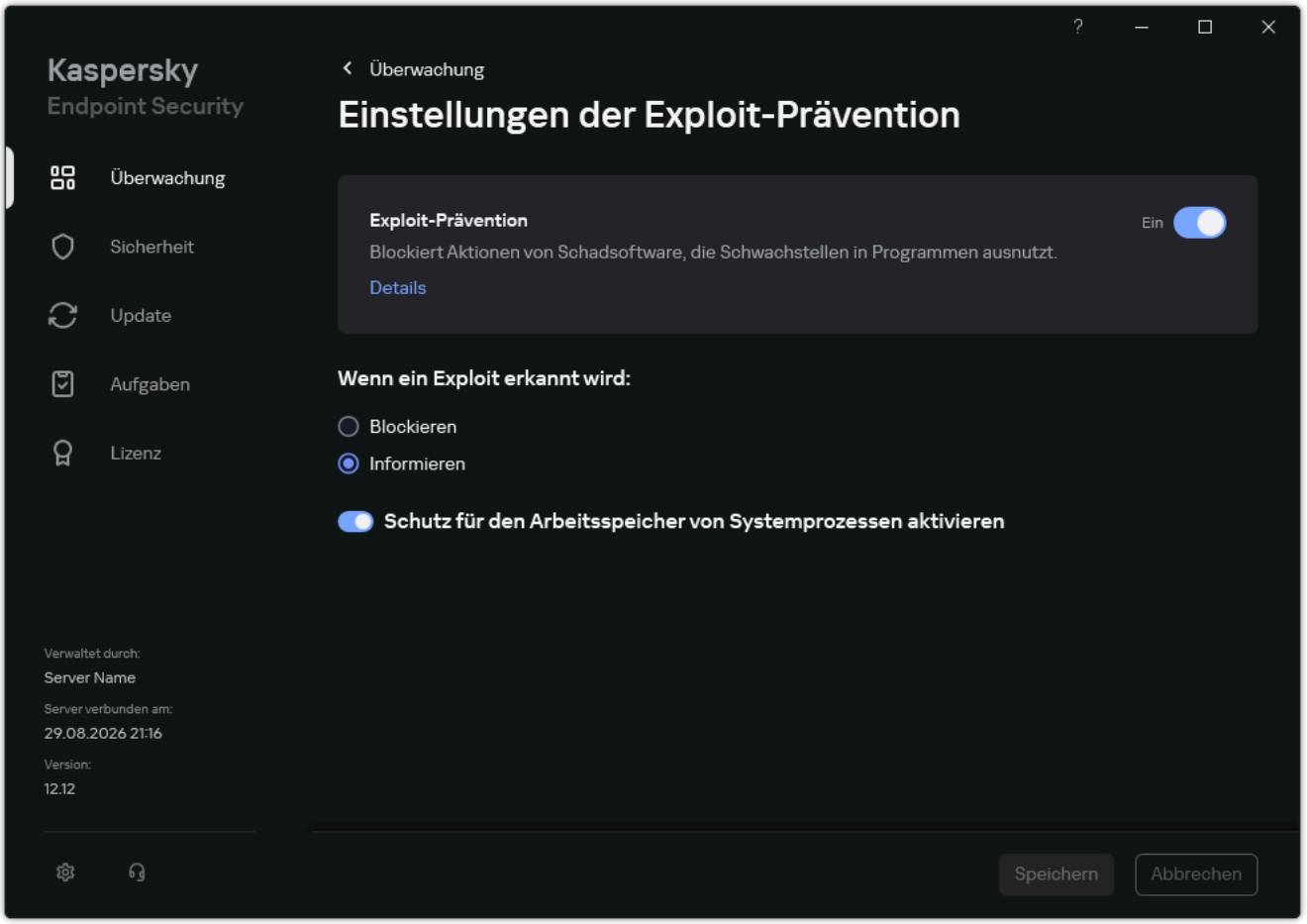
So aktivieren oder deaktivieren Sie über die Web Console und Cloud Console den Schutz für den Arbeitsspeicher von Systemprozessen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Exploit-Prävention**.
5. Verwenden Sie den Schalter **Schutz des Arbeitsspeichers von Systemprozessen AKTIVIERT**, um diese Funktion zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie über die App-Oberfläche den Schutz für den Arbeitsspeicher von Systemprozessen

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Exploit-Prävention** aus.



Einstellungen zur Exploit-Prävention

3. Verwenden Sie den Schalter **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**, um diese Funktion zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Verhaltensanalyse

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.

Die Verhaltensanalyse ist standardmäßig aktiviert und läuft in dem Modus, der von Kaspersky empfohlen wird. Wenn eine schädliche Aktivität erkannt wird, löscht Kaspersky Endpoint Security die ausführbare Datei des schädlichen Programms.

Es wird davor gewarnt, die Verhaltensanalyse ohne triftigen Grund zu deaktivieren, da dies die Effektivität der Schutzkomponenten beeinträchtigt. Die Schutzkomponenten können die von der Verhaltensanalyse empfangenen Daten abfragen, um Bedrohungen zu erkennen.

So aktivieren oder deaktivieren Sie die Verhaltensanalyse (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Verhaltensanalyse** aus.
5. Verwenden Sie das Kontrollkästchen **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Wählen Sie die entsprechende Aktion im Block **Aktion, wenn Schadsoftware-Aktivität erkannt wird**:
   - **Löschen**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.
   - **Blockieren**. Wenn dieses Element gewählt wird, beendet Kaspersky Endpoint Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.
   - **Informieren**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Endpoint Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die Verhaltensanalyse (in der Web Console und Cloud Console)

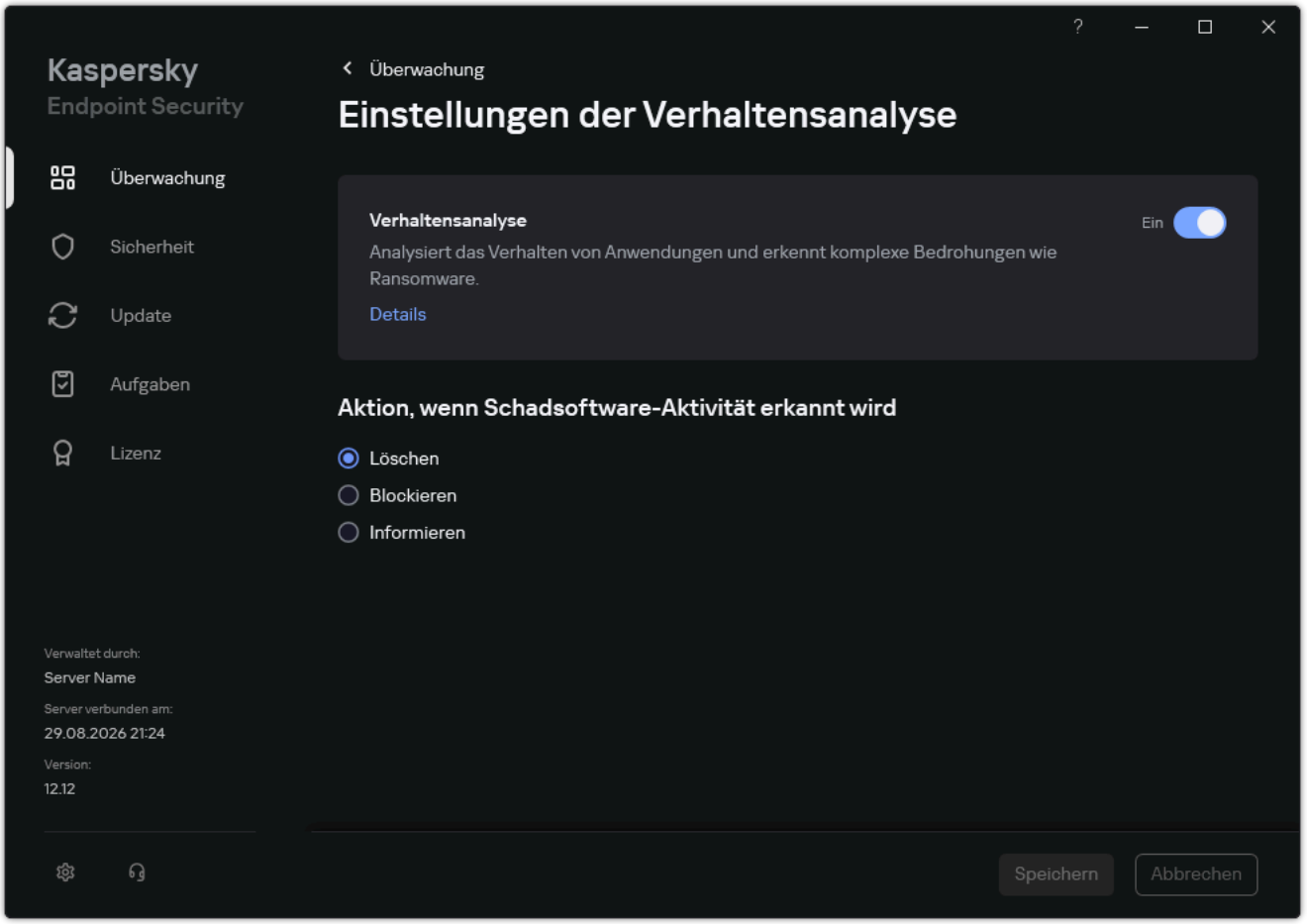
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Verhaltensanalyse**
5. Verwenden Sie den Schalter **Verhaltensanalyse AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Wählen Sie die entsprechende Aktion im Block **Aktion beim Fund einer Bedrohung**:

   - **Löschen**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.
   - **Blockieren**. Wenn dieses Element gewählt wird, beendet Kaspersky Endpoint Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.
   - **Informieren**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Endpoint Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die Verhaltensanalyse (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Verhaltensanalyse** aus.



Einstellungen der Verhaltensanalyse

3. Verwenden Sie den Schalter **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Wählen Sie die entsprechende Aktion im Block **Aktion, wenn Schadsoftware-Aktivität erkannt wird**:

   - **Löschen**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.
   - **Blockieren**. Wenn dieses Element gewählt wird, beendet Kaspersky Endpoint Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.
   - **Informieren**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Endpoint Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.

5. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verhaltensanalyse aktiviert ist, verwendet Kaspersky Endpoint Security daher Vorlagen für gefährliches Verhalten, um die Aktivität von Programmen im Betriebssystem zu analysieren.

Schutz vor Verschlüsselung

Der Schutz vor der externen Verschlüsselung freigegebener Ordner, der bisher Teil der Komponente „Verhaltensanalyse“ war, wird ab Kaspersky Endpoint Security 12.12 für Windows von der separaten Komponente Schutz vor Verschlüsselung übernommen.

Die Komponente gewährleistet die Vorgangsnachverfolgung nur für jene Dateien, die sich auf Massenspeichergeräten mit NTFS-Dateisystem befinden und die nicht mit einem EFS-System verschlüsselt wurden.

Die Komponente „Schutz vor Verschlüsselung“ analysiert die Aktivität in freigegebenen Ordnern. 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.

Damit die Komponente „Schutz vor Verschlüsselung“ funktioniert, müssen Sie die Komponente „Verhaltensanalyse“ aktivieren.

Wenn Kaspersky Endpoint Security einen Versuch erkennt, Dateien in freigegebenen Ordnern zu verändern, führt das Programm die folgenden Aktionen aus:

- Blockiert den Zugriff auf Datei-Änderungen für die Sitzung, die durch die bösartige Aktivität initiiert wurde (die Datei ist schreibgeschützt).
- Erstellung von Backup-Kopien der Dateien, die geändert wurden.
- Fügt einen Eintrag zu den Berichten der lokalen Programmoberfläche hinzu und sendet Informationen über eine erkannte schädliche Aktivität an Kaspersky Security Center.
- Ist dabei die Komponente „Rollback von schädlichen Aktionen“ aktiviert, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.

Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren und deaktivieren

Der Schutz vor der externen Verschlüsselung freigegebener Ordner ist standardmäßig aktiviert und funktioniert, wie von den Kaspersky-Experten empfohlen. Um diese Funktionalität zu konfigurieren, können Sie bei Bedarf einen Schutzbereich erstellen und Ausnahmen festlegen. Standardmäßig werden freigegebene Ordner automatisch identifiziert und die Dateiaktivität wird in allen Ordnern überwacht. Wenn ein Versuch erkannt wird, Dateien in freigegebenen Ordnern extern zu verschlüsseln, blockiert Kaspersky Endpoint Security die Sitzung des Remote-Benutzers für eine Stunde (Standardeinstellung).

Die Funktion für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist nach der Installation von Kaspersky Endpoint Security bis zum Neustart des Computers beschränkt.

So aktivieren oder deaktivieren Sie den Schutz von freigegebenen Ordnern vor externer Verschlüsselung in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Schutz vor Verschlüsselung** aus.
4. Verwenden Sie das Kontrollkästchen **Schutz vor Verschlüsselung**, um die Erkennung von Aktivitäten zu aktivieren oder zu deaktivieren, die für externe Verschlüsselung typisch sind.
5. Wählen Sie aus, welche Aktion das Programm ausführen soll, wenn versucht wird, Dateien in freigegebenen Ordnern zu verändern:
   - **Verbindung blockieren für n Minuten**. Ist diese Option ausgewählt und Kaspersky Endpoint Security erkennt einen Versuch, Dateien in gemeinsamen Ordnern zu ändern, so blockiert die App den Zugriff auf die Dateiänderung für die Sitzung, die die schädliche Aktivität initiiert hat, und erstellt Backup-Kopien der veränderten Dateien.

     Ist die Komponente „Rollback von schädlichen Aktionen“ aktiviert und die Option **Verbindung blockieren für n Minuten** ausgewählt, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.

   - **Informieren**. Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch zur Änderung von Dateien in freigegebenen Ordnern erkennt, fügt das Programm Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über eine erkannte schädliche Aktivität an Kaspersky Security Center.
6. Bei Bedarf können Sie einen Schutzbereich bearbeiten und Ausnahmen festlegen.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Schutz von freigegebenen Ordnern vor externer Verschlüsselung in der Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz → Verhaltensanalyse → Schutz vor Verschlüsselung**.
5. Verwenden Sie den Schalter **Schutz vor Verschlüsselung AKTIVIERT**, um die Erkennung von Aktivitäten, die für externe Verschlüsselung typisch sind, zu aktivieren oder zu deaktivieren.

6. Wählen Sie aus, welche Aktion das Programm ausführen soll, wenn versucht wird, Dateien in freigegebenen Ordnern zu verändern:

   - **Verbindung blockieren für (Min.) n Minuten**. Ist diese Option ausgewählt und Kaspersky Endpoint Security erkennt einen Versuch, Dateien in gemeinsamen Ordnern zu ändern, so blockiert die App den Zugriff auf die Dateiänderung für die Sitzung, die die schädliche Aktivität initiiert hat, und erstellt Backup-Kopien der veränderten Dateien.

     Ist die Komponente „Rollback von schädlichen Aktionen“ aktiviert und die Option **Verbindung blockieren für (Min.) n Minuten** ausgewählt, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.

   - **Informieren**. Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch zur Änderung von Dateien in freigegebenen Ordnern erkennt, fügt das Programm Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über eine erkannte schädliche Aktivität an Kaspersky Security Center.

7. Bei Bedarf können Sie einen Schutzbereich bearbeiten und Ausnahmen festlegen.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Schutz von freigegebenen Ordnern vor externer Verschlüsselung in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz → Schutz vor Verschlüsselung** aus.

3. Verwenden Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung freigegebener Ordner**, um die Erkennung von Aktivitäten zu aktivieren oder zu deaktivieren, die für externe Verschlüsselung typisch sind.

4. Verwenden Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung freigegebener Ordner**, um die Erkennung von Aktivitäten zu aktivieren oder zu deaktivieren, die für externe Verschlüsselung typisch sind.

5. Wählen Sie aus, welche Aktion das Programm ausführen soll, wenn versucht wird, Dateien in freigegebenen Ordnern zu verändern:

   - **Verbindung blockieren für (Min.) n Minuten**. Ist diese Option ausgewählt und Kaspersky Endpoint Security erkennt einen Versuch, Dateien in gemeinsamen Ordnern zu ändern, so blockiert die App den Zugriff auf die Dateiänderung für die Sitzung, die die schädliche Aktivität initiiert hat, und erstellt Backup-Kopien der veränderten Dateien.

     Ist die Komponente „Rollback von schädlichen Aktionen“ aktiviert und die Option **Verbindung blockieren für (Min.) n Minuten** ausgewählt, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.

   - **Informieren**. Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch zur Änderung von Dateien in freigegebenen Ordnern erkennt, fügt das Programm Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über eine erkannte schädliche Aktivität an Kaspersky Security Center.

6. Bei Bedarf können Sie einen Schutzbereich bearbeiten und Ausnahmen festlegen.

7. Speichern Sie die vorgenommenen Änderungen.

Sperrdauer für einen nicht vertrauenswürdigen Computer konfigurieren

Ein *nicht vertrauenswürdiger Computer* ist ein Remote-Computer, der bösartige Aktivitäten ausführt oder Daten verschlüsselt. Kaspersky Endpoint Security blockiert die Sitzung des Remote-Benutzers standardmäßig für eine Stunde. Nach Ablauf der Sperrdauer entfernt Kaspersky Endpoint Security den Computer aus der Sperrliste und stellt den Zugriff auf den freigegebenen Ordner wieder her.

So konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Schutz vor Verschlüsselung** aus.

4. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Option **Verbindung blockieren für n Min.** aus.

5. Konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer, der schädliche Aktivitäten ausführt oder Daten verschlüsselt.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer in der Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz → Verhaltensanalyse → Schutz vor Verschlüsselung**.

5. Konfigurieren Sie unter **Aktion beim Fund einer Bedrohung** die Sperrdauer für einen nicht vertrauenswürdigen Computer, der bösartige Aktivitäten ausführt oder Daten verschlüsselt.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz → Schutz vor Verschlüsselung** aus.

3. Wählen Sie im Block **Aktion beim Fund einer Bedrohung** die Variante **Verbindung blockieren für (Min.)** aus.

4. Konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer, der schädliche Aktivitäten ausführt oder Daten verschlüsselt.

5. Speichern Sie die vorgenommenen Änderungen.

Daraufhin wird der Remote-Computer gesperrt. Um den Remote-Computer zu entsperren, können Sie Kaspersky Endpoint Security neu starten.

Schutzbereich bearbeiten

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.

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. Beispielsweise kann die „Verhaltensanalyse“ Fehlalarme auslösen, wenn der Benutzer in einem gemeinsamen Ordner Dateien mit der Erweiterung ENC verwendet. Diese Aktivität gleicht einem Verhaltensmuster, das für externe Verschlüsselung charakteristisch ist. Wenn Sie zu Datenschutzzwecken verschlüsselte Dateien in einem gemeinsamen Ordner ablegen, fügen Sie diesen Ordner den Ausnahmen hinzu.

> Sie können auch Computer ausschließen, von denen Versuchen zur externen Verschlüsselung nicht verarbeitet werden sollen.

So bearbeiten Sie einen Schutzbereich in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Schutz vor Verschlüsselung** aus.

4. Wählen Sie im Block **Schutzbereich** die Variante **Nur die angegebenen freigegebenen Ordner** aus.

5. Klicken Sie in der Ordnerliste auf **Hinzufügen**.

6. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Pfad des freigegebenen Ordners ein, den Sie in den Schutzbereich aufnehmen möchten (z. B. `C:\Share`).

   > Um einen freigegebenen Ordner zum Schutzbereich hinzuzufügen, verwenden Sie einen lokalen Pfad.

7. Klicken Sie auf **OK**.

8. Legen Sie bei Bedarf Ausnahmen für den Schutzbereich fest:

   a. Klicken Sie im Block **Untersuchungsausnahmen** auf **Nach Maske**.

   b. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

c. Geben Sie im angezeigten Fenster eine Dateierweiterung im Format `*.<file extension>` oder einen Ordnerpfad an. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Einige Dateierweiterungen werden vom Programm nicht für Ausnahmen unterstützt. Daher können Sie eine Ausnahme als `*.docx` oder `**\Folder\**` angeben.

Sie können ein Objekt von der Untersuchung ausschließen, ohne es aus der Liste der Objekte im Schutzbereich zu entfernen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

9. Speichern Sie die vorgenommenen Änderungen.

So bearbeiten Sie den Schutzbereich in der Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Schutz vor Verschlüsselung**.
5. Wählen Sie im Block **Schutzbereich** die Variante **Nur die angegebenen freigegebenen Ordner** aus.
6. Klicken Sie in der Ordnerliste auf **Hinzufügen**.
7. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Pfad des freigegebenen Ordners ein, den Sie in den Schutzbereich aufnehmen möchten (z. B. `C:\Share`).

   Um einen freigegebenen Ordner zum Schutzbereich hinzuzufügen, verwenden Sie einen lokalen Pfad.
8. Klicken Sie auf **OK**.
9. Legen Sie bei Bedarf Ausnahmen für den Schutzbereich fest:

   a. Klicken Sie im oberen Fensterbereich auf den Link **Untersuchungsausnahmen**.

   b. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

   c. Geben Sie im angezeigten Fenster eine Dateierweiterung im Format `*.<file extension>` oder einen Ordnerpfad an. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

   Einige Dateierweiterungen werden vom Programm nicht für Ausnahmen unterstützt. Daher können Sie eine Ausnahme als `*.docx` oder `**\Folder\**` angeben.

   Sie können ein Objekt von der Untersuchung ausschließen, ohne es aus der Liste der Objekte im Schutzbereich zu entfernen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.
10. Speichern Sie die vorgenommenen Änderungen.

So bearbeiten Sie einen Schutzbereich in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Schutz vor Verschlüsselung** aus.

3. Wählen Sie im Block **Schutzbereich** die Variante **Nur die angegebenen freigegebenen Ordner** aus.

4. Klicken Sie in der Ordnerliste auf **Hinzufügen**.

5. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Pfad des freigegebenen Ordners ein, den Sie in den Schutzbereich aufnehmen möchten (z. B. `C:\Share`).

   Um einen freigegebenen Ordner zum Schutzbereich hinzuzufügen, verwenden Sie einen lokalen Pfad.

6. Klicken Sie auf **OK**.

7. Legen Sie bei Bedarf Ausnahmen für den Schutzbereich fest:

   a. Klicken Sie im oberen Fensterbereich auf den Link **Ausnahmen nach Maske**.

   b. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

   c. Geben Sie im angezeigten Fenster eine Dateierweiterung im Format `*.<file extension>` oder einen Ordnerpfad an. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

      Einige Dateierweiterungen werden vom Programm nicht für Ausnahmen unterstützt. Daher können Sie eine Ausnahme als `*.docx` oder `**\Folder\**` angeben.

   Sie können ein Objekt von der Untersuchung ausschließen, ohne es aus der Liste der Objekte im Schutzbereich zu entfernen. Deaktivieren Sie dazu das Kontrollkästchen neben dem Objekt.

8. Speichern Sie die vorgenommenen Änderungen.

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.

3. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.

4. Klicken Sie auf **Hinzufügen**.

5. Klicken Sie auf **Durchsuchen** und wählen Sie den gemeinsamen Ordner aus.

Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

- 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` funktioniert nicht.

- 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.

Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `?:\Users\*\Folder\` ein.

6. Wählen Sie im Block **Schutzkomponenten** die Komponente **Verhaltensanalyse** aus.

7. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

8. Wählen Sie den Status **Aktiv** für die Ausnahme.

   Über den Schalter können Sie eine Ausnahme jederzeit stoppen.

9. Speichern Sie die vorgenommenen Änderungen.

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.

5. Klicken Sie im folgenden Fenster auf den Link **Ausnahmen für die Schadsoftware-Untersuchung**.

6. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.

7. Markieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn dieses Kontrollkästchen deaktiviert ist, blendet Kaspersky Endpoint Security die konsolidierte Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus.

8. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können Untersuchungsausnahmen in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens eine Untersuchungsausnahme hinzu.

   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält das Programm *vordefinierte Untersuchungsausnahmen*. Außerdem wurden vordefinierte Untersuchungsausnahmen hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte Untersuchungsausnahmen auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

9. Wählen Sie aus, wie Sie die Ausnahme hinzufügen möchten: **Datei- oder Ordnerpfad**.

10. Geben Sie den Pfad des freigegebenen Ordners ein.

    Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

    - 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` funktioniert nicht.

    - 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.

    Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `C:\Users\*\Folder\` ein.

11. Wählen Sie im Block **Ausnahme anwenden auf** die Komponente **Verhaltensanalyse** aus.

12. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

13. Wählen Sie den Status **Zu Ausnahmen hinzufügen** für die Ausnahme.

    Über den Schalter können Sie eine Ausnahme jederzeit stoppen.

14. Speichern Sie die vorgenommenen Änderungen.

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.

4. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme → Untersuchungsausnahmen** auf **Einstellungen**.

   Dies öffnet ein Fenster mit einer Liste der Ausnahmen.

5. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.

6. Markieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn dieses Kontrollkästchen deaktiviert ist, blendet Kaspersky Endpoint Security die konsolidierte Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus.

7. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können Untersuchungsausnahmen in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens eine Untersuchungsausnahme hinzu.

   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält das Programm *vordefinierte Untersuchungsausnahmen*. Außerdem wurden vordefinierte Untersuchungsausnahmen hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte Untersuchungsausnahmen auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

8. Klicken Sie auf **Hinzufügen**.

9. Aktivieren Sie im Block **Eigenschaften** das Kontrollkästchen **Datei oder Ordner**.

10. Mit dem Link **Wählen Sie eine Datei oder einen Ordner aus** im Block **Beschreibung der Untersuchungsausnahme (zum Ändern auf unterstrichene Elemente klicken)** wird das Fenster **Datei- oder Ordnername** geöffnet.

11. Klicken Sie auf **Durchsuchen** und wählen Sie den gemeinsamen Ordner aus.

    Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

    - 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` funktioniert nicht.

    - 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.

    Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `?:\Users\*\Folder\` ein.

12. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

13. Klicken Sie auf den Link im Block **Beschreibung der Untersuchungsausnahme (zum Ändern auf unterstrichene Elemente klicken)**, um das Fenster **Schutzkomponenten** zu öffnen.

14. Aktivieren Sie das Kontrollkästchen neben der Komponente **Verhaltensanalyse**.

15. Speichern Sie die vorgenommenen Änderungen.

Vertrauenswürdige Computer für die externe Datenverschlüsselung hinzufügen

Wenn Ihr Unternehmen für die Dateiübermittlung die Verschlüsselung externer Daten verwendet, müssen Sie eine Liste mit vertrauenswürdigen Computern erstellen. Die Datenverschlüsselung durch vertrauenswürdige Computer wird von Kaspersky Endpoint Security nicht überwacht.

Damit die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, funktioniert, muss der Dienst für die Anmeldungsüberwachung aktiviert werden. Der Dienst für die Anmeldungsüberwachung ist standardmäßig deaktiviert (weitere Informationen über die Aktivierung der Anmeldungsüberwachung finden Sie auf der Website der Microsoft Corporation).

Die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, funktioniert nicht, wenn der betreffende Remote-Computer bereits vor dem Start von Kaspersky Endpoint Security eingeschaltet war. Sie können diesen Remote-Computer nach dem Start von Kaspersky Endpoint Security neu starten, damit die Funktionalität, mit der Adressen aus dem Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ausgeschlossen werden können, auf diesem Remote-Computer funktioniert.

So fügen Sie in der Verwaltungskonsole (MMC) einen vertrauenswürdige Computer für die externe Datenverschlüsselung hinzu

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Schutz vor Verschlüsselung** aus.
5. Klicken Sie im Block **Untersuchungsausnahmen** auf **Nach Name oder IP-Adresse**.
6. Klicken Sie im angezeigten Fenster auf **Nach Name oder IP-Adresse**.
7. Geben Sie die IP-Adressen, den IP-Adressbereich oder die Namen der Computers ein, deren Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.

   Beispiele:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`

- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie in der Kaspersky Security Center Web Console einen vertrauenswürdigen Computer für die externe Verschlüsselung von Daten hinzu

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.
5. Klicken Sie im rechten Fensterbereich auf den Link **Ausnahmen für den Schutz vor Verschlüsselung**.
6. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
7. Geben Sie die IP-Adressen, den IP-Adressbereich oder die Namen der Computers ein, deren Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.

   Beispiele:

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie in der Programmoberfläche einen vertrauenswürdigen Computer für die externe Datenverschlüsselung hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Schutz vor Verschlüsselung** aus.
3. Klicken Sie im oberen Fensterbereich auf den Link **Ausnahmen nach Name oder IP-Adresse**.
4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
5. Geben Sie die IP-Adressen, den IP-Adressbereich oder die Namen der Computers ein, deren Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.

Beispiele:

- `192.168.0.0 - 192.168.255.255`
- `192.168.0.0/24`
- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren einer Liste der Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern

Sie können die Liste der Ausnahmen in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Adressen desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup für die Listen der Erweiterungen anzulegen oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Ausnahmen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Schutz vor Verschlüsselung** aus.
4. Klicken Sie im Block **Untersuchungsausnahmen** auf **Nach Name oder IP-Adresse**.
5. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Ausnahmen in die XML-Datei.

6. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf die Schaltfläche → **Importieren**.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   c. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste der Ausnahmen in der Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Schutz vor Verschlüsselung**.
5. Klicken Sie auf den Link **Ausnahmen nach Name oder IP-Adresse**.
6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

      Kaspersky Endpoint Security exportiert die Liste der Ausnahmen in eine json-Datei im standardmäßigen Download-Ordner.

7. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der JSON-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen" kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem verarbeitet Kaspersky Endpoint Security folgende Typen von schädlicher Programmaktivität:

- **Dateiaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht ausführbare Dateien, die von Schadsoftware erstellt wurden (auf allen Datenträgern, außer auf Netzlaufwerken).
  - löscht ausführbare Dateien, die von Programmen erstellt wurden, in welche Schadsoftware eingedrungen ist.
  - stellt Dateien wieder her, die von Schadsoftware verändert oder gelöscht wurden.

  Die Funktionalität zur Wiederherstellung von Dateien besitzt bestimmte Beschränkungen.

- **Aktivität der Registrierung**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden.
  - stellt Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden, nicht wieder her.

- **Systemaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - beendet Prozesse, die von Schadsoftware gestartet wurden.
  - beendet Prozesse, in die Schadsoftware eingedrungen ist.
  - stellt Prozesse, die von Schadsoftware beendet wurden, nicht wieder her.

- **Netzwerkaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - verbietet die Netzwerkaktivität von Schadsoftware.
  - verbietet die Netzwerkaktivität von Prozessen, in die Schadsoftware eingedrungen ist.

Ein Rollback von Schadsoftware-Aktionen kann entweder von der Komponente Schutz vor bedrohlichen Dateien, Verhaltensanalyse oder bei einer Schadsoftware-Untersuchung gestartet werden.

Das Rollback der Aktionen schädlicher Programme betrifft lediglich eine eng eingeschränkte Auswahl an Daten. Ein Rollback hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und die Integrität der Daten auf Ihrem Computer.

So aktivieren und deaktivieren Sie die Komponente „Rollback von schädlichen Aktionen“ in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Rollback von schädlichen Aktionen** aus.

4. Verwenden Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, um die Komponente zu aktivieren oder zu deaktivieren.

5. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Rollback von schädlichen Aktionen“ in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Host-Schutz** → **Verhaltensanalyse** → **Rollback von schädlichen Aktionen**.

5. Verwenden Sie den Schalter **Rollback von schädlichen Aktionen AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und deaktivieren Sie die Komponente „Rollback von schädlichen Aktionen“ in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Rollback von schädlichen Aktionen** aus.

3. Verwenden Sie den Schalter **Rollback von schädlichen Aktionen**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Wenn Rollback von schädlichen Aktionen aktiviert ist, rollt Kaspersky Endpoint Security die von bösartigen Programmen im Betriebssystem ausgeführten Aktionen zurück.

Kaspersky Security Network



Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Für den Empfang dieser Daten ist Kaspersky Security Network vorgesehen.

Die KSN-Funktionalität ist im Programm in den USA möglicherweise nicht verfügbar

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. 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 Konfiguration des Zugriffs auf KSN 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.

Ausführliche Informationen darüber, welche statistischen Informationen, die während der Teilnahme an KSN generiert werden, an Kaspersky gesendet werden und wie solche Informationen gespeichert und gelöscht werden, finden Sie in der Erklärung zu Kaspersky Security Network und auf der Kaspersky-Website. 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 Arbeit mit Kaspersky-Reputationsdatenbanken:

- 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.

  - Die Übertragung von Daten aus dem Land ihres Standorts oder aus dem Unternehmens-LAN ist rechtlich oder durch Unternehmenssicherheitsrichtlinien untersagt.

Verwendung von Kaspersky Security Network aktivieren und deaktivieren

Kaspersky Endpoint Security verwendet standardmäßig den erweiterten KSN-Modus. Im *erweiterten KSN-Modus* überträgt Kaspersky Endpoint Security zusätzliche Daten an Kaspersky.

So aktivieren oder deaktivieren Sie die KSN-Nutzung (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Kaspersky Security Network** aus.
4. Verwenden Sie den Schalter **Kaspersky Security Network**, um die Komponente zu aktivieren oder zu deaktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Endpoint Security die Erklärung zu Kaspersky Security Network an. Bitte lesen und akzeptieren Sie die Nutzungsbedingungen von Kaspersky Security Network (KSN), wenn Sie damit einverstanden sind.
5. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Erweiterten KSN-Modus aktivieren**. Der erweiterte KSN-Modus ist standardmäßig aktiviert.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die KSN-Nutzung (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Kaspersky Security Network**.
5. Verwenden Sie den Schalter **Verwendung von Kaspersky Security Network (KSN) AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Endpoint Security die Erklärung zu Kaspersky Security Network an. Bitte lesen und akzeptieren Sie die Nutzungsbedingungen von Kaspersky Security Network (KSN), wenn Sie damit einverstanden sind.
6. Deaktivieren Sie bei Bedarf den Schalter **Erweiterten KSN-Modus verwenden**. Der erweiterte KSN-Modus ist standardmäßig aktiviert.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie die KSN-Nutzung (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz → Kaspersky Security Network** aus.

3. Verwenden Sie den Schalter **Kaspersky Security Network**, um die Komponente zu aktivieren oder zu deaktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Endpoint Security die Erklärung zu Kaspersky Security Network an. Bitte lesen und akzeptieren Sie die Nutzungsbedingungen von Kaspersky Security Network (KSN), wenn Sie damit einverstanden sind.

4. Deaktivieren Sie bei Bedarf den Schalter **Erweiterten KSN-Modus aktivieren**. Der erweiterte KSN-Modus ist standardmäßig aktiviert.

5. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verwendung des KSN aktiviert ist, verwendet Kaspersky Endpoint Security daher Informationen über die Reputation von Dateien, Webressourcen und Programmen, die vom Kaspersky Security Network empfangen werden.

Einschränkungen von Kaspersky Private Security Network

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. Mit Kaspersky Private Security Network können Sie Ihre eigene lokale Reputationsdatenbank verwenden, um die Reputation von Objekten (Dateien oder Webadressen) zu überprüfen. Die Reputation eines Objekts, das der lokalen Reputationsdatenbank hinzugefügt wird, hat eine höhere Priorität als ein Objekt, das dem KSN/KPSN hinzugefügt wird. Stellen Sie sich zum Beispiel vor, Kaspersky Endpoint Security untersucht einen Computer und fordert die Reputation einer Datei im KSN/KPSN an. Wenn die Datei in der lokalen Reputationsdatenbank als *Nicht vertrauenswürdig* verzeichnet ist, in KSN/KPSN aber als *Vertrauenswürdig*, betrachtet Kaspersky Endpoint Security die Datei als *Nicht vertrauenswürdig* und führt die für erkannte Bedrohungen vorgesehene Aktion aus.

In einigen Fällen fordert Kaspersky Endpoint Security jedoch möglicherweise nicht die Reputation eines Objekts im KSN/KPSN an. Wenn dies der Fall ist, empfängt Kaspersky Endpoint Security keine Daten aus der lokalen Reputationsdatenbank von KPSN. Kaspersky Endpoint Security fragt aus folgenden Gründen möglicherweise nicht nach der Reputation eines Objekts im KSN/KPSN:

- Kaspersky-Programme verwenden Offline-Reputationsdatenbanken. Offline-Reputationsdatenbanken wurden entwickelt, um die Ressourcen während des Betriebs von Kaspersky-Programmen zu optimieren und kritisch wichtige Objekte auf dem Computer zu schützen. Offline-Reputationsdatenbanken werden von Kaspersky-Experten auf der Grundlage von Daten aus dem Kaspersky Security Network erstellt. Kaspersky-Programme aktualisieren Offline-Reputationsdatenbanken mit Antiviren-Datenbanken des jeweiligen Programms. Wenn Offline-Reputationsdatenbanken Informationen über ein untersuchtes Objekt enthalten, fordert das Programm die Reputation dieses Objekts nicht vom KSN/KPSN an.

- Untersuchungsausnahmen (vertrauenswürdige Zone) werden in den Programmeinstellungen konfiguriert. Wenn dies der Fall ist, berücksichtigt der Antrag die Reputation des Objekts in der lokalen Reputationsdatenbank nicht.

- Das Programm verwendet Technologien zur Untersuchungsoptimierung (iSwift oder iChecker) oder speichert in einem Cache die Reputationsanforderungen an KSN bzw. KPSN. Wenn dies der Fall ist, fordert das Programm möglicherweise nicht die Reputation von zuvor untersuchten Objekten an.

- Um die Arbeitslast zu optimieren, untersucht das Programm Dateien in einem bestimmten Format und einer bestimmten Größe. Die Liste der relevanten Formate und Größenbeschränkungen werden von Kaspersky-Experten festgelegt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können auch Optimierungseinstellungen für Untersuchungen in der Programmoberfläche konfigurieren, z. B. für die Komponente Schutz vor bedrohlichen Dateien.

- Kaspersky Endpoint Security im Light Agent-Modus tauscht über einen KSN-Proxyserver Daten mit dem KSN-Server aus. Die direkte Interaktion mit KSN wird nicht unterstützt.

Cloud-Modus für die Schutzkomponenten aktivieren und deaktivieren

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.

Bei der Verwendung von Kaspersky Private Security Network ist die Funktionalität des Cloud-Modus ab Version von Kaspersky Private Security Network 3.0 verfügbar.

Wenn das Programm im Light Agent-Modus ausgeführt wird, ist der Cloud-Modus nicht verfügbar.

So aktivieren und deaktivieren Sie den Cloud-Modus für die Schutzkomponenten (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz** → **Kaspersky Security Network** aus.
4. Verwenden Sie das Kontrollkästchen **Cloud-Modus aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.
5. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren und deaktivieren Sie den Cloud-Modus für die Schutzkomponenten (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Kaspersky Security Network**.
5. Verwenden Sie den Schalter **Cloud-Modus verwenden**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren oder deaktivieren Sie den Cloud-Modus für die Schutzkomponenten (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Erweiterter Schutz** → **Kaspersky Security Network** aus.
3. Verwenden Sie den Schalter **Cloud-Modus aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen lädt Kaspersky Endpoint Security beim nächsten Update eine Light-Version oder Vollversion der Antiviren-Datenbanken herunter.

Falls die eingeschränkte Version der Antiviren-Datenbanken nicht verfügbar ist, schaltet Kaspersky Endpoint Security automatisch zur Verwendung der vollständigen Version der Antiviren-Datenbanken um.

KSN Proxy-Einstellungen

Benutzercomputer, die vom Administrationsserver für Kaspersky Security Center verwaltet werden, können entweder direkt mit KSN interagieren oder über den KSN Proxy-Dienst.

Wenn das Programm im Light Agent-Modus ausgeführt wird, wird die direkte Kommunikation mit KSN nicht unterstützt. Kaspersky Endpoint Security kommuniziert über den KSN-Proxyserver mit den KSN-Servern.

Der Dienst KSN Proxy bietet folgende Möglichkeiten:

- Ein Benutzercomputer kann Anfragen an KSN ausführen und Informationen an KSN übertragen, auch wenn er keinen direkten Internetzugang besitzt.
- Der KSN Proxy-Dienst übernimmt die Zwischenspeicherung von aufbereiteten Daten. Dadurch wird der Verbindungskanal zu dem externen Netzwerk entlastet und der Empfang angeforderter Informationen durch den Benutzercomputer wird beschleunigt.

Wenn KSN aktiviert ist und die KSN-Erklärung akzeptiert wurde, verwendet das Programm standardmäßig einen Proxyserver für die Verbindung mit Kaspersky Security Network. Als Proxyserver verwendet das Programm den Kaspersky Security Center-Administrationsserver über den TCP-Port 13111. Falls KSN Proxy nicht verfügbar ist, müssen Sie überprüfen, ob folgende Bedingungen erfüllt sind:

- Der Dienst `ksnproxy` wird auf dem Administrationsserver ausgeführt.
- Port 13111 wird von der Firewall auf dem Computer nicht gesperrt.

Sie können KSN Proxy wie folgt konfigurieren: KSN Proxy aktivieren oder deaktivieren, und den Verbindungsport konfigurieren. Öffnen Sie dazu die Eigenschaften des Administrationsservers. Weitere Informationen über die KSN Proxy-Konfiguration finden Sie in der Hilfe zu Kaspersky Security Center. Außerdem können Sie KSN Proxy für bestimmte Computer über die Kaspersky Endpoint Security-Richtlinie aktivieren oder deaktivieren.

So aktivieren oder deaktivieren Sie KSN Proxy über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Erweiterter Schutz → Kaspersky Security Network** aus.
4. Verwenden Sie im Block **KSN Proxy-Einstellungen** das Kontrollkästchen **Administrationsserver als KSN-Proxyserver verwenden**, um KSN Proxy zu aktivieren oder zu deaktivieren.
5. Aktivieren Sie bei Bedarf das Kontrollkästchen **Kaspersky Security Network-Server verwenden, wenn kein KSN-Proxyserver verfügbar**.

   Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security die KSN-Server, wenn der KSN Proxy-Dienst nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird).
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie KSN Proxy in der „Web Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Kaspersky Security Network**.
5. Verwenden Sie das Kontrollkästchen **Administrationsserver als KSN-Proxyserver verwenden**, um KSN Proxy zu aktivieren oder zu deaktivieren.
6. Aktivieren Sie bei Bedarf das Kontrollkästchen **Kaspersky Security Network-Server verwenden, wenn kein KSN-Proxyserver verfügbar**.

   Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security die KSN-Server, wenn der KSN Proxy-Dienst nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird). Das Kontrollkästchen ist standardmäßig deaktiviert.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Die KSN Proxy-Adresse stimmt mit der Adresse des Administrationsservers überein. Wenn der Domänenname des Administrationsservers geändert wird, müssen Sie die KSN Proxy-Adresse manuell aktualisieren.

Um die KSN Proxy-Adresse zu konfigurieren:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
3. Wählen Sie im Kontextmenü des Ordners **Installationspakete** den Punkt **Eigenschaften** aus.
4. Geben Sie auf der Registerkarte **Allgemein** im angezeigten Fenster die neue Adresse des KSN-Proxyservers an.
5. Speichern Sie die vorgenommenen Änderungen.

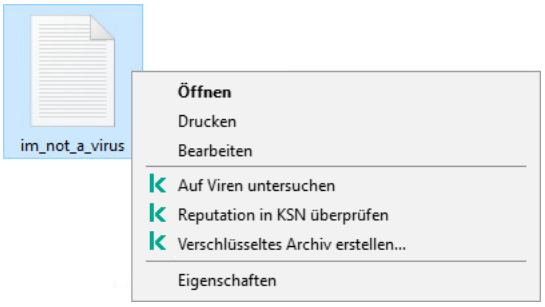
Reputation einer Datei in Kaspersky Security Network überprüfen

Wenn Sie an der Sicherheit einer Datei zweifeln, können Sie die Reputation in Kaspersky Security Network überprüfen.

Die Reputationsprüfung ist verfügbar, wenn Sie die Bedingungen der Erklärung zu Kaspersky Security Network akzeptiert haben.

Um die Reputation einer Datei in Kaspersky Security Network zu überprüfen,

öffnen Sie das Kontextmenü der Datei und wählen Sie den Punkt **Reputation in KSN überprüfen** aus (s. Abb. unten).



Kontextmenü einer Datei

Kaspersky Endpoint Security zeigt die Reputation der Datei an:

Vertrauenswürdig (Kaspersky Security Network). Das Programm betrachtet eine Datei als vertrauenswürdig, wenn eine oder mehrere der folgenden Bedingungen erfüllt sind:

- Die Datei ist von einem vertrauenswürdigen Anbieter digital signiert.
- Die Datei hat in Kaspersky Security Network eine vertrauenswürdige Reputation.
- Der Benutzer hat die Datei in die Gruppe „Vertrauenswürdig“ verschoben.

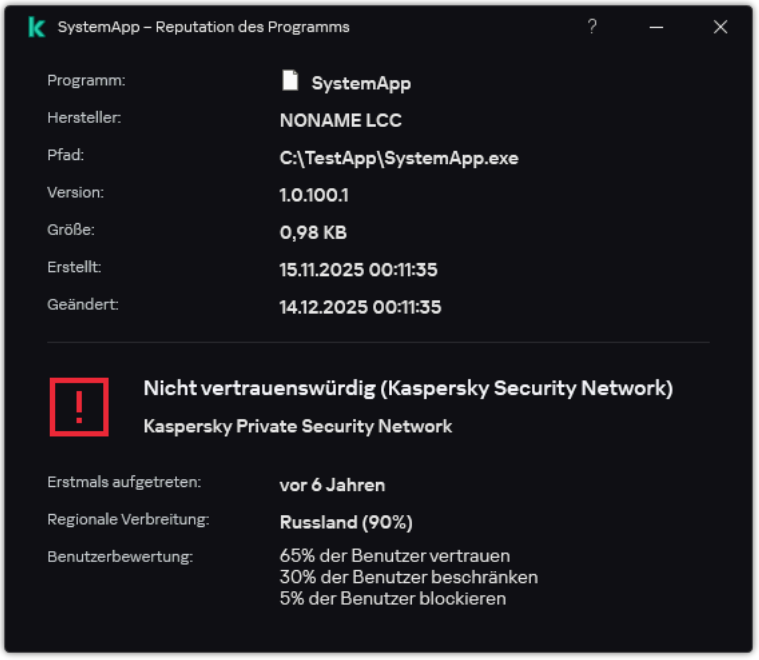
legitimes Programm, mit dem ein Angreifer den Computer oder die Benutzerdaten beschädigen kann. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Angreifern verwendet werden. Nähere Informationen zu legalen Programmen, die von Angreifern missbraucht werden können, um den Computer oder die Daten des Anwenders zu beschädigen, erhalten Sie auf der Website der Viren-Enzyklopädie von Kaspersky. Diese Programme können Sie zur Liste der vertrauenswürdigen Programme hinzufügen.

Nicht vertrauenswürdig (Kaspersky Security Network). Virus oder anderes Programm, das eine Bedrohung darstellt.

Unbekannt (Kaspersky Security Network). In Kaspersky Security Network liegen keine Informationen über die Datei vor. Sie können die Datei mithilfe der Antiviren-Datenbanken untersuchen (Punkt **Auf Viren untersuchen** im Kontextmenü).

Kaspersky Endpoint Security zeigt die KSN-Variante an, mit der die Reputation der Datei ermittelt wurde: *Kaspersky Security Network* oder *Kaspersky Private Security Network*.

Außerdem zeigt Kaspersky Endpoint Security zusätzliche Informationen über die Datei an (s. Abb. unten).



Reputation einer Datei in Kaspersky Security Network

Untersuchung verschlüsselter Verbindungen

Nach der Installation fügt Kaspersky Endpoint Security dem Systemspeicher für vertrauenswürdige Zertifikate (Windows-Zertifikatspeicher) ein Kaspersky-Zertifikat hinzu. Kaspersky Endpoint Security verwendet dieses Zertifikat, um verschlüsselte Verbindungen zu untersuchen. Kaspersky Endpoint Security umfasst auch die Verwendung der Systemspeicherung von vertrauenswürdigen Zertifikaten in Firefox und Thunderbird, um den Datenverkehr dieser Programme zu untersuchen.

Die Komponenten Web-Kontrolle, Schutz vor E-Mail-Bedrohungen, Schutz vor Web-Bedrohungen, Verhaltensanalyse und Exploit-Prävention können den Netzwerkverkehr, der mit folgenden Protokollen über verschlüsselte Verbindungen übertragen wird, entschlüsseln und untersuchen:

- SSL 3.0;
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Untersuchung verschlüsselter Verbindungen aktivieren

Standardmäßig untersucht Kaspersky Endpoint Security verschlüsselte Verbindungen nicht immer, sondern nur, wenn die Schutzkomponenten eine Untersuchung anfordern.

So aktivieren Sie die Untersuchung von verschlüsselten Verbindungen (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Netzwerkeinstellungen** aus.
5. Wählen Sie im Block **Untersuchung verschlüsselter Verbindungen** den Modus für die Untersuchung verschlüsselter Verbindungen aus:
   - **Verschlüsselte Verbindungen untersuchen**. Kaspersky Endpoint Security kann nicht auf Inhalte von Websites zugreifen, deren Adressen mit `https://` beginnen.
   - **Verschlüsselte Verbindungen auf Anfrage von Schutzkomponenten untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr nur, wenn die Untersuchung von den Komponenten „Schutz vor Web-Bedrohungen“, „Schutz vor E-Mail-Bedrohungen“ und „Web-Kontrolle“ angefordert wird.
   - **Verschlüsselte Verbindungen immer untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr auch dann, wenn die Schutzkomponenten deaktiviert sind.

   Kaspersky Endpoint Security überprüft keine geschützten Verbindungen, die von vertrauenswürdigen Programmen hergestellt wurden, für die die Überprüfung des Datenverkehrs deaktiviert ist. Kaspersky Endpoint Security untersucht keine geschützten Verbindungen aus der vordefinierten Liste der vertrauenswürdigen Websites. Die vordefinierte Liste der vertrauenswürdigen Websites wird von Kaspersky-Experten erstellt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können die vordefinierte Liste der vertrauenswürdigen Websites nur in der Oberfläche von Kaspersky Endpoint Security anzeigen. Sie können die Liste in der Konsole von Kaspersky Security Center nicht anzeigen.
6. Fügen Sie falls erforderlich Untersuchungsausnahmen hinzu: vertrauenswürdige Adressen und Programme.
7. Passen Sie die Einstellungen für die Untersuchung verschlüsselter Verbindungen an (siehe folgende Tabelle).
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Untersuchung von verschlüsselten Verbindungen (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.
5. Aktivieren Sie unter **Untersuchung verschlüsselter Verbindungen** den Schalter **Untersuchung verschlüsselter Verbindungen AKTIVIERT**.

   Wenn der Schalter deaktiviert ist, kann Kaspersky Endpoint Security nicht auf Inhalte von Websites zugreifen, deren Adressen mit `https://` beginnen.
6. Klicken Sie auf **Einstellungen** und wählen Sie den Modus für die Untersuchung verschlüsselter Verbindungen aus:

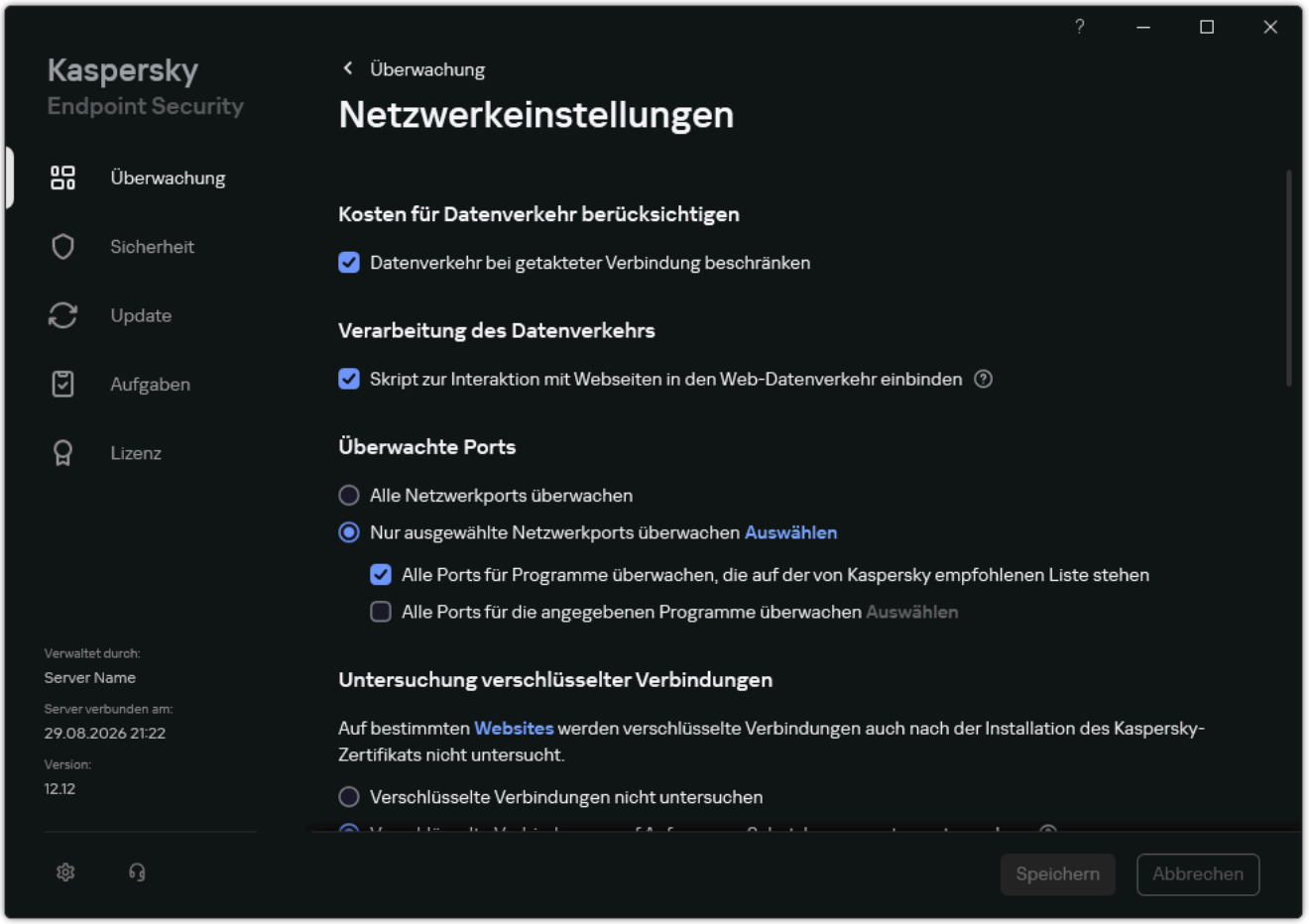
   - **Verschlüsselte Verbindungen auf Anfrage von Schutzkomponenten untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr nur, wenn die Untersuchung von den Komponenten „Schutz vor Web-Bedrohungen“, „Schutz vor E-Mail-Bedrohungen“ und „Web-Kontrolle“ angefordert wird.
   - **Verschlüsselte Verbindungen immer untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr auch dann, wenn die Schutzkomponenten deaktiviert sind.

   Kaspersky Endpoint Security überprüft keine geschützten Verbindungen, die von vertrauenswürdigen Programmen hergestellt wurden, für die die Überprüfung des Datenverkehrs deaktiviert ist. Kaspersky Endpoint Security untersucht keine geschützten Verbindungen aus der vordefinierten Liste der vertrauenswürdigen Websites. Die vordefinierte Liste der vertrauenswürdigen Websites wird von Kaspersky-Experten erstellt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können die vordefinierte Liste der vertrauenswürdigen Websites nur in der Oberfläche von Kaspersky Endpoint Security anzeigen. Sie können die Liste in der Konsole von Kaspersky Security Center nicht anzeigen.
7. Fügen Sie falls erforderlich Untersuchungsausnahmen hinzu: vertrauenswürdige Adressen und Programme.
8. Passen Sie die Einstellungen für die Untersuchung verschlüsselter Verbindungen an (siehe folgende Tabelle).
9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Untersuchung von verschlüsselten Verbindungen (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Netzwerkeinstellungen** aus.



Einstellungen für die Untersuchung verschlüsselter Verbindungen

3. Wählen Sie im Block **Untersuchung verschlüsselter Verbindungen** den Modus für die Untersuchung verschlüsselter Verbindungen aus:

   - **Verschlüsselte Verbindungen nicht untersuchen**. Kaspersky Endpoint Security kann nicht auf Inhalte von Websites zugreifen, deren Adressen mit `https://` beginnen.

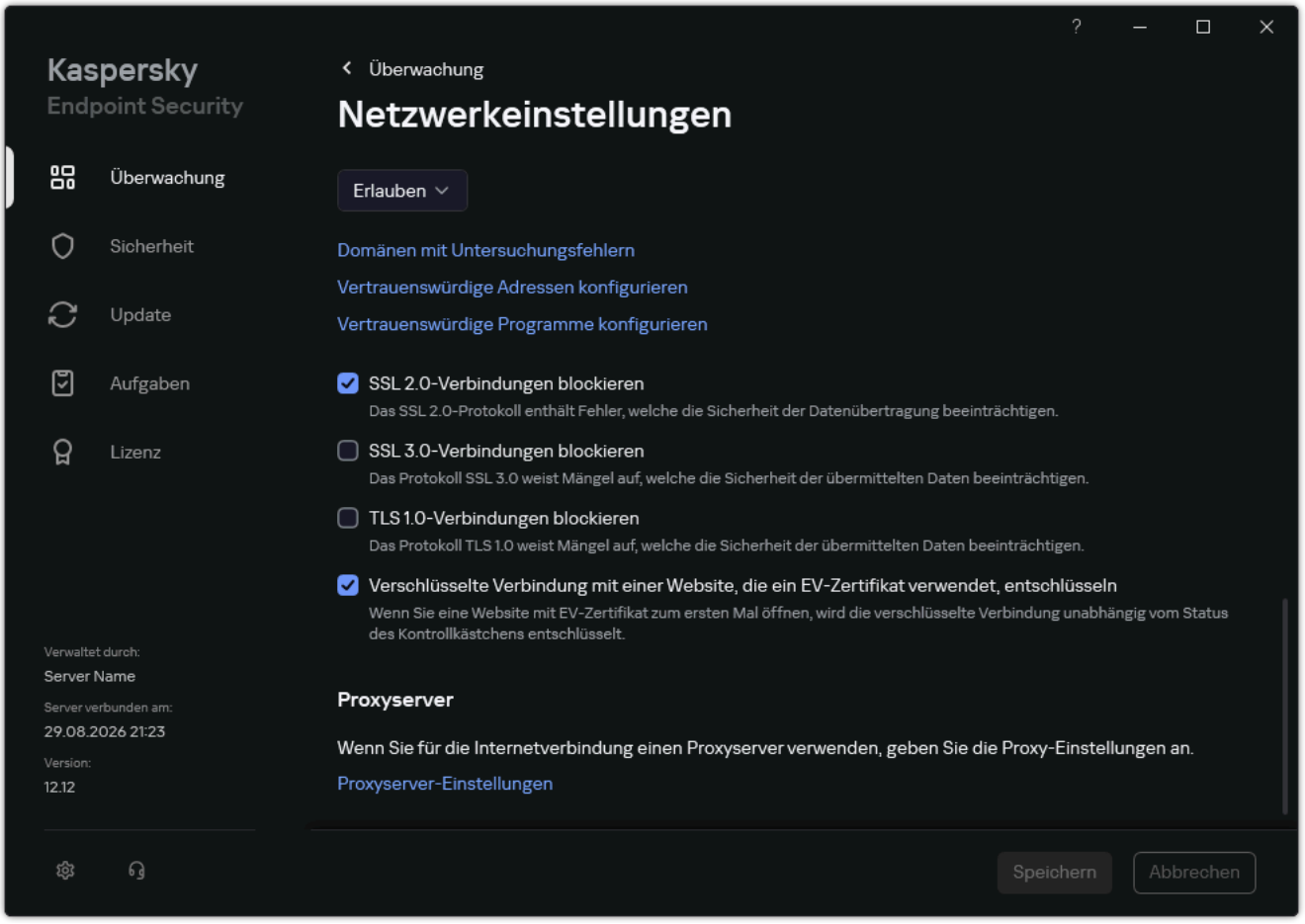
   - **Verschlüsselte Verbindungen auf Anfrage von Schutzkomponenten untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr nur, wenn die Untersuchung von den Komponenten „Schutz vor Web-Bedrohungen“, „Schutz vor E-Mail-Bedrohungen“ und „Web-Kontrolle“ angefordert wird.

   - **Verschlüsselte Verbindungen immer untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr auch dann, wenn die Schutzkomponenten deaktiviert sind.

Kaspersky Endpoint Security überprüft keine geschützten Verbindungen, die von vertrauenswürdigen Programmen hergestellt wurden, für die die Überprüfung des Datenverkehrs deaktiviert ist. Kaspersky Endpoint Security untersucht keine geschützten Verbindungen aus der vordefinierten Liste der vertrauenswürdigen Websites. Die vordefinierte Liste der vertrauenswürdigen Websites wird von Kaspersky-Experten erstellt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können die vordefinierte Liste der vertrauenswürdigen Websites nur in der Oberfläche von Kaspersky Endpoint Security anzeigen. Sie können die Liste in der Konsole von Kaspersky Security Center nicht anzeigen.

4. Fügen Sie falls erforderlich Untersuchungsausnahmen hinzu: vertrauenswürdige Adressen und Programme.

5. Passen Sie die Einstellungen für die Untersuchung verschlüsselter Verbindungen an (siehe folgende Tabelle).



Erweiterte Einstellungen für die Untersuchung verschlüsselter Verbindungen

6. Speichern Sie die vorgenommenen Änderungen.

Einstellung	Beschreibung
Vertrauenswürdige Stammzertifikate	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.
Besuch einer Domäne mit nicht vertrauenswürdigem Zertifikat	• **Erlauben**. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat erfolgt, erlaubt Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite enthält eine Warnung und Informationen über den Grund, aus welchem ein Besuch dieser Domäne als riskant gilt. Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann. Wenn eine Drittanbieter-Anwendung oder ein Drittanbieter-Dienst eine Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat herstellt, erstellt Kaspersky Endpoint Security ein eigenes Zertifikat für die Untersuchung des Datenverkehrs. Das neue Zertifikat hat den Status *Nicht vertrauenswürdig*. Dies ist notwendig, um die Drittanbieter-Anwendung vor der nicht vertrauenswürdigen Verbindung zu warnen, da die HTML-Seite in diesem Fall nicht angezeigt und die Verbindung im Hintergrundmodus hergestellt werden kann. • **Blockieren**. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat erfolgt, blockiert Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite informiert über den Grund, aus dem der Wechsel zu dieser Domäne blockiert wurde.
Beim Besuch einer Domäne mit Untersuchungsfehler wegen verschlüsselten Verbindungen	• **Blockieren**. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, blockiert Kaspersky Endpoint Security die Netzwerkverbindung. • **Erlauben und Domäne zu Ausnahmen hinzufügen**. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, fügt Kaspersky Endpoint Security die Domäne zur Liste der Domänen mit Untersuchungsfehlern hinzu und überwacht den verschlüsselten Netzwerkverkehr beim Besuch dieser Domäne nicht. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich. Um den Inhalt der Liste zurückzusetzen, wählen Sie das Element **Blockieren** aus. Kaspersky Endpoint Security generiert auch ein Ereignis für den Fehler bei der Untersuchung der verschlüsselten Verbindung.
SSL 2.0-Verbindungen blockieren	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.
SSL 3.0-Verbindungen blockieren	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.
TLS 1.0-Verbindungen blockieren	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.
Verschlüsselte Verbindung mit einer Website, die ein EV-Zertifikat verwendet, entschlüsseln	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. Ist das Kontrollkästchen aktiviert, werden geschützte Verbindungen, die ein EV-Zertifikat verwenden, vom Programm entschlüsselt und überwacht. Ist das Kontrollkästchen deaktiviert, hat Kaspersky Endpoint Security keinen Zugriff auf den Inhalt des HTTPS-Datenverkehrs. Deshalb kontrolliert das Programm den HTTPS-Datenverkehr nur nach 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.

Installation von vertrauenswürdigen Stammzertifikaten

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.

So installieren Sie vertrauenswürdige Stammzertifikate über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
4. Klicken Sie im Block **Vertrauenswürdige Stammzertifikate** auf **Hinzufügen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster ein vertrauenswürdiges Stammzertifikat aus.

   Kaspersky Endpoint Security unterstützt Zertifikate mit den Erweiterungen PEM, DER und CRT.
6. Speichern Sie die vorgenommenen Änderungen.

So installieren Sie vertrauenswürdige Stammzertifikate über die Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Netzwerkeinstellungen**.
5. Klicken Sie auf den Link **Vertrauenswürdige Stammzertifikate**.
6. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf **Hinzufügen** und wählen Sie ein vertrauenswürdiges Stammzertifikat aus.

   Kaspersky Endpoint Security unterstützt Zertifikate mit den Erweiterungen PEM, DER und CRT.
7. Speichern Sie die vorgenommenen Änderungen.

So installieren Sie vertrauenswürdige Stammzertifikate über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.

3. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Zertifikate anzeigen**.

4. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf **Hinzufügen** und wählen Sie ein vertrauenswürdiges Stammzertifikat aus.

   Kaspersky Endpoint Security unterstützt Zertifikate mit den Erweiterungen PEM, DER und CRT.

5. Speichern Sie die vorgenommenen Änderungen.

Nun verwendet Kaspersky Endpoint Security bei der Untersuchung des Datenverkehrs neben dem Systemzertifikatspeicher zusätzlich auch einen eigenen Zertifikatspeicher.

Untersuchung von verschlüsselten Verbindungen mit einem nicht vertrauenswürdigen Zertifikat

Nach der Installation fügt Kaspersky Endpoint Security dem Systemspeicher für vertrauenswürdige Zertifikate (Windows-Zertifikatspeicher) ein Kaspersky-Zertifikat hinzu. Kaspersky Endpoint Security verwendet dieses Zertifikat, um verschlüsselte Verbindungen zu untersuchen. Wenn ein Benutzer eine Domäne mit einem nicht vertrauenswürdigen Zertifikat besucht, können Sie den Benutzerzugriff auf diese Domäne zulassen oder verbieten (siehe folgende Anleitung).

Wenn Sie dem Benutzer den Besuch von Domänen mit nicht vertrauenswürdigen Zertifikaten erlaubt haben, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Wenn im *Browser* eine Domäne mit einem nicht vertrauenswürdigen Zertifikat besucht wird, verwendet Kaspersky Endpoint Security das Kaspersky-Zertifikat, um den Datenverkehr zu untersuchen. Kaspersky Endpoint Security zeigt eine HTML-Seite mit einer Warnung an und nennt den Grund, aus dem der Besuch der entsprechenden Domäne nicht empfohlen wird (siehe folgende Abbildung). Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann. Nach Klick auf diesen Link zeigt Kaspersky Endpoint Security eine Stunde lang keine Warnungen über ein nicht vertrauenswürdiges Zertifikat an, wenn zu anderen Ressourcen in derselben Domäne gewechselt wird. Außerdem generiert Kaspersky Endpoint Security ein Ereignis über das Herstellen einer verschlüsselten Verbindung mit einem nicht vertrauenswürdigen Zertifikat.

  In einigen Fällen kann Kaspersky Endpoint Security eine HTML-Seite nicht anzeigen und im Browser erscheint eine Warnung (siehe folgende Abbildung). Dies passiert beispielsweise, wenn eine Webressource die veraltete Version eines Netzwerkprotokolls und einen nicht standardmäßigen Port verwendet. In diesen Fällen sperrt Kaspersky Endpoint Security den Zugriff auf diese Domäne und im Browser erscheint das Standardfenster `ERR_CONNECTION_RESET`. Um auf eine Webressource zuzugreifen, können Sie die Domäne den Ausnahmen hinzufügen oder ein vertrauenswürdiges Zertifikat verwenden.

- Wenn *eine Drittanbieter-Anwendung oder ein Drittanbieter-Dienst* eine Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat herstellt, erstellt Kaspersky Endpoint Security ein eigenes Zertifikat für die Untersuchung des Datenverkehrs. Das neue Zertifikat hat den Status *Nicht vertrauenswürdig*. Dies ist notwendig, um die Drittanbieter-Anwendung vor der nicht vertrauenswürdigen Verbindung zu warnen, da die HTML-Seite in diesem Fall nicht angezeigt und die Verbindung im Hintergrundmodus hergestellt werden kann. Darum wird die Verbindung möglicherweise getrennt, wenn eine Drittanbieter-Anwendung über integrierte Tools zur Zertifikatsprüfung verfügt. In diesem Fall müssen Sie sich an den Domänenbesitzer wenden und eine vertrauenswürdige Verbindung einrichten. Wenn keine vertrauenswürdige Verbindung eingerichtet werden kann, können Sie die Drittanbieter-Anwendung zur Liste der vertrauenswürdigen Anwendungen hinzufügen. Außerdem generiert Kaspersky Endpoint Security ein Ereignis über das Herstellen einer verschlüsselten Verbindung mit einem nicht vertrauenswürdigen Zertifikat.

So konfigurieren Sie die Untersuchung verschlüsselter Verbindungen mit einem nicht vertrauenswürdigen Zertifikat über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
4. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Erweiterte Einstellungen**.
5. Wählen Sie im folgenden Fenster aus, welchen Betriebsmodus die App beim Besuch einer Domäne mit einem nicht vertrauenswürdigen Zertifikat verwendet: **Erlauben** oder **Blockieren**.
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung verschlüsselter Verbindungen mit einem nicht vertrauenswürdigen Zertifikat über die Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Netzwerkeinstellungen**.
5. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf den Link **Einstellungen**.
6. Wählen Sie im folgenden Fenster aus, welchen Betriebsmodus die App beim Besuch einer Domäne mit einem nicht vertrauenswürdigen Zertifikat verwendet: **Verbindung erlauben** oder **Verbindung blockieren**.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Untersuchung verschlüsselter Verbindungen mit einem nicht vertrauenswürdigen Zertifikat über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.

3. Wählen Sie im Block **Untersuchung verschlüsselter Verbindungen** aus, welchen Betriebsmodus die App beim Besuch einer Domäne mit einem nicht vertrauenswürdigen Zertifikat verwendet: **Erlauben** oder **Blockieren**.

4. Speichern Sie die vorgenommenen Änderungen.



Warnung über den Besuch einer Domäne mit nicht vertrauenswürdigem Zertifikat

Kaspersky-Zertifikat zum eigenen Zertifikatspeicher hinzufügen

Browser und E-Mail-Clients verwenden das Zertifikat, um die Sicherheit und Authentizität von Webressourcen zu überprüfen. Das Zertifikat dient auch zur Datenverschlüsselung zwischen Webressourcen und dem Benutzer. Die meisten Browser und E-Mail-Clients verwenden den Speicher für vertrauenswürdige Zertifikate (Windows-Zertifikatspeicher). So zum Beispiel Google Chrome. Einige Browser und E-Mail-Clients verwenden standardmäßig ihren eigenen Zertifikatspeicher anstelle des Windows-Zertifikatspeichers. So zum Beispiel Firefox und Thunderbird.

Nach der Installation fügt Kaspersky Endpoint Security dem Systemspeicher für vertrauenswürdige Zertifikate (Windows-Zertifikatspeicher) ein Kaspersky-Zertifikat hinzu. Wenn Kaspersky Security Center in Ihrem Unternehmen bereitgestellt ist und eine Richtlinie auf einen Computer angewendet wird, aktiviert Kaspersky Endpoint Security automatisch die Verwendung des Windows-Zertifikatspeichers in Browsern und E-Mail-Clients, um den Datenverkehr dieser Programme zu untersuchen. Wenn keine Richtlinie auf den Computer angewendet wird, können Sie den Zertifikatspeicher auswählen, der von Browsern und E-Mail-Clients verwendet werden soll. Wenn Sie einen eigenen Zertifikatspeicher ausgewählt haben, fügen Sie das Kaspersky-Zertifikat manuell zu diesem Speicher hinzu. Dies hilft, Fehler bei der Arbeit mit HTTPS-Verkehr zu vermeiden.

Um den Datenverkehr im Browser Mozilla Firefox und im E-Mail-Client Thunderbird zu untersuchen, müssen Sie die Untersuchung verschlüsselter Verbindungen aktivieren. Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, untersucht das Programm den Datenverkehr im Browser Mozilla Firefox und im E-Mail-Client Thunderbird nicht. Um den Datenverkehr in den E-Mail-Clients MyOffice Mail und R7-Office Organizer zu untersuchen, muss auch die Untersuchung verschlüsselter Verbindungen aktiviert sein.

Bevor Sie ein Zertifikat zum eigenen Zertifikatspeicher des Browsers oder des E-Mail-Agenten hinzufügen, exportieren Sie das Kaspersky-Zertifikat aus der Windows-Systemsteuerung (Eigenschaften von Internet). Weitere Informationen über das Hinzufügen eines Zertifikats zum Speicher finden Sie beispielsweise auf der Website des technischen Supports von Mozilla.

Sie können den Zertifikatspeicher nur in der lokalen Benutzeroberfläche des Programms auswählen.

So wählen Sie einen Zertifikatspeicher zur Untersuchung verschlüsselter Verbindungen in Browsern und E-Mail-Clients aus:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
3. Aktivieren Sie im Block **Untersuchung verschlüsselter Verbindungen** das Kontrollkästchen **Folgenden Speicher verwenden, um verschlüsselte Verbindungen in Anwendungen mit eigenem Zertifikatspeicher zu untersuchen**.
4. Wählen Sie einen Zertifikatspeicher aus:
   - **Windows-Zertifikatspeicher (empfohlen)**. Das Kaspersky-Stammzertifikat wird zu diesem Speicher hinzugefügt, während Kaspersky Endpoint Security installiert wird.
   - **Eigener Zertifikatspeicher**. Mozilla Firefox und Thunderbird verwenden ihre eigenen Zertifikatspeicher. Wenn der Mozilla-Zertifikatspeicher ausgewählt ist, müssen Sie das Kaspersky-Stammzertifikat in den Browser-Eigenschaften manuell zu diesem Speicher hinzufügen.

     Die Mail-Clients MyOffice Mail und R7-Office Organizer verwenden ebenfalls ihren eigenen Zertifikatspeicher.
5. Speichern Sie die vorgenommenen Änderungen.

Geschützte Verbindungen von der Untersuchung ausschließen

Die meisten Web-Ressourcen verwenden geschützte Verbindungen. Die Kaspersky-Experten empfehlen, die Untersuchung verschlüsselter Verbindungen zu aktivieren. Wenn die Untersuchung verschlüsselter Verbindungen Sie bei der Arbeit stört, können Sie die entsprechende Website als Ausnahme zu den *vertrauenswürdigen Adressen* hinzufügen. 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.

Wenn ein vertrauenswürdiges Programm eine geschützte Verbindung verwendet, können Sie die Untersuchung verschlüsselter Verbindungen für dieses Programm deaktivieren. Sie können die Untersuchung verschlüsselter Verbindungen beispielsweise für Cloud-Speicher-Programme deaktivieren, da solche Programme eine Zwei-Faktor-Authentifikation mit einem eigenen Zertifikat verwenden.

So schließen Sie über die Verwaltungskonsole (MMC) eine Webadresse von der Untersuchung verschlüsselter Verbindungen aus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
5. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Vertrauenswürdige Adressen konfigurieren**.

6. Klicken Sie auf **Hinzufügen**.

7. Geben Sie einen Domänennamen oder eine IP-Adresse ein, damit das Programm Kaspersky Endpoint Security die geschützten Verbindungen nicht untersucht, die beim Wechsel zu dieser Webseite hergestellt werden.

   Kaspersky Endpoint Security unterstützt das Zeichen `*` für die Eingabe einer Maske in Domänennamen.

   > Kaspersky Endpoint Security unterstützt das Symbol `*` bei IP-Adressen nicht. Sie können eine breite Auswahl an IP-Adressen mithilfe einer Subnetz-Maske auswählen (zum Beispiel 198.51.100.0/24).

   Beispiele:

   - `domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Der Eintrag umfasst keine Unterdomänen (z. B. `subdomain.domain.com`).
   - `subdomain.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.
   - `*.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So schließen Sie in der Web Console eine Webadresse von der Untersuchung verschlüsselter Verbindungen aus

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Netzwerkeinstellungen**.

5. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Vertrauenswürdige Domänen**.

6. Klicken Sie auf **Hinzufügen**.

7. Geben Sie einen Domänennamen oder eine IP-Adresse ein, damit das Programm Kaspersky Endpoint Security die geschützten Verbindungen nicht untersucht, die beim Wechsel zu dieser Webseite hergestellt werden.

   Kaspersky Endpoint Security unterstützt das Zeichen `*` für die Eingabe einer Maske in Domänennamen.

   > Kaspersky Endpoint Security unterstützt das Symbol `*` bei IP-Adressen nicht. Sie können eine breite Auswahl an IP-Adressen mithilfe einer Subnetz-Maske auswählen (zum Beispiel 198.51.100.0/24).

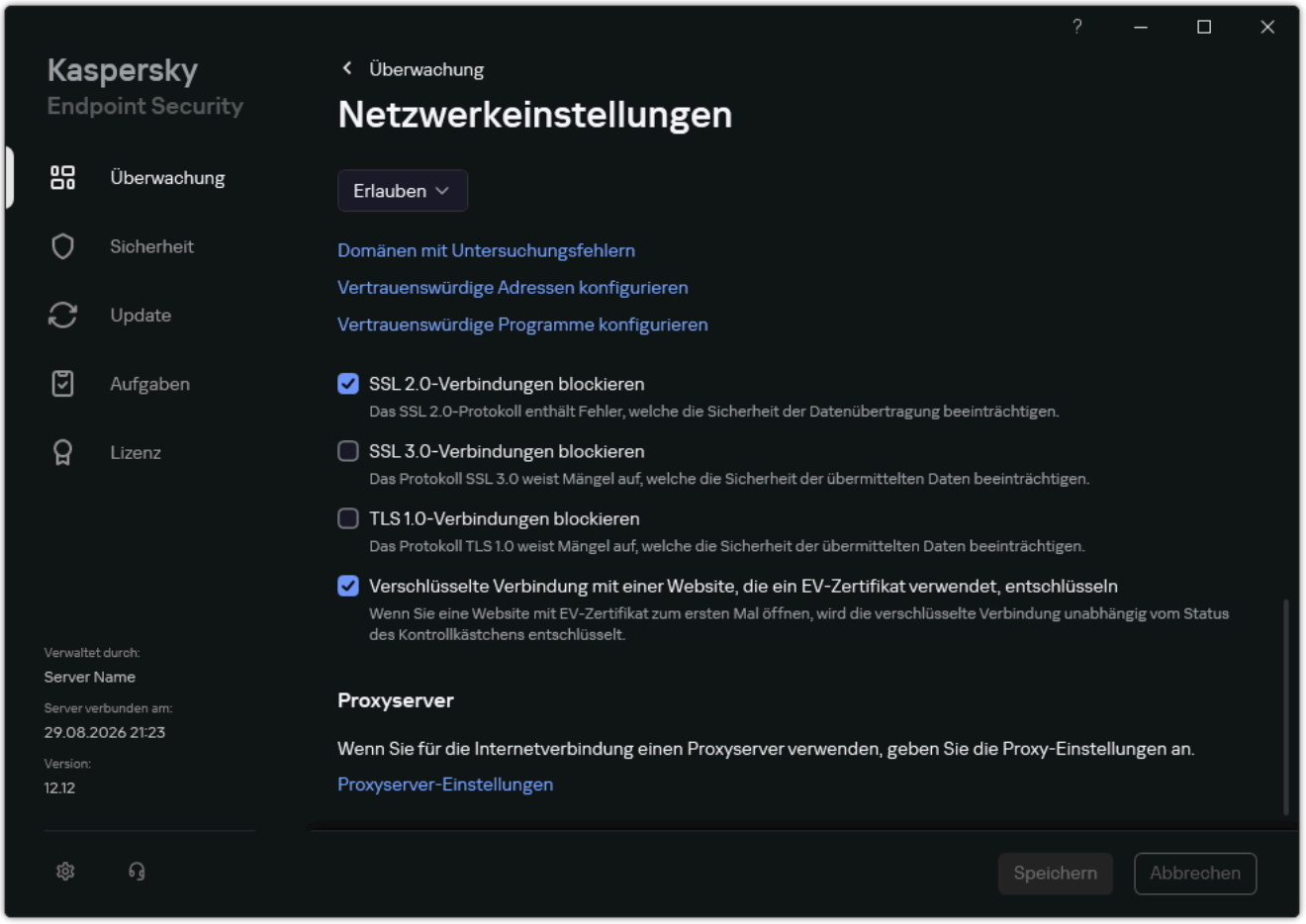
Beispiele:

- `domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Der Eintrag umfasst keine Unterdomänen (z. B. `subdomain.domain.com`).
- `subdomain.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.
- `*.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So schließen Sie über die App-Benutzeroberfläche eine Webadresse von der Untersuchung verschlüsselter Verbindungen aus

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.



Netzwerkeinstellungen für die App

3. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Vertrauenswürdige Adressen konfigurieren**.
4. Klicken Sie auf **Hinzufügen**.

5. Geben Sie einen Domänennamen oder eine IP-Adresse ein, damit das Programm Kaspersky Endpoint Security die geschützten Verbindungen nicht untersucht, die beim Wechsel zu dieser Webseite hergestellt werden.

   Kaspersky Endpoint Security unterstützt das Zeichen `*` für die Eingabe einer Maske in Domänennamen.

   > Kaspersky Endpoint Security unterstützt das Symbol `*` bei IP-Adressen nicht. Sie können eine breite Auswahl an IP-Adressen mithilfe einer Subnetz-Maske auswählen (zum Beispiel 198.51.100.0/24).

   Beispiele:

   - `domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Der Eintrag umfasst keine Unterdomänen (z. B. `subdomain.domain.com`).
   - `subdomain.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.
   - `*.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.

6. Speichern Sie die vorgenommenen Änderungen.

Geschützte Verbindungen, bei denen Fehler auftreten, werden von Kaspersky Endpoint Security standardmäßig nicht untersucht und die Website wird zur Liste *Domänen mit Untersuchungsfehlern* hinzugefügt. Kaspersky Endpoint Security erstellt für jeden Benutzer eine separate Liste und überträgt diese Daten nicht an Kaspersky Endpoint Security. Sie können das Blockieren einer Verbindung beim Auftreten eines Fehlers aktivieren. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich.

Um die Liste der Domänen mit Untersuchungsfehlern anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Netzwerkeinstellungen** aus.
3. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf **Domänen mit Untersuchungsfehlern**.

   Die Liste der Domänen mit Untersuchungsfehlern wird geöffnet. Um die Liste zurückzusetzen, müssen Sie in der Richtlinie das Blockieren einer Verbindung beim Auftreten eines Fehlers aktivieren, die Richtlinie anwenden, die Einstellung auf den ursprünglichen Zustand zurücksetzen und die Richtlinie erneut anwenden.

Die Kaspersky-Experten pflegen eine Liste mit vertrauenswürdigen Websites, die Kaspersky Endpoint Security unabhängig von den Programmeinstellungen nicht untersucht. Dies sind die *globalen Ausnahmen*.

Um die globalen Ausnahmen für die Untersuchung des geschützten Datenverkehrs einzusehen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
3. Klicken Sie im Block **Untersuchung verschlüsselter Verbindungen** auf den Link für die Liste mit vertrauenswürdigen Websites.

Dies öffnet eine Liste von Websites, die von Kaspersky-Experten zusammengestellt wurde. Kaspersky Endpoint Security überprüft geschützte Verbindungen nicht auf Websites auf der Liste. Die Tabelle wird beim Update der Datenbanken und Module von Kaspersky Endpoint Security aktualisiert.

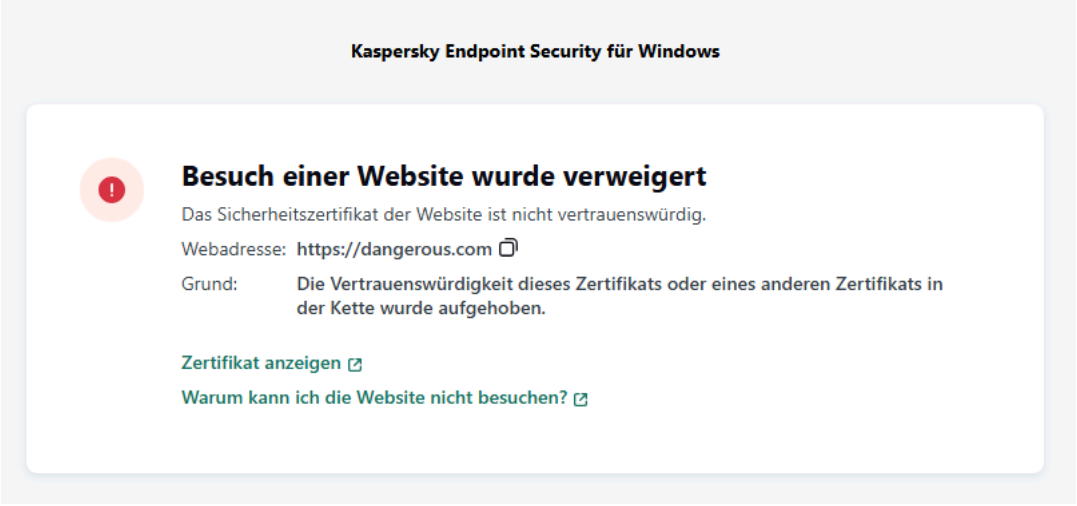
Blockieren des Zugriffs auf Domänen mit nicht vertrauenswürdigen Zertifikaten

Wenn der Zugriff auf eine Domäne mit einem nicht vertrauenswürdigen Zertifikat blockiert wird, zeigt Kaspersky Endpoint Security in einigen Fällen im Browser eine HTML-Warnseite an, auf der der Link zur angeforderten Webressource fehlt.

Dies kann aus folgenden Gründen geschehen:

- Der Administrator hat den Zugriff auf eine Domäne mit einem nicht vertrauenswürdigen Zertifikat blockiert.
- Die Domäne verfügt über ein nicht vertrauenswürdiges oder ungültiges Zertifikat, und der Webserver verwendet den Mechanismus HTTP Strict Transport Security (HSTS). *HSTS* ist ein Sicherheitsmechanismus, der die Verwendung des sicheren HTTPS-Protokolls für die Kommunikation zwischen einem Client und einem Webserver erzwingt. In diesem Fall können Sie auch dann nicht auf die Domäne zugreifen, wenn Sie sie zur Liste vertrauenswürdiger Adressen hinzugefügt haben. Der HSTS-Mechanismus wird in RFC 6797 beschrieben.

  In einigen Fällen kann die Website direkt im Browser geöffnet werden, ohne Kaspersky Endpoint Security zu verwenden. Browser erkennen gesperrte Zertifikate nicht immer, während Kaspersky Endpoint Security beim Verbindungsaufbau online prüft, ob das Zertifikat gesperrt wurde. Dadurch kann das Programm ein Zertifikatproblem vor dem Browser erkennen und die entsprechende Fehlermeldung anzeigen.



Warnung über den Besuch einer Domäne mit nicht vertrauenswürdigem Zertifikat

Daten löschen

Kaspersky Endpoint Security kann die Daten auf Benutzercomputern mithilfe einer Aufgabe ferngesteuert löschen.

Kaspersky Endpoint Security löscht die Daten wie folgt:

- im unbeaufsichtigten Modus.
- auf Festplatten und Wechseldatenträgern.
- für alle Benutzerkonten auf dem Computer.

Kaspersky Endpoint Security führt die Aufgabe *Daten zurücksetzen* für einen beliebigen Lizenzierungstyp aus, selbst nach Ablauf der Lizenz.

Modi für die Datenlöschung

Diese Aufgabe bietet die folgenden Modi zur Datenlöschung:

- Sofortige Datenlöschung.

  In diesem Modus können Sie beispielsweise veraltete Daten löschen, um Speicherplatz freizugeben.

- Aufgeschobene Datenlöschung.

  Dieser Modus dient beispielsweise zum Schutz von Daten auf einem Notebook bei Verlust oder Diebstahl. Sie können festlegen, dass die Daten automatisch gelöscht werden, wenn das Notebook das Unternehmensnetzwerk verlässt und längere Zeit nicht mehr mit Kaspersky Security Center synchronisiert wird.

Es ist nicht möglich, einen Zeitplan für die Datenlöschung in den Aufgabeneigenschaften anzupassen. Die Daten können entweder sofort nach dem Aufgabenstart manuell gelöscht werden oder die aufgeschobene Datenlöschung kann festgelegt werden, falls keine Verbindung zu Kaspersky Security Center besteht.

Beschränkungen

Die Datenlöschung besitzt die folgenden Beschränkungen:

- Die Aufgabe *Daten zurücksetzen* kann nur durch den Administrator für Kaspersky Security Center verwaltet werden. Die Aufgabe kann auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht angepasst oder gestartet werden.
- Für das NTFS-Dateisystem löscht Kaspersky Endpoint Security nur die Namen der grundlegenden Datenströme. Die Namen alternativer Datenströme können nicht gelöscht werden.
- Wenn Kaspersky Endpoint Security eine symbolische Verknüpfungsdatei löscht, werden auch die Dateien gelöscht, deren Pfade in der symbolischen Verknüpfung angegeben sind.

Erstellung einer Aufgabe zur Datenlöschung

Um die Daten auf Benutzercomputern zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Daten zurücksetzen**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Daten löschen (Diebstahlschutz)*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

   > Wenn zur Administrationsgruppe, für welche die Aufgabe gilt, neue Computer hinzugefügt wurden, wird die Aufgabe zur sofortigen Datenlöschung auf den neuen Computern nur unter der Bedingung gestartet, dass zwischen dem Abschluss der Aufgabenausführung und dem Hinzufügen der neuen Computer weniger als 5 Minuten lagen.

5. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

6. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Daten zurücksetzen**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

7. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

8. Wählen Sie eine Methode für die Datenlöschung aus:

   - **Mit Betriebssystemmitteln löschen**. Kaspersky Endpoint Security löscht die Dateien mithilfe von Betriebssystemmitteln und verschiebt die Dateien nicht in den Papierkorb.

   - **Endgültig löschen, Wiederherstellung nicht möglich**. Kaspersky Endpoint Security überschreibt die Dateien mit zufälligen Daten. Nach der Löschung ist es praktisch unmöglich, die Daten wiederherzustellen.

9. Wenn Sie die Datenlöschung aufschieben möchten, aktivieren Sie das Kontrollkästchen **Daten automatisch löschen, falls es keine Verbindung zu Kaspersky Security Center gab seit n Tag(en)**. Legen Sie die Anzahl der Tage fest.

   Die Aufgabe zur aufgeschobenen Datenlöschung wird jedes Mal ausgeführt, wenn der Zeitraum für das Fehlen einer Verbindung mit Kaspersky Security Center überschritten wird.

   Wenn Sie die aufgeschobene Datenlöschung konfigurieren, sollten Sie beachten, dass Mitarbeiter unterschiedliche Arbeitszeitpläne haben können. Berücksichtigen Sie auch den Zeitplan für die Arbeit von mobilen Mitarbeitern. Details über die Verwendung von Offline-Computern und über mobile Benutzer finden Sie in der Hilfe zu Kaspersky Security Center.

   Wenn der Computer ausgeschaltet wird und die Verbindung länger unterbrochen wurde als für die festgelegte Dauer, löscht Kaspersky Endpoint Security die Daten nach dem Einschalten des Computers nicht sofort. Das Programm wartet eine Stunde lang auf die Synchronisierung mit Kaspersky Security Center. Dadurch wird das unbefugte Löschen von Daten auf Computern von Benutzern verhindert, die ihren Computer beispielsweise vor dem Urlaub ausgeschaltet haben.

   Ist das Kontrollkästchen deaktiviert, so wird die Aufgabe sofort nach der Synchronisierung mit Kaspersky Security Center ausgeführt.

10. Erstellen Sie eine Liste der zu löschenden Objekte:

    - **Ordner**. Kaspersky Endpoint Security löscht alle Dateien in dem Ordner und in den Unterordnern. Bei der Eingabe des Ordnerpfads unterstützt Kaspersky Endpoint Security keine Masken und Umgebungsvariablen.

    - **Dateien nach Erweiterung**. Kaspersky Endpoint Security führt eine Suche nach Dateien mit den angegebenen Erweiterungen auf allen Computerlaufwerken aus, dazu gehören auch Wechseldatenträger. Um mehrere Erweiterungen hinzuzufügen, verwenden Sie das Zeichen „`;`“ oder „`,`“.

    - **Vordefinierter Bereich**. Kaspersky Endpoint Security löscht die Dateien aus den folgenden Bereichen:

      - **Dokumente**. Dateien im Standardordner *Dokumente* des Betriebssystems, sowie untergeordnete Ordner.

      - **Cookies-Dateien**. Dateien, in denen der Browser die Daten von Websites speichert, die der Benutzer besucht hat (z. B. Daten für die Benutzerautorisierung).

      - **Desktop**. Dateien im Standardordner *Desktop* des Betriebssystems, sowie untergeordnete Ordner.

      - **Temporäre Dateien für Internet Explorer**. Temporäre Dateien, die mit der Nutzung des Browsers Internet Explorer zusammenhängen: Kopien von Webseiten, Bilder und Mediendateien.

- **Temporäre Dateien**. Temporäre Dateien, die mit der Verwendung Programmen zusammenhängen, die auf dem Computer installiert sind. Beispiel: Das Programm Microsoft Office erstellt temporäre Dateien mit Backup-Kopien von Dokumenten.

- **Outlook-Dateien**. Dateien, die mit der Nutzung des Mail-Clients Outlook zusammenhängen: Datendateien (PST), Offlinedatendateien (OST), Offlineadressbuch-Dateien (OAB) und Dateien für Persönliches Adressbuch (PAB).

- **Benutzerprofil**. Auswahl von Dateien und Ordnern, in denen Betriebssystemeinstellungen für ein lokales Benutzerkonto gespeichert sind.

Sie können auf jeder Registerkarte eine Liste der zu löschenden Objekte erstellen. Kaspersky Endpoint Security erstellt eine allgemeine konsolidierte Liste und löscht im Rahmen der Aufgabe die Dateien aus dieser Liste.

Dateien, welche für die Funktion von Kaspersky Endpoint Security erforderlich sind, können nicht gelöscht werden.

11. Speichern Sie die vorgenommenen Änderungen.

12. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

13. Klicken Sie auf **Starten**.

Dadurch werden die Daten auf den Benutzercomputern im ausgewählten Modus gelöscht: sofort oder bei fehlender Verbindung. Kann Kaspersky Endpoint Security eine Datei nicht löschen, da sie beispielsweise gerade vom Benutzer verwendet wird, so versucht das Programm nicht, die Datei erneut zu löschen. Um die Datenlöschung abzuschließen, starten Sie die Aufgabe erneut.

Kontrolle des Computers

Web-Kontrolle

Die „Web-Kontrolle“ verwaltet den Zugriff durch Benutzer auf Webressourcen. Dadurch lässt sich Datenverkehr einsparen und die zweckentfremdete Nutzung der Arbeitszeit reduzieren. Wenn ein Benutzer versucht, eine Website zu öffnen, auf den die „Web-Kontrolle“ den Zugriff beschränkt, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an (siehe folgende Abb.).

Um die Web-Kontrolle zu verwenden, müssen Sie die Erstkonfiguration des Programms abschließen:

- Aktivieren Sie für die Kontrolle des HTTPS-Datenverkehrs die Untersuchung verschlüsselter Verbindungen (standardmäßig aktiviert).
- Wählen Sie die Ports aus, die Kaspersky Endpoint Security überwachen soll (standardmäßig überwacht das Programm alle Ports).
- Wählen Sie die Programme aus, deren Datenverkehr durch Kaspersky Endpoint Security überwacht werden soll. Die meisten Browser stehen bereits auf der Liste der von Kaspersky empfohlenen Programme. Wenn Ihr Browser nicht auf der Liste steht, fügen Sie ihn manuell hinzu.
- Wir empfehlen, ein Webseiten-Interaktionsskript in den Web-Datenverkehr einzubinden (die Skript-Injektion ist standardmäßig deaktiviert). Dieses Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen für die Ereignisanzeige des Programms, die Ereignisanzeige des Betriebssystems und Berichte.

Methoden zur Verwaltung des Zugriffs auf Websites

Mithilfe der „Web-Kontrolle“ kann der Zugriff auf Websites wie folgt angepasst werden:

- **Website-Kategorie**. 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). So können Sie z. B. den Benutzerzugriff auf die Kategorie „*Soziale Netzwerke*“ oder auf andere Kategorien beschränken.
- **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. festlegen, dass der Zugriff auf den Datentyp *Dateien für Office-Programme* nur für die Website-Kategorie *Web-E-Mail* beschränkt werden soll.

Regeln für den Zugriff auf Websites

Die „Web-Kontrolle“ verwaltet den Zugriff von Benutzern auf Websites mithilfe von *Zugriffsregeln*. Sie können eine Regel für den Zugriff auf Websites wie folgt zusätzlich anpassen:

- Benutzer, für welche die Regel gilt.

  Sie können beispielsweise den Internetzugriff über einen Browser für alle Unternehmensmitarbeiter beschränken, aber die IT-Abteilung ausnehmen.

- Zeitplan für die Regel.

  Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Prioritäten für Zugriffsregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, 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. Es kann beispielsweise vorkommen, dass Kaspersky Endpoint Security ein Unternehmensportal als soziales Netzwerk betrachtet. Um den Zugriff auf soziale Netzwerke zu beschränken und Zugriff auf das Web-Portal des Unternehmens zu gewähren, erstellen Sie zwei Regeln: eine Verbotsregel für die Website-Kategorie „*Soziale Netzwerke*“ und eine Erlaubnisregel für das Unternehmens-Web-Portal. Die Zugriffsregel für das Unternehmens-Web-Portal muss eine höhere Priorität haben als die Zugriffsregel für soziale Netzwerke.





Benachrichtigungen der „Web-Kontrolle"

Hinzufügen einer Web-Ressourcen-Zugriffsregel

Eine *Zugriffsregel für Webressourcen* ist eine Auswahl von Filtern und Aktionen, die Kaspersky Endpoint Security anwendet, wenn Benutzer Webressourcen besuchen. Zugriffsregeln können einen Zeitplan die Regel enthalten.

Es wird davon abgeraten, mehr als 1.000 Zugriffsregeln für Webressourcen zu erstellen, da es andernfalls zu Systeminstabilität kommen kann.

Eine Zugriffsregel für Webressourcen besteht aus einer Auswahl von Filtern und aus einer Aktion, die Kaspersky Endpoint Security ausführt, wenn ein Benutzer die in der Regel beschriebenen Webressourcen zur im Regelzeitplan festgelegten Zeit besucht. Mithilfe von Filtern kann der Bereich der Webressourcen genau festgelegt werden, auf die der Zugriff durch die Komponente „Web-Kontrolle" kontrolliert wird.

Folgende Filter sind verfügbar:

- **Inhaltsfilter**. Die Web-Kontrolle unterteilt die Webressourcen nach Inhaltskategorien und Datentypkategorien. Sie können den Zugriff der Benutzer auf jene Daten kontrollieren, die sich in Webressourcen befinden, welche zu den durch diese Kategorien definierten Datentypen gehören. Wenn ein Benutzer Webressourcen besucht, die zu einer gewählten Inhaltskategorie und / oder Datentypkategorie gehören, führt Kaspersky Endpoint Security die in der Regel festgelegte Aktion aus.

- **Filter für Adressen von Webressourcen**. Sie können den Zugriff der Benutzer auf alle Adressen von Webressourcen oder auf bestimmte Adressen von Webressourcen und / oder Adressgruppen von Webressourcen kontrollieren.

  Wenn die Filterung nach Inhalt und die Filterung nach Web-Ressourcenadressen angegeben ist und die angegebenen Web-Ressourcenadressen und/oder Gruppen von Web-Ressourcenadressen zu den ausgewählten Inhaltskategorien oder Datentypkategorien gehören, kontrolliert Kaspersky Endpoint Security nicht den Zugriff auf alle Web-Ressourcen in den ausgewählten Inhaltskategorien und/oder Datentypkategorien. Stattdessen kontrolliert das Programm nur den Zugriff auf die angegebenen Web-Ressourcenadressen und/oder Gruppen von Web-Ressourcenadressen.

- **Filter für Namen von Benutzern und Benutzergruppen**. Sie können Benutzer und / oder Benutzergruppen festlegen, für die der Zugriff auf Webressourcen nach der Regel kontrolliert werden soll.

- **Zeitplan der Regel**. Sie können einen Zeitplan für die Regel erstellen. Der Zeitplan für eine Regel bestimmt die Zeit, in der Kaspersky Endpoint Security den Zugriff auf die in einer Regel festgelegten Webressourcen kontrolliert.

Nach der Installation von Kaspersky Endpoint Security ist die Regelliste der Komponente „Web-Kontrolle“ nicht leer. Die *Standardregel* ist voreingestellt. Abhängig von der ausgewählten Aktion erlaubt oder verbietet diese Regel allen Benutzern den Zugriff auf alle Webressourcen, die nicht unter andere Regeln fallen.

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, 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. Es kann beispielsweise vorkommen, dass Kaspersky Endpoint Security ein Unternehmensportal als soziales Netzwerk betrachtet. Um den Zugriff auf soziale Netzwerke zu beschränken und Zugriff auf das Web-Portal des Unternehmens zu gewähren, erstellen Sie zwei Regeln: eine Verbotsregel für die Website-Kategorie „*Soziale Netzwerke*“ und eine Erlaubnisregel für das Unternehmens-Web-Portal. Die Zugriffsregel für das Unternehmens-Web-Portal muss eine höhere Priorität haben als die Zugriffsregel für soziale Netzwerke.

So fügen Sie eine Zugriffsregel für Webressourcen in der Verwaltungskonsole (MMC) hinzu oder löschen sie

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Web-Kontrolle** aus.

4. Aktivieren Sie das Kontrollkästchen **Web-Kontrolle**.

5. Klicken Sie im Block **Einstellungen der Web-Kontrolle** auf **Hinzufügen**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

6. Konfigurieren Sie die Zugriffsregel für Webressourcen (siehe folgende Tabelle).

7. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

   > 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.

8. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine Zugriffsregel für Webressourcen über Web Console und Cloud Console hinzu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

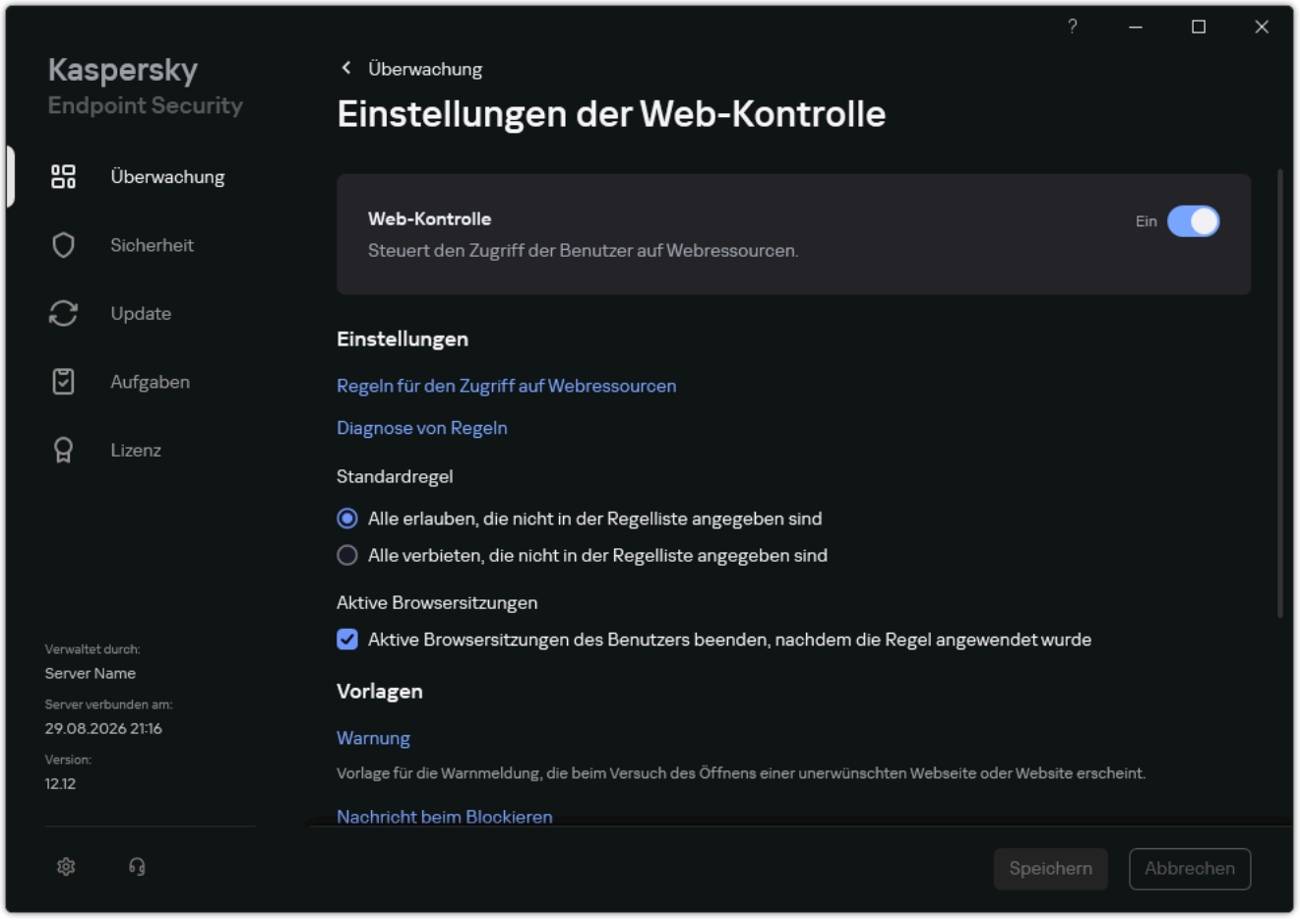
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle → Web-Kontrolle**.
5. Aktivieren Sie den Schalter **Web-Kontrolle AKTIVIERT**.
6. Klicken Sie im Block **Regelliste** auf **Hinzufügen**.
7. Konfigurieren Sie die Zugriffsregel für Webressourcen (siehe folgende Tabelle).
8. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

   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.
9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie über die App-Benutzeroberfläche eine Zugriffsregel für Webressourcen hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Aktivieren Sie den Schalter **Web-Kontrolle**.

4. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.

5. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

6. Konfigurieren Sie die Zugriffsregel für Webressourcen (siehe folgende Tabelle).

7. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

   > 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.

8. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird die neue Regel der Web-Kontrolle zur Liste hinzugefügt. Falls erforderlich, können Sie die Regel der Web-Kontrolle bearbeiten. Außerdem können Sie die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren, ohne sie aus der Liste zu entfernen.

Einstellungen einer Regel der Web-Kontrolle

Einstellung	Beschreibung
Regelname	Name der Regel der Web-Kontrolle.
Status	• **Ein**. • **Aus**. Sie können die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren.
Aktion	• **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen. • **Blockieren**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde. • **Warnen**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.
Inhalt des Filters	• **Nach Inhaltskategorien**. Sie können den Benutzerzugriff auf Webressourcen nach Kategorien steuern (z. B. die Kategorie *Soziale Netzwerke*). • **Nach Datentypen**. Sie können den Benutzerzugriff auf Web-Ressourcen auf der Grundlage des spezifischen Datentyps der veröffentlichten Daten (z. B. *Bilddateien*) steuern.
Adressen	• **Für alle Adressen**. Web-Kontrolle filtert Web-Ressourcen nicht nach Adressen. • **Für bestimmte Adressen**. Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können. Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, ist für das https-Protokoll nur die Filterung nach dem Servernamen verfügbar.
Benutzer	• **Auf alle Benutzer**. Web-Kontrolle filtert keine Web-Ressourcen für bestimmte Benutzer. • **Auf bestimmte Benutzer und/oder Gruppen**. Web-Kontrolle filtert Web-Ressourcen nur für bestimmte Benutzer. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.
Zeitplan der Regel	Der Zeitplan für eine Regel bestimmt die Zeit, in der Kaspersky Endpoint Security den Zugriff auf die in einer Regel festgelegten Webressourcen kontrolliert. Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Nach Adressen von Webressourcen filtern.

Um den Zugriff auf individuelle Webressourcen zu kontrollieren, müssen Sie eine Regel für die Web-Kontrolle erstellen, eine Liste mit Webadressen erstellen und eine Aktion für die Web-Kontrolle auswählen. Beim Erstellen einer Liste mit Webadressen können Sie URL-Adressen eingeben oder Masken verwenden.

Regeln können einen Zeitplan für die Regel sowie eine Liste mit Benutzern umfassen, für welche die Regel gilt. Beispiel: Sie können den Zugriff auf Websites während der Arbeitszeit beschränken oder den Besuch von Websites nur für bestimmte Benutzergruppen zulassen.

So aktivieren Sie einen Adressfilter für Webressourcen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Web-Kontrolle** aus.
4. Aktivieren Sie das Kontrollkästchen **Web-Kontrolle**.

5. Klicken Sie im Block **Einstellungen der Web-Kontrolle** auf **Hinzufügen**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

6. Konfigurieren Sie die Zugriffsregel für Webressourcen:

   a. Tragen Sie im Feld **Name** einen Namen für die Regel ein.

   b. Wählen Sie in der Dropdown-Liste **Auf Adressen anwenden** die Option **Für bestimmte Adressen**.

   c. Erstellen Sie eine Liste mit Adressen von Webressourcen. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren.

   > Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, ist für das https-Protokoll nur die Filterung nach dem Servernamen verfügbar.

   d. Wählen Sie in der Dropdown-Liste **Auf Benutzer anwenden** den passenden Filter für die Benutzer aus:

   - **Für alle Benutzer**. Web-Kontrolle filtert Web-Ressourcen nicht nach Adressen.
   - **Für bestimmte Benutzer oder Gruppen**. Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   e. Wählen Sie in der Dropdown-Liste **Aktion** eine Option aus:

   - **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Verbieten**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde.
   - **Warnen**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.

   f. Wählen Sie in der Dropdown-Liste **Zeitplan der Regel** einen Zeitplan aus oder erstellen Sie einen neuen Zeitplan.

7. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

   > 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.

8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie einen Adressfilter für Webressourcen über Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Web-Kontrolle**.
5. Aktivieren Sie den Schalter **Web-Kontrolle AKTIVIERT**.
6. Klicken Sie im Block **Regelliste** auf **Hinzufügen**.
7. Konfigurieren Sie die Zugriffsregel für Webressourcen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Wählen Sie den Status **Aktiviert** für die Webressourcen-Zugriffsregel.

   Sie können die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren, ohne sie aus der Liste zu entfernen.

   c. Wählen Sie im Block **Aktion** die entsprechende Option:

   - **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Blockieren**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde.
   - **Informieren**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.

   d. Wählen Sie unter **Gültigkeitsbereich** den Punkt **Individuelle Websites** auswählen.

   e. Konfigurieren Sie den Inhaltsfilter:

   - **Individuelle Adresse**. Erstellen Sie eine Liste mit Adressen von Webressourcen. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren.

     Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, ist für das https-Protokoll nur die Filterung nach dem Servernamen verfügbar.

   - **Datentyp**. Sie können den Benutzerzugriff auf Web-Ressourcen auf der Grundlage des spezifischen Datentyps der veröffentlichten Daten (z. B. *Bilddateien*) steuern.

f. Wählen Sie unter **Benutzer oder Gruppe** die Benutzer aus, auf welche die Web-Kontrolle diese Regel anwenden soll.

Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

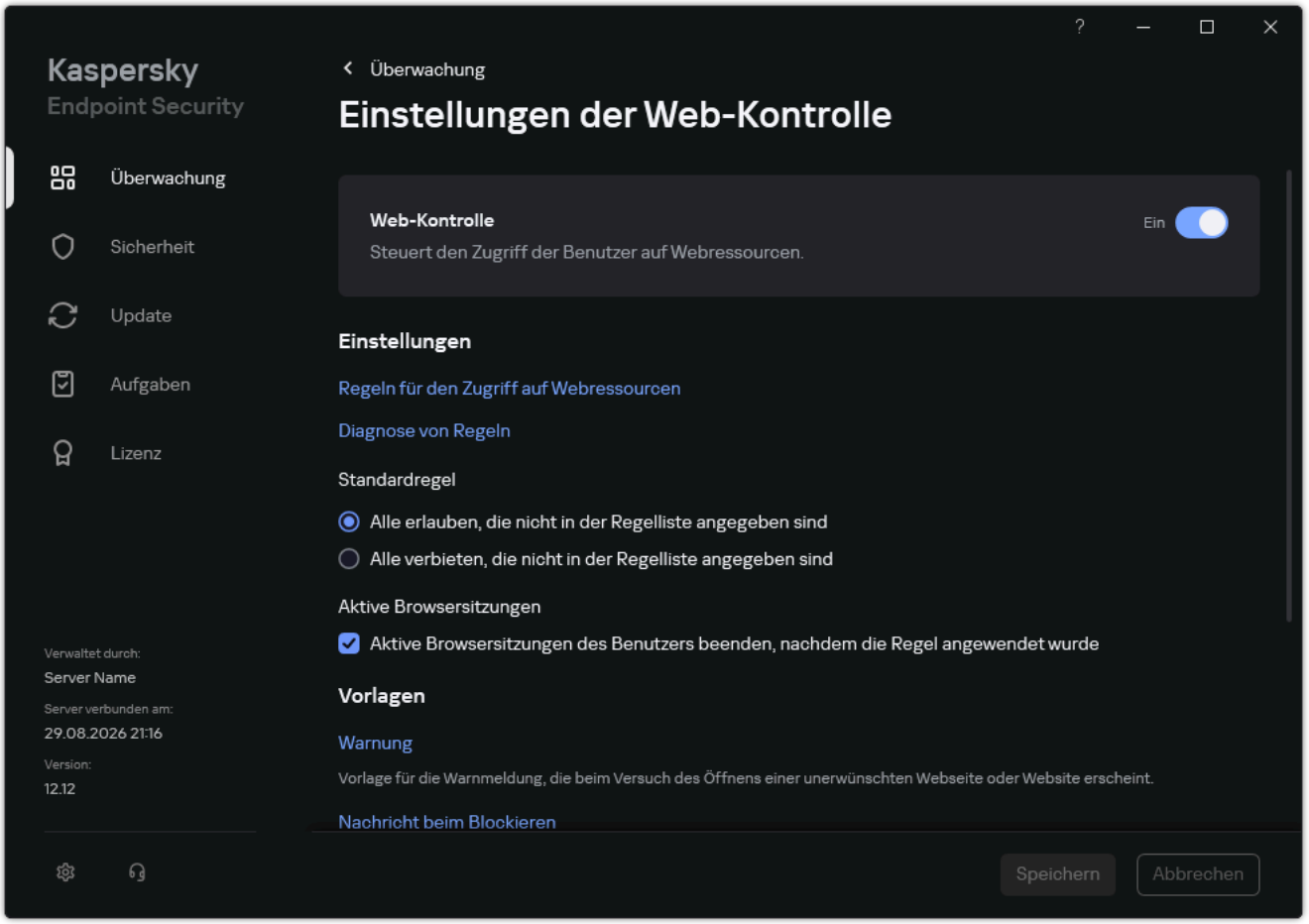
g. Wählen Sie im Block **Zugriffszeitplan** einen Zeitplan aus oder erstellen Sie einen neuen Zeitplan.

8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über die App-Benutzeroberfläche einen Adressfilter für Webressourcen

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.

4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

5. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

6. Wählen Sie den Status **Ein** für die Webressourcen-Zugriffsregel.

Sie können die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren.

7. Wählen Sie im Block **Aktion** die entsprechende Option:

   - **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Blockieren**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde.
   - **Warnen**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.

8. Wählen Sie unter **Adressen** den Punkt **Für bestimmte Adressen** auswählen.

   Erstellen Sie eine Liste mit Adressen von Webressourcen. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren.

   > Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, ist für das https-Protokoll nur die Filterung nach dem Servernamen verfügbar.

9. Wählen Sie im Block **Benutzer** den entsprechenden Filter für Benutzer aus:

   - **Auf alle Benutzer**. Web-Kontrolle filtert keine Web-Ressourcen für bestimmte Benutzer.
   - **Auf bestimmte Benutzer und/oder Gruppen**. Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

10. Wählen Sie in der Dropdown-Liste **Zeitplan der Regel** einen Zeitplan aus oder erstellen Sie einen neuen Zeitplan.

11. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

    > 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.

12. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird die neue Regel der Web-Kontrolle zur Liste hinzugefügt. Falls erforderlich, können Sie die Regel der Web-Kontrolle bearbeiten. Außerdem können Sie die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren, ohne sie aus der Liste zu entfernen.

Nach dem Inhalt von Webressourcen filtern.

Für die Zugriffskontrolle nach Webressourcen-Inhalten bietet die Web-Kontrolle einen Kategorienfilter und einen Filter für Datentypen.

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). So können Sie z. B. den Benutzerzugriff auf die Kategorie „*Soziale Netzwerke*“ oder auf andere Kategorien beschränken.

Sie können den Website-Zugriff nach dem Datentyp beschränken, z. B. um Bilder auszublenden. Kaspersky Endpoint Security ermittelt den Datentyp aufgrund des Dateiformats, nicht nach der Erweiterung. Die Web-Kontrolle unterscheidet die folgenden Datentypen:

- Video
- Audiodaten
- Dateien für Office-Programme
- Ausführbare Dateien
- Archive
- Bilddateien
- Skripte

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*“.

Regeln können einen Zeitplan für die Regel sowie eine Liste mit Benutzern umfassen, für welche die Regel gilt. Beispiel: Sie können den Zugriff auf Websites während der Arbeitszeit beschränken oder den Besuch von Websites nur für bestimmte Benutzergruppen zulassen.

So aktivieren Sie einen Inhaltsfilter für Webressourcen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Web-Kontrolle** aus.
4. Aktivieren Sie das Kontrollkästchen **Web-Kontrolle**.
5. Klicken Sie im Block **Einstellungen der Web-Kontrolle** auf **Hinzufügen**.

   Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

6. Konfigurieren Sie die Zugriffsregel für Webressourcen:

   a. Tragen Sie im Feld **Name** einen Namen für die Regel ein.

   b. Wählen Sie in der Dropdown-Liste **Inhalt filtern** den passenden Inhaltsfilter aus:

   - **Nach Inhaltskategorien**. Sie können den Benutzerzugriff auf Webressourcen nach Kategorien steuern (z. B. die Kategorie *Soziale Netzwerke*).
   - **Nach Datentypen**. Sie können den Benutzerzugriff auf Web-Ressourcen auf der Grundlage des spezifischen Datentyps der veröffentlichten Daten (z. B. *Bilddateien*) steuern.
   - **Nach Inhaltskategorien und Datentypen**. Filter nach Inhaltskategorien und Datentypen sind aktiviert.

   Konfigurieren Sie die Filtereinstellungen, nachdem Sie die Filter ausgewählt haben.

   c. Wählen Sie in der Dropdown-Liste **Auf Benutzer anwenden** den passenden Filter für die Benutzer aus:

   - **Für alle Benutzer**. Web-Kontrolle filtert Web-Ressourcen nicht nach Adressen.
   - **Für bestimmte Benutzer oder Gruppen**. Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   d. Wählen Sie in der Dropdown-Liste **Aktion** eine Option aus:

   - **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Verbieten**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde.
   - **Warnen**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.

   e. Wählen Sie in der Dropdown-Liste **Zeitplan der Regel** einen Zeitplan aus oder erstellen Sie einen neuen Zeitplan.

7. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

   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.

8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie einen Inhaltsfilter für Webressourcen über Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Web-Kontrolle**.
5. Aktivieren Sie den Schalter **Web-Kontrolle AKTIVIERT**.
6. Klicken Sie im Block **Regelliste** auf **Hinzufügen**.
7. Konfigurieren Sie die Zugriffsregel für Webressourcen:
   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.
   b. Wählen Sie den Status **Aktiviert** für die Webressourcen-Zugriffsregel.
      Sie können die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren.
   c. Wählen Sie im Block **Aktion** die entsprechende Option:
      - **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
      - **Blockieren**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde.
      - **Informieren**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.
   d. Wählen Sie unter **Gültigkeitsbereich** den Punkt **Inhaltskategorie** auswählen.
   e. Konfigurieren Sie den Inhaltsfilter:
      - **Inhaltskategorie**. Sie können den Benutzerzugriff auf Webressourcen nach Kategorien steuern (z. B. die Kategorie *Soziale Netzwerke*).
      - **Datentyp**. Sie können den Benutzerzugriff auf Web-Ressourcen auf der Grundlage des spezifischen Datentyps der veröffentlichten Daten (z. B. *Bilddateien*) steuern.

f. Wählen Sie unter **Benutzer oder Gruppe** die Benutzer aus, auf welche die Web-Kontrolle diese Regel anwenden soll.

Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

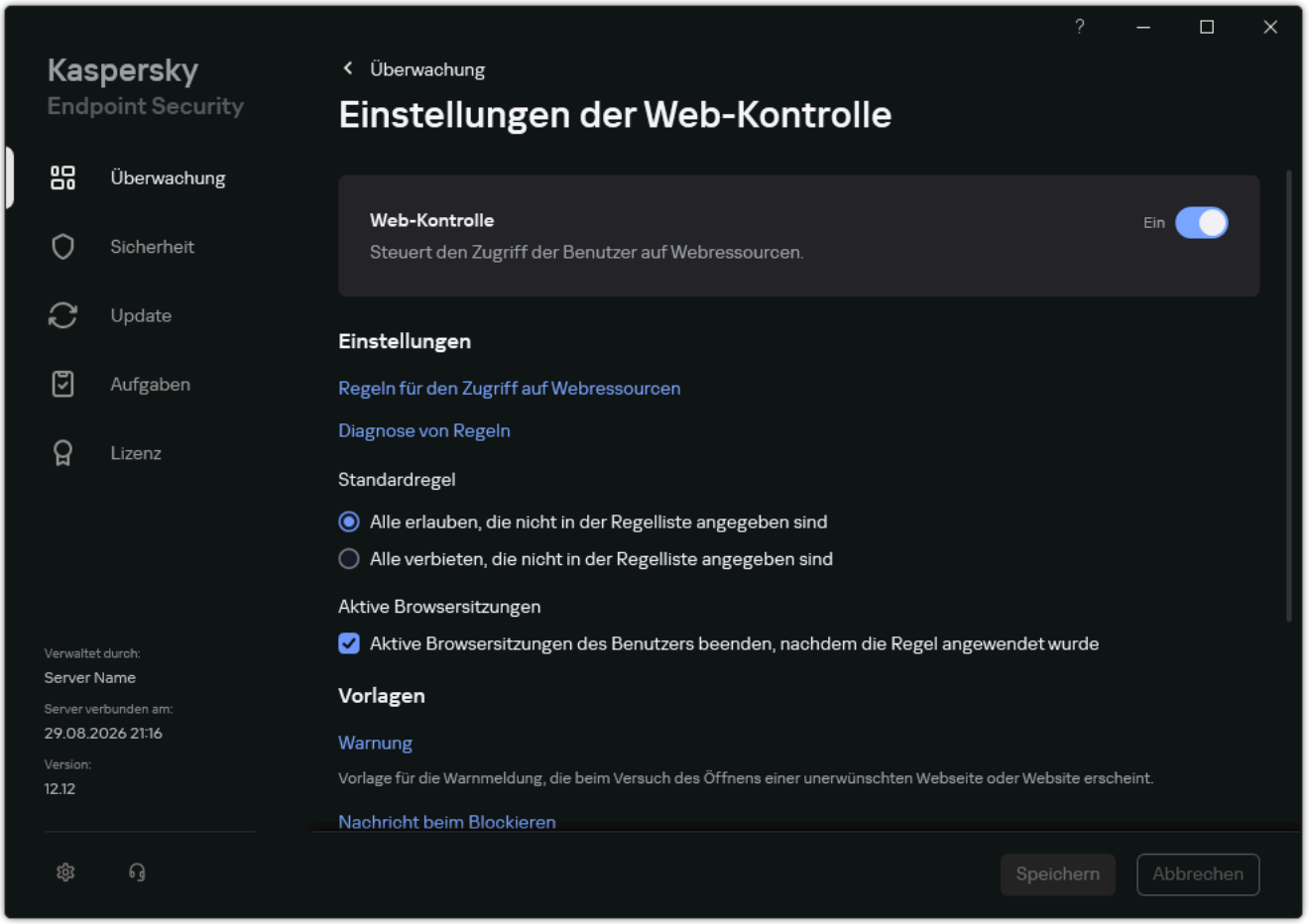
g. Wählen Sie im Block **Zugriffszeitplan** einen Zeitplan aus oder erstellen Sie einen neuen Zeitplan.

8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über die App-Benutzeroberfläche einen Inhaltsfilter für Webressourcen

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.

4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

Das Fenster **Regel für den Zugriff auf Webressourcen** wird geöffnet.

5. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

6. Wählen Sie den Status **Ein** für die Webressourcen-Zugriffsregel.

Sie können die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren.

7. Wählen Sie im Block **Aktion** die entsprechende Option:

   - **Erlauben**. Die Web-Kontrolle erlaubt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen.
   - **Blockieren**. Die Web-Kontrolle sperrt den Zugriff auf Webressourcen, die den Regeleinstellungen entsprechen, und meldet, dass der Zugriff auf die Website verweigert wurde.
   - **Warnen**. Wenn der Benutzer versucht, Zugriff auf eine Webressource zu erhalten, die der Regel entspricht, warnt die Web-Kontrolle vor dem Besuch dieser Webressource. Die Warnmeldung enthält Links, über die der Benutzer auf die angeforderte Webressource zugreifen kann.

8. Wählen Sie im Block **Inhalt des Filters** den entsprechenden Inhaltsfilter aus:

   - **Nach Inhaltskategorien**. Sie können den Benutzerzugriff auf Webressourcen nach Kategorien steuern (z. B. die Kategorie *Soziale Netzwerke*).
   - **Nach Datentypen**. Sie können den Benutzerzugriff auf Web-Ressourcen auf der Grundlage des spezifischen Datentyps der veröffentlichten Daten (z. B. *Bilddateien*) steuern.

   So konfigurieren Sie den Inhaltsfilter:

   a. Klicken Sie auf den Link **Einstellungen**.

   b. Aktivieren Sie die Kontrollkästchen für die entsprechenden Inhaltskategorien und/oder Datentypen.

   Ist das Kontrollkästchen für eine Inhaltskategorie und/oder einen Datentyp aktiviert, so verwendet Kaspersky Endpoint Security die Regel, um den Zugriff auf die Webressourcen zu kontrollieren, die den gewählten Inhaltskategorien und/oder Dateitypen angehören.

   c. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.

9. Wählen Sie im Block **Benutzer** den entsprechenden Filter für Benutzer aus:

   - **Auf alle Benutzer**. Web-Kontrolle filtert Web-Ressourcen nicht nach Adressen.
   - **Auf bestimmte Benutzer und/oder Gruppen**. Die Web-Kontrolle filtert nur Web-Ressourcenadressen aus der Liste. Sie können eine Webadresse eingeben oder Masken verwenden. Sie können auch eine Liste von Webressourcen-Adressen aus einer TXT-Datei exportieren. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können. So erstellen Sie eine Liste der Benutzer, auf die Sie die Regel anwenden möchten:

     a. Klicken Sie auf **Hinzufügen**.

     b. Wählen Sie im folgenden Fenster die Benutzer oder Benutzergruppen aus, auf die Sie die Zugriffsregel für Webressourcen anwenden möchten.

     c. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.

10. Wählen Sie entweder aus der Dropdown-Liste **Zeitplan der Regel** den Namen des entsprechenden Zeitplans oder erstellen Sie auf Basis des gewählten Regelzeitplans einen neuen Zeitplan. Gehen Sie dazu folgendermaßen vor:

    a. Klicken Sie auf **Bearbeiten oder neu hinzufügen**.

    b. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

    c. Geben Sie im angezeigten Fenster den Namen des Regelzeitplans ein.

    d. Konfigurieren Sie den Zeitplan für den Zugriff auf die Web-Ressource für Benutzer.

    e. Kehren Sie zum Fenster für die Konfiguration der Web-Ressourcen-Zugriffsregel zurück.

11. Wenn die Web-Kontrolle die Verbindung mit einer verbotenen Webressource sofort nach dem Übernehmen der Richtlinie trennen soll, aktivieren Sie das Kontrollkästchen **Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde**.

    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.

12. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird die neue Regel der Web-Kontrolle zur Liste hinzugefügt. Falls erforderlich, können Sie die Regel der Web-Kontrolle bearbeiten. Außerdem können Sie die Zugriffsregel für Webressourcen jederzeit mit dem Schalter deaktivieren, ohne sie aus der Liste zu entfernen.

Zugriffsregeln für Webressourcen testen

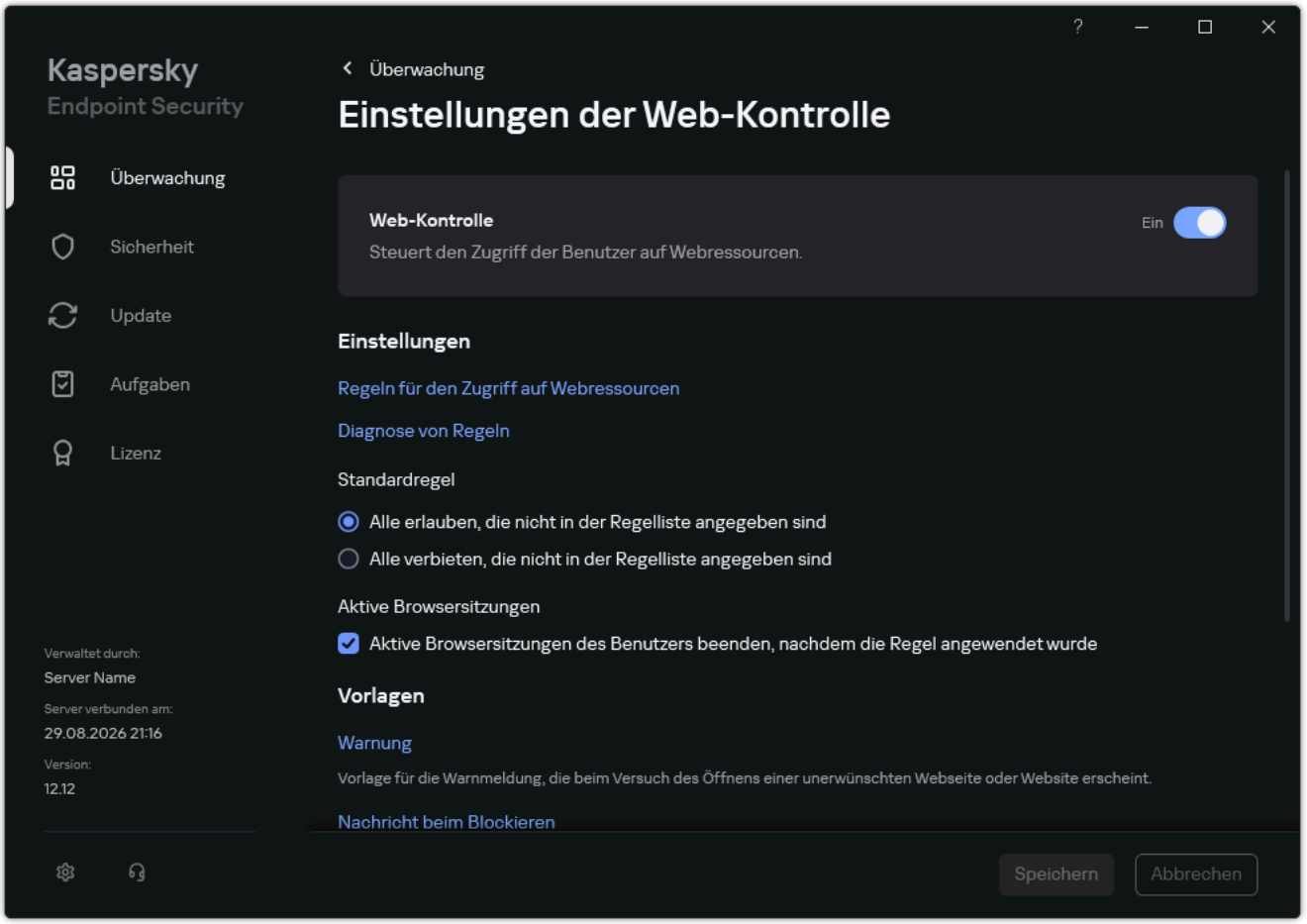
Wenn Sie die Web-Kontrolle konfigurieren, sperren Sie möglicherweise versehentlich den Zugriff auf Webressourcen, die Benutzer zum Arbeiten benötigen. Um herauszufinden, welche Regel der Web-Kontrolle den Zugriff auf Webressourcen blockiert, können Sie das Tool *Diagnose von Regel der Web-Kontrolle* verwenden. Die Diagnose von Regel der Web-Kontrolle ist nur in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar. In der Kaspersky Security Center-Konsole können Sie nicht feststellen, welche Regel der Web-Kontrolle eine bestimmte Ressource enthält.

Hält der Benutzer die Zugriffssperre für eine Webressource für einen Irrtum, so kann der Benutzer mit einem Link aus der Sperrmeldung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.

Gehen Sie folgendermaßen vor, um die Regeln für den Zugriff auf Webressourcen zu testen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Klicken Sie im Block **Einstellungen** auf den Link **Diagnose von Regeln**.

   Das Fenster **Diagnose von Regeln** wird geöffnet.

4. Wenn Sie die Regeln, nach denen Kaspersky Endpoint Security den Zugriff auf eine bestimmte Webressource überwacht, testen möchten, aktivieren Sie das Kontrollkästchen **Geben Sie eine Adresse an**. Geben Sie die Adresse der Webressource unten im Feld ein.

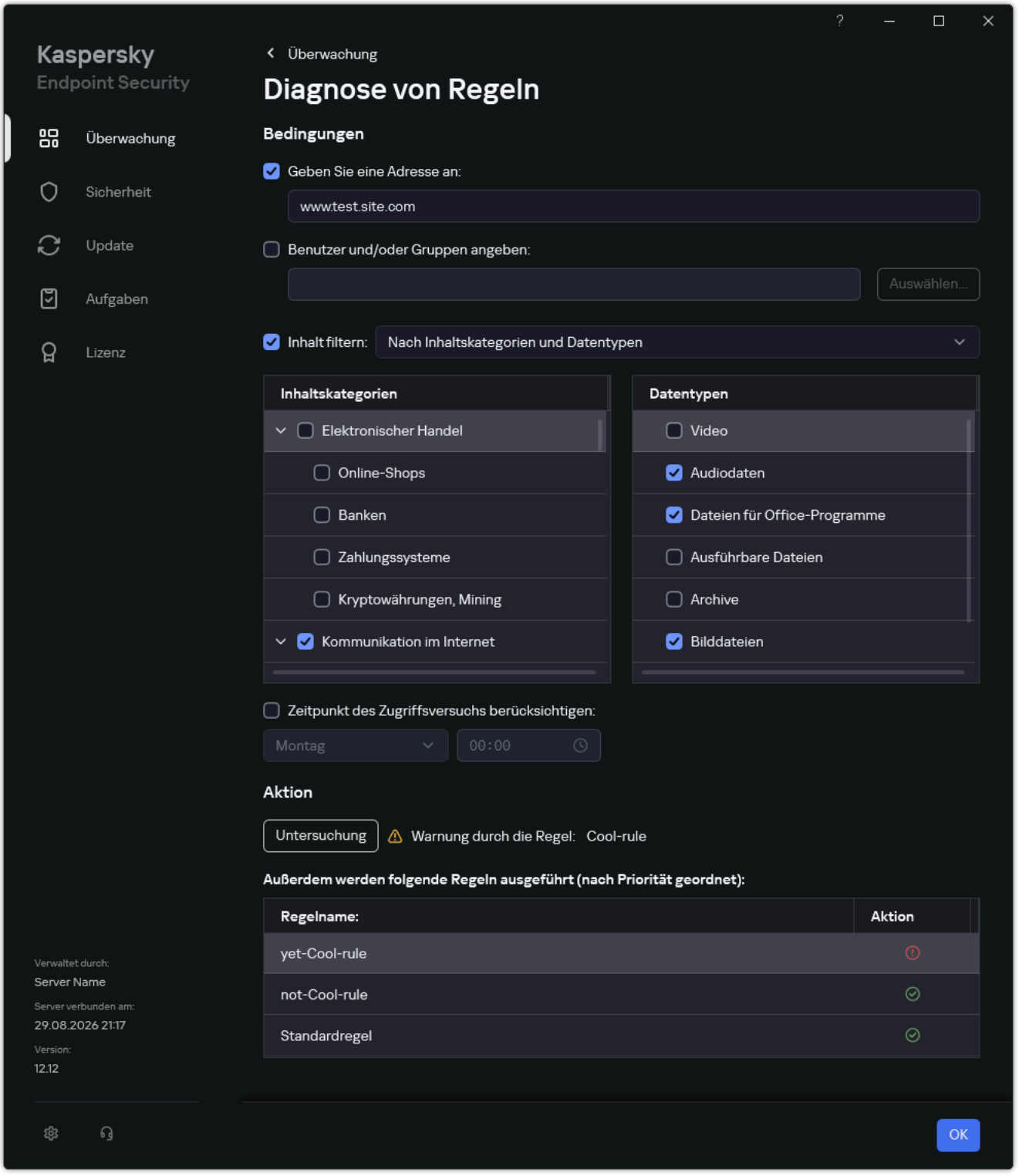
5. Erstellen Sie eine Liste der Benutzer und/oder Benutzergruppen, um die Regeln zu überprüfen, nach denen Kaspersky Endpoint Security den Zugriff auf Webressourcen für bestimmte Benutzer und/oder Benutzergruppen kontrolliert.

6. Wenn Sie die Regeln testen möchten, die Kaspersky Endpoint Security zur Steuerung des Zugriffs auf Webressourcen bestimmter Inhaltskategorien und/oder Datentyp-Kategorien verwendet, aktivieren Sie das Kontrollkästchen **Inhalt filtern** und wählen Sie die entsprechende Option aus der Dropdown-Liste (**Nach Inhaltskategorien**, **Nach Datentypen** oder **Nach Inhaltskategorien und Datentypen**).

7. Aktivieren Sie das Kontrollkästchen **Zeitpunkt des Zugriffsversuchs berücksichtigen**, wenn bei der Regelprüfung der Zeitpunkt (Wochentag und Uhrzeit) berücksichtigt werden soll, zu dem ein Zugriffsversuch auf die Webressourcen erfolgt, die in den Bedingungen für die Regeldiagnose festgelegt wurden. Geben Sie nun einen Wochentag und eine Uhrzeit an.

8. Klicken Sie auf **Untersuchung**.

Nach der Überprüfung wird eine Meldung über die Aktion angezeigt, die Kaspersky Endpoint Security bei einem Zugriffsversuch auf die angegebene Webressource in Übereinstimmung mit der zuerst ausgelösten Regel ausführen würde (Erlauben, Verbieten, Warnen). Die zuerst ausgelöste Regel ist jene Regel, die in der Regelliste der Web-Kontrolle unter jenen Regeln, welche die Diagnosebedingungen erfüllen, an erster Stelle steht. Die Meldung wird rechts von der Schaltfläche **Untersuchung** angezeigt. Die darunter angezeigte Tabelle enthält eine Liste der übrigen ausgelösten Regeln mit Angabe der Aktion, die Kaspersky Endpoint Security ausführt. Die Regeln sind in absteigender Reihenfolge nach der Priorität angeordnet.



Exportieren und Importieren von Regeln der „Web-Kontrolle“

Sie können die Liste der Regeln für die Web-Kontrolle in eine xlm oder json-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Adressen desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie ein Backup für die Liste der Regeln für die Web-Kontrolle anlegen oder die Liste auf einen anderen Server migrieren.

So exportieren und importieren Sie eine Liste von Regeln für die „Web-Kontrolle“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Web-Kontrolle** aus.
4. Um die Liste der Regeln für die „Web-Kontrolle“ zu exportieren:
   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.
   b. Klicken Sie auf den Link **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Speichern Sie die Datei.
      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.
5. Um die Liste der Regeln für die „Web-Kontrolle“ zu importieren:
   a. Klicken Sie auf den Link **Importieren**.
      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.
   b. Öffnen Sie die Datei.
      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
6. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste mit Regeln für die „Web-Kontrolle“ über die „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **Web-Kontrolle**.

5. Um die Liste der Regeln zu exportieren, gehen Sie im Block **Regelliste** wie folgt vor:

   a. Wählen Sie die Regeln, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine json-Datei im standardmäßigen Download-Ordner.

6. Zum Importieren der Liste der Regeln gehen Sie im Block **Regelliste** wie folgt vor:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

Adressen von Webressourcen für eine Regel der Web-Kontrolle exportieren und importieren

Wenn Sie in einer Webressourcen-Zugriffsregel eine Adressliste für Webressourcen erstellt haben, können Sie die Liste in eine Datei exportieren:

- Im txt-Format in der Verwaltungskonsole (MMC)
- Im JSON-Format in der Web Console
- Im csv-Format über die Programmoberfläche

Die Liste kann später aus dieser Datei importiert werden, um beim Anpassen von Regeln keine neue Adressliste für Webressourcen manuell erstellen zu müssen. Die Möglichkeit zum Export und Import einer Adressliste für Webressourcen ist beispielsweise vorteilhaft, wenn Sie Regeln mit ähnlichen Einstellungen erstellen möchten.

Sie können auch alle Regeln der Web-Kontrolle exportieren bzw. importieren, nicht nur die Adressen der Webressourcen für eine konkrete Regel.

So exportieren bzw. importieren Sie die Adressen von Webressourcen für eine Regel der Web-Kontrolle über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.

3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Web-Kontrolle** aus.

5. Wählen Sie im Block **Einstellungen der Web-Kontrolle** die Regel aus, deren Adressliste für Webressourcen exportiert oder importiert werden soll.

   Die Eigenschaften der Regel der Web-Kontrolle werden angezeigt.

6. Um die Liste der Webressourcen zu exportieren, gehen Sie in der Adressliste wie folgt vor:

   a. Wählen Sie die Adressen aus, die Sie exportieren möchten.

      Wenn Sie keine Adresse ausgewählt haben, exportiert Kaspersky Endpoint Security alle Adressen.

   b. Klicken Sie auf die Schaltfläche .

   c. Geben Sie im angezeigten Fenster den Namen der TXT-Datei ein, in welche Sie die Liste der Webressourcen-Adressen exportieren möchten, und wählen Sie den Ordner, in dem Sie diese Datei speichern möchten.

   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die Liste der Adressen von Webressourcen in eine TXT-Datei.

7. Um die Liste der Webressourcen zu importieren, gehen Sie in der Adressliste wie folgt vor:

   a. Klicken Sie auf die Schaltfläche .

      Wählen Sie in dem sich öffnenden Fenster die TXT-Datei aus, aus der Sie die Liste der Webressourcen importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der TXT-Datei ergänzt werden soll.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So exportieren bzw. importieren Sie in der Web Console die Adressen von Webressourcen für eine Regel der Web-Kontrolle

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **Web-Kontrolle**.

5. Wählen Sie im Block **Regelliste** die Regel aus, deren Adressliste für Webressourcen exportiert oder importiert werden soll.

   Die Eigenschaften der Regel der Web-Kontrolle werden angezeigt.

6. Klicken Sie im Block **Gültigkeitsbereich** → **Individuelle Websites** auf **Ändern**.

7. Um die Liste der Webressourcen zu exportieren, gehen Sie in der Adressliste wie folgt vor:

   a. Wählen Sie die Adressen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

      Kaspersky Endpoint Security exportiert die Liste der Adressen von Webressourcen in eine JSON-Datei im standardmäßigen Download-Ordner.

8. Um die Liste der Webressourcen zu importieren, gehen Sie in der Adressliste wie folgt vor:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie in dem sich öffnenden Fenster die JSON-Datei aus, aus der Sie die Liste der Adressen von Webressourcen importieren möchten.

   b. Öffnen Sie die Datei.

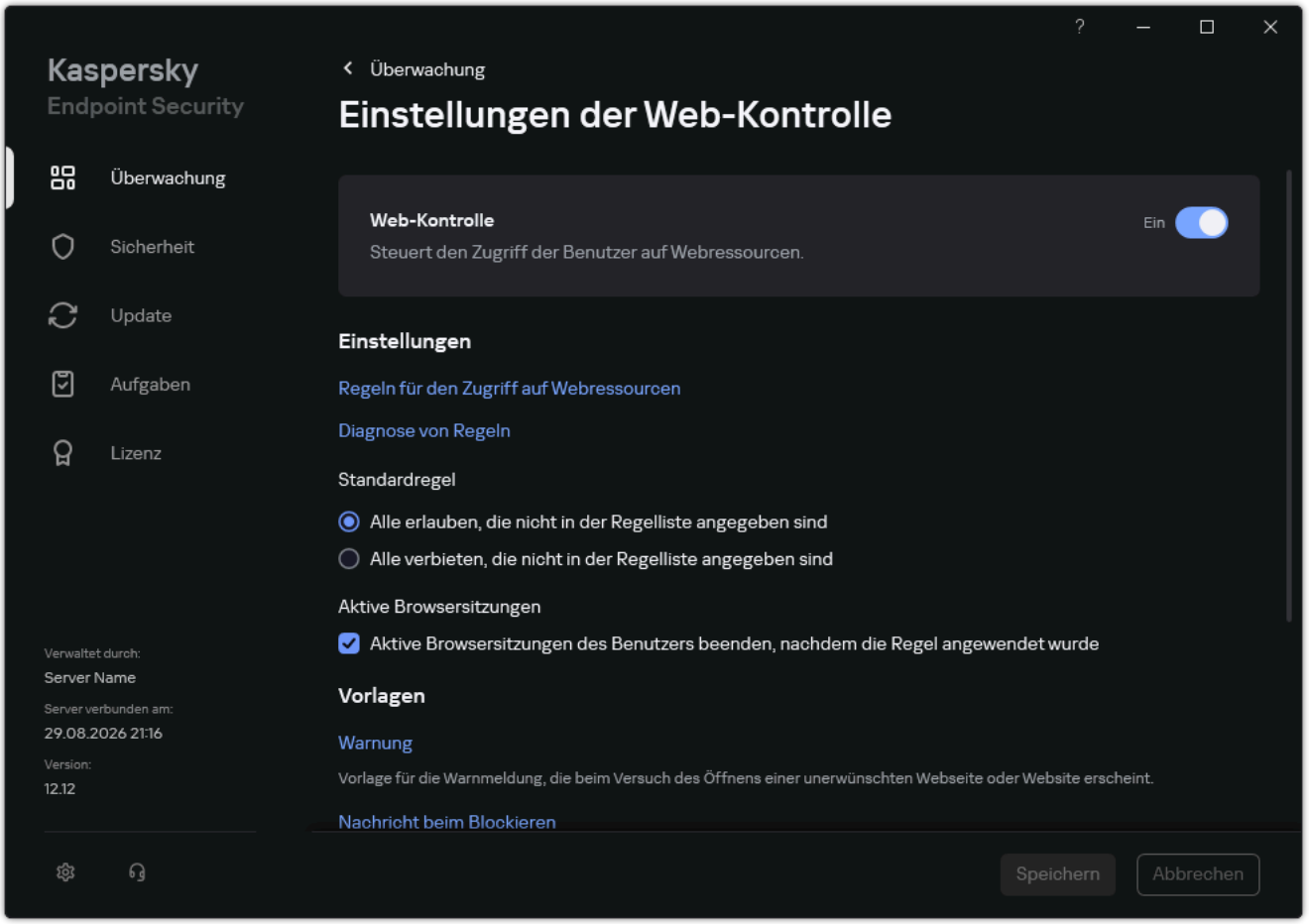
      Wenn es auf dem Computer bereits eine Liste mit Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der JSON-Datei ergänzt werden soll.

   Auf dieselbe Weise können Sie Gruppen von Websites exportieren und importieren.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So exportieren bzw. importieren Sie über die App-Benutzeroberfläche die Adressen von Webressourcen für eine Regel der Web-Kontrolle

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Klicken Sie im Block **Einstellungen** auf **Regeln für den Zugriff auf Webressourcen**.
4. Wählen Sie die Regel, deren Adressliste für Webressourcen exportiert oder importiert werden soll.
5. Um die Liste der vertrauenswürdigen Webadressen zu exportieren, gehen Sie im Block **Adressen** wie folgt vor:

   a. Wählen Sie die Adressen aus, die Sie exportieren möchten.

   Wenn Sie keine Adresse ausgewählt haben, exportiert Kaspersky Endpoint Security alle Adressen.

   b. Klicken Sie auf **Export**.

   c. Geben Sie im angezeigten Fenster den Namen der CSV-Datei ein, in welche Sie die Liste der Webressourcen-Adressen exportieren möchten, und wählen Sie den Ordner, in dem Sie diese Datei speichern möchten.

   d. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die Liste der Adressen von Webressourcen in eine CSV-Datei.

6. Um die Liste der Webressourcen zu importieren, gehen Sie im Block **Adressen** wie folgt vor:

   a. Klicken Sie auf **Import**.

      Wählen Sie in dem sich öffnenden Fenster die CSV-Datei aus, aus der Sie die Liste der Webressourcen importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Adressen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der CSV-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

Überwachung der Internetaktivitäten von Benutzern

Kaspersky Endpoint Security erlaubt es, Daten über den Besuch aller Websites zu protokollieren, einschließlich erlaubter Websites. So können Sie einen vollständigen Verlauf aller im Browser besuchten Websites erhalten. Kaspersky Endpoint Security sendet Ereignisse über die Benutzeraktivitäten an Kaspersky Security Center, an den lokalen Bericht für Kaspersky Endpoint Security, an das Windows-Ereignisprotokoll. Um in Kaspersky Security Center Ereignisse zu erhalten, müssen die Ereigniseinstellungen in der Verwaltungskonsole oder in „Web Console“ angepasst werden. Sie können außerdem festlegen, dass „Web-Kontrolle“-Ereignisse per E-Mail gesendet werden und Benachrichtigungen auf dem Bildschirm des Benutzercomputers angezeigt 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.

Kaspersky Endpoint Security erstellt die folgenden Ereignisse über die Internetaktivitäten des Benutzers:

- Website blockieren (Status *Kritisch*).
- Besuch einer nicht empfohlenen Website (Status *Warnung*).
- Besuch einer erlaubten Website (Status *Information*).

Bevor Sie die Überwachung der Internet-Aktivitäten der Benutzer aktivieren, müssen Sie Folgendes tun:

- Fügen Sie ein Webseiten-Interaktionsskript in den Webverkehr ein (siehe die Anweisungen unten). Das Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen.
- Zur Kontrolle des HTTPS-Datenverkehrs muss die Untersuchung verschlüsselter Verbindungen aktiviert werden.

Webseiten-Interaktionsskript einbetten

So fügen Sie über die Verwaltungskonsole (MMC) ein Webseiten-Interaktionsskript in den Web-Datenverkehr ein

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
4. Aktivieren Sie im Block **Untersuchung verschlüsselter Verbindungen** das Kontrollkästchen **Skript zur Interaktion mit Webseiten in den Web-Datenverkehr einbinden**.
5. Speichern Sie die vorgenommenen Änderungen.

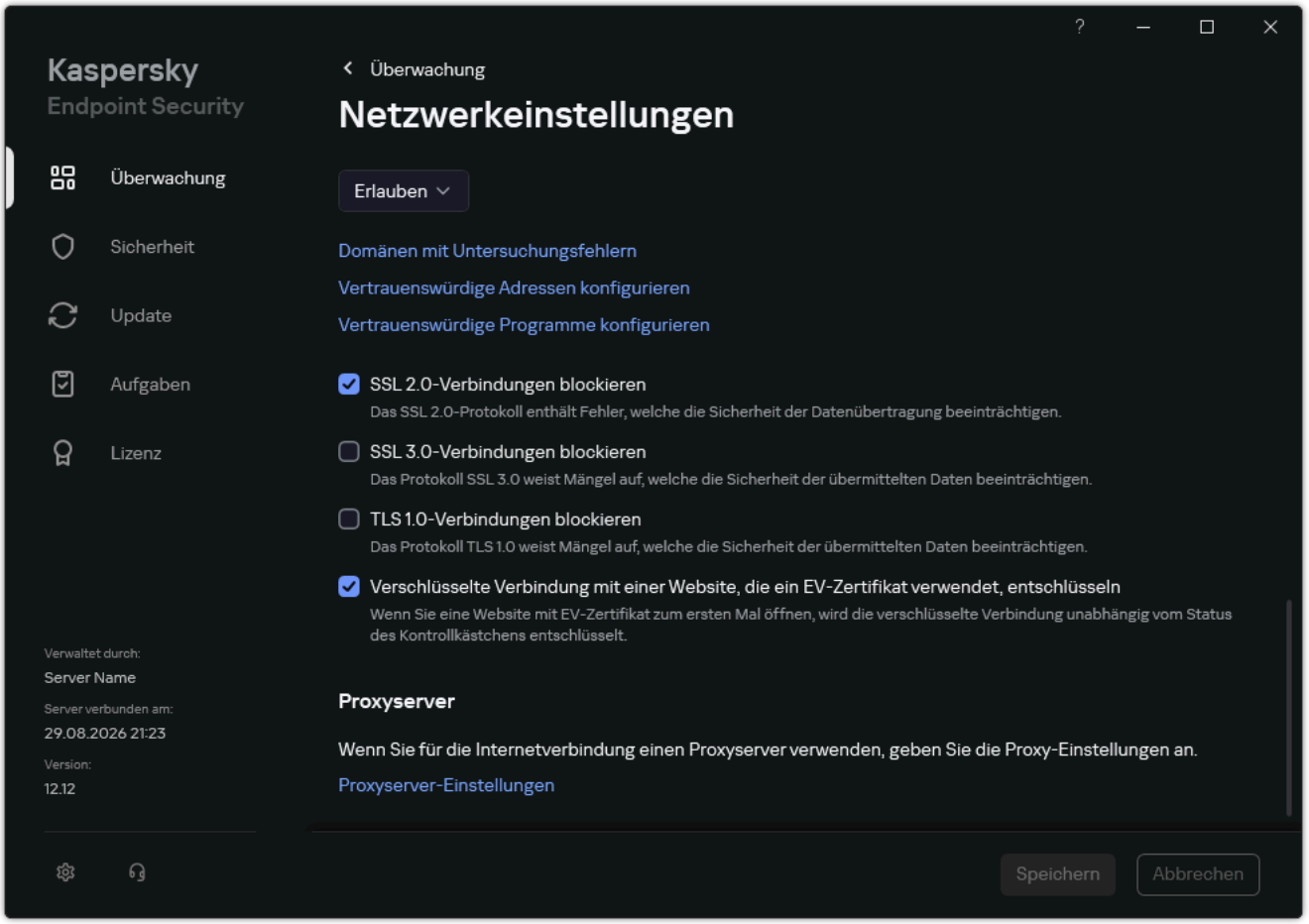
So fügen Sie über die Web Console und Cloud Console ein Webseiten-Interaktionsskript in den Web-Datenverkehr ein

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.
5. Aktivieren Sie unter **Überwachung von Internetverbindungen** den Schalter **Überwachung von Internetverbindungen AKTIVIERT**.
6. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie über die App- Benutzeroberfläche ein Webseiten-Interaktionsskript in den Web-Datenverkehr ein

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.



Netzwerkeinstellungen für die App

3. Aktivieren Sie im Block **Verarbeitung des Datenverkehrs** das Kontrollkästchen **Skript zur Interaktion mit Webseiten in den Web-Datenverkehr einbinden**.
4. Speichern Sie die vorgenommenen Änderungen.

Infolgedessen wird Kaspersky Endpoint Security ein Skript zur Interaktion mit Webseiten in den Web-Datenverkehr injizieren. Dieses Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen für die Ereignisanzeige des Programms, die Ereignisanzeige des Betriebssystems und Berichte.

Protokollierung von Ereignissen der „Web-Kontrolle“ konfigurieren

Um die Protokollierung von „Web-Kontrolle“-Ereignissen auf dem Benutzercomputer anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Benutzeroberfläche** aus.
3. Klicken Sie im Block **Meldungen** auf **Benachrichtigungen konfigurieren**.

4. Wählen Sie im folgenden Fenster den Abschnitt **Web-Kontrolle**.

   Eine Tabelle der „Web-Kontrolle“-Ereignisse und Benachrichtigungsmethoden wird geöffnet.

5. Passen Sie für jedes Ereignis eine Benachrichtigungsmethode an: **Im lokalen Bericht speichern** und **Im Windows-Ereignisprotokoll speichern**.

   Damit Ereignisse protokolliert werden, die sich auf den Besuch erlaubter Websites beziehen, muss die „Web-Kontrolle“ zusätzlich angepasst werden (s. Anleitung unten).

   In der Ereignistabelle können Sie außerdem eine Bildschirmbenachrichtigung und eine E-Mail-Benachrichtigung aktivieren. Für den Versand von E-Mail-Benachrichtigungen müssen die Einstellungen des SMTP-Servers angepasst werden. Weitere Informationen über den Versand von E-Mail-Benachrichtigungen finden Sie in der Hilfe zu Kaspersky Security Center.

6. Speichern Sie die vorgenommenen Änderungen.

Künftig protokolliert Kaspersky Endpoint Security die Ereignisse über die Internetaktivitäten des Benutzers.

Die „Web-Kontrolle“ sendet Ereignisse, welche die Benutzeraktivität betreffen, wie folgt an Kaspersky Security Center:

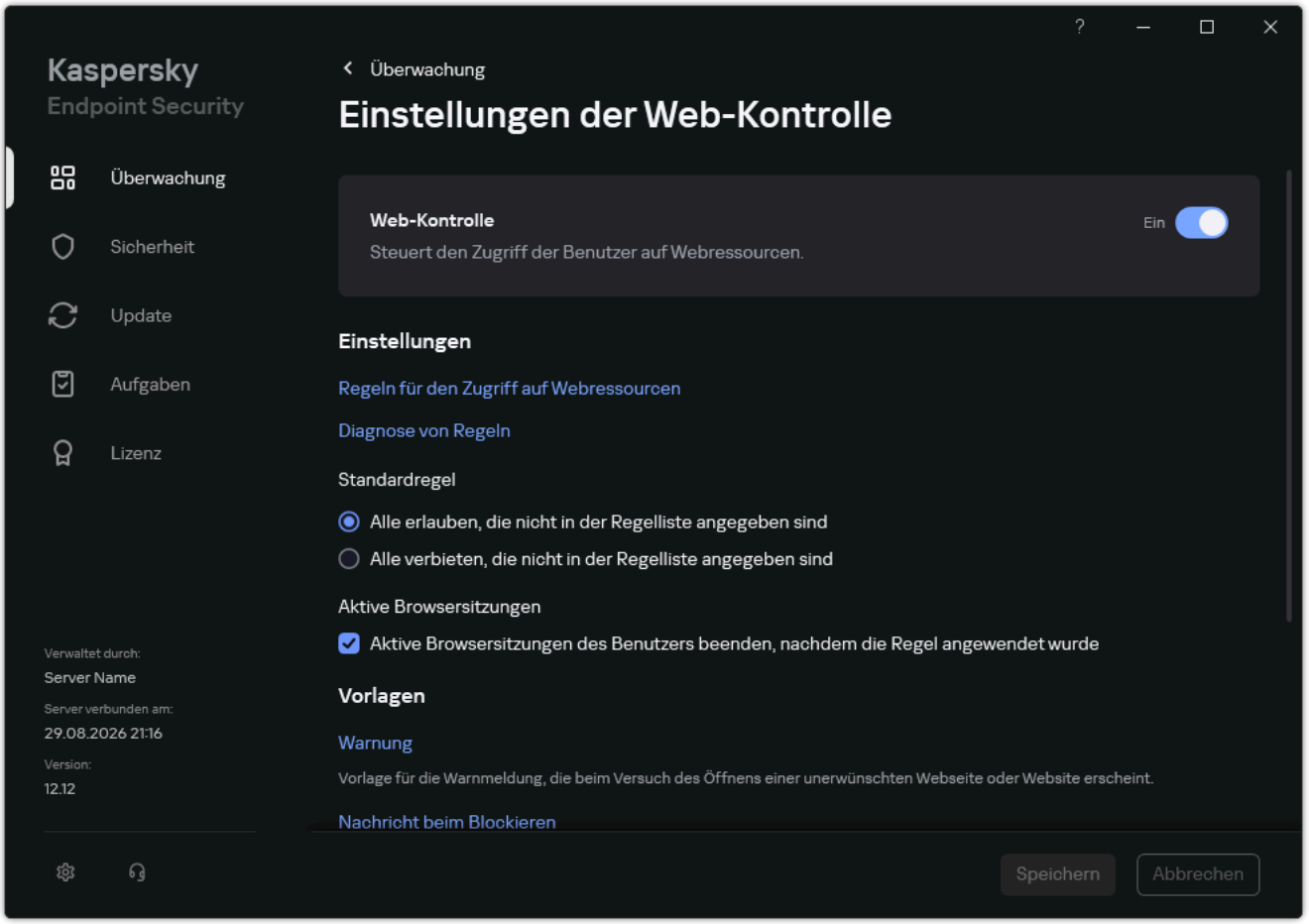
- Wenn Sie Kaspersky Security Center verwenden, sendet die „Web-Kontrolle“ Ereignisse über alle Objekte, aus denen eine Webseite besteht. Deshalb kann es sein, dass bei der Sperrung einer Webseite mehrere Ereignisse erstellt werden. Beispiel: Bei der Sperrung der Webseite http://www.example.com kann Kaspersky Endpoint Security Ereignisse über die folgenden Objekte senden: http://www.example.com, http://www.example.com/icon.ico, http://www.example.com/file.js und so weiter.

- Wenn Sie Kaspersky Security Center Cloud Console verwenden, gruppiert die „Web-Kontrolle“ die Ereignisse und sendet nur das Protokoll und die Domäne der Webseite. Wenn der Benutzer beispielsweise die nicht empfohlenen Webseiten http://www.example.com/main, http://www.example.com/contact und http://www.example.com/gallery besucht hat, sendet Kaspersky Endpoint Security nur ein Ereignis für das Objekt http://www.example.com.

Protokollierung von Ereignissen beim Besuch erlaubter Websites

So aktivieren Sie die Protokollierung von Ereignissen beim Besuch erlaubter Websites

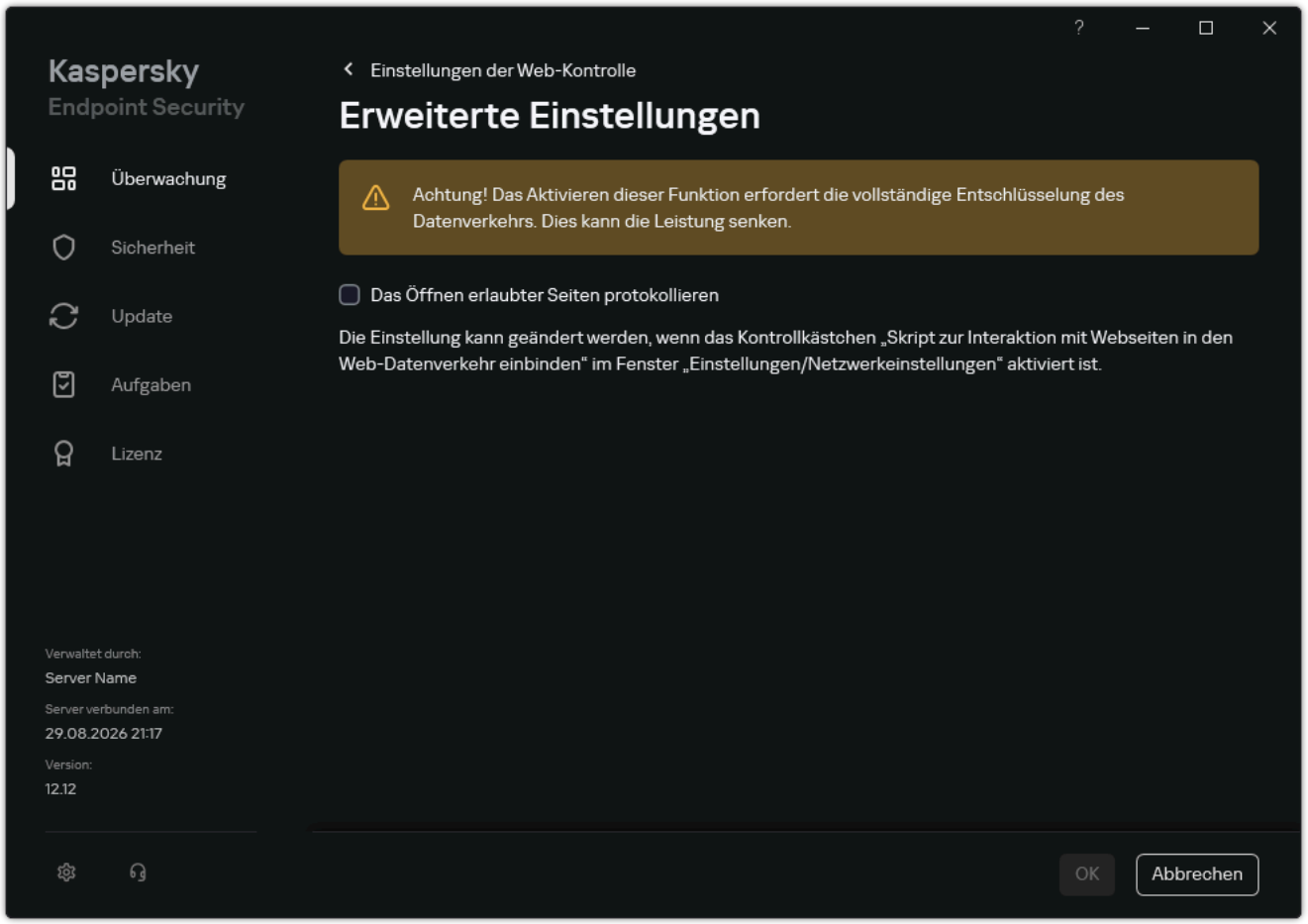
1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Klicken Sie im Block **Erweitert** auf **Erweiterte Einstellungen**.

4. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Das Öffnen erlaubter Seiten protokollieren**.



Erweiterte Einstellungen der „Web-Kontrolle”

5. Speichern Sie die vorgenommenen Änderungen.

Künftig können Sie einen vollständigen Verlauf aller im Browser besuchten Websites einsehen.

Meldungsvorlagen für die Web-Kontrolle ändern

Abhängig davon, welche Aktion in den Eigenschaften der Regeln für die Web-Kontrolle festgelegt ist, zeigt Kaspersky Endpoint Security beim Versuch eines Benutzers, Zugriff auf Webressourcen zu erhalten, eine Meldung an (die Antwort des HTTP-Servers wird durch eine HTML-Seite mit einer Meldung ersetzt). Folgende Meldungstypen sind möglich:

- Warnmeldung. Eine solche Meldung warnt den Benutzer, dass vom Besuch einer Webressource abgeraten wird und/oder der Besuch gegen die Sicherheitsrichtlinie des Unternehmens verstößt. Kaspersky Endpoint Security zeigt eine Warnmeldung an, wenn in den Einstellungen der Regel, die diese Webressource beschreibt, die Option **Warnen** ausgewählt ist.

  Hält der Benutzer die Warnung für einen Irrtum, so kann der Benutzer mit einem Link aus der Warnung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.

- Meldung über die Sperrung einer Webressource. Kaspersky Endpoint Security zeigt eine Meldung über die Sperrung einer Webressource an (siehe Abbildung unten), wenn in den Einstellungen der Regel, die diese Webressource beschreibt, die Option **Blockieren** ausgewählt ist.

Hält der Benutzer die Zugriffssperre auf eine Webressource für einen Irrtum, so kann der Benutzer mit einem Link aus der Sperrmeldung eine vorgefertigte Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken.



Nachricht über die Sperrung von Webressourcen

Für die Warnmeldung, für die Meldung über die Sperrung einer Webressource und für die Nachricht an den Administrator des lokalen Unternehmensnetzwerks sind Vorlagen vorgesehen. Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden. Wenn eine Nachricht generiert wird, ruft Kaspersky Endpoint Security den Wert der Variablen aus den Betriebssystemeinstellungen ab und fügt ihn passend zum Computer, Benutzer und Ereignis in die Nachricht ein.

So ändern Sie die Nachrichtenvorlage der Web-Kontrolle über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Web-Kontrolle** aus.
4. Klicken Sie im Block **Einstellungen für Nachrichtenvorlagen** auf **Vorlagen**.

5. Konfigurieren Sie die Nachrichtenvorlagen der Web-Kontrolle:

   - **Warnung**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die vor einem Zugriffsversuch auf eine nicht empfehlenswerte Webressource warnt.

   - **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 der Nachricht, die an den Administrator des lokalen Netzwerks gesendet wird, wenn der Zugriff nach Meinung des Benutzers irrtümlich blockiert wurde. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Zugriffsverbot auf Webseite**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable** und wählen Sie die gewünschte Variable in der Liste aus.

   Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Standard** wiederherstellen.

6. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie die Nachrichtenvorlage der Web-Kontrolle in der Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle → Web-Kontrolle**.

5. Klicken Sie im Block **Vorlagen für Nachrichten** auf den Link **Nachricht beim Blockieren einer Website** und konfigurieren Sie die Vorlagen für Nachrichten der Web-Kontrolle:

   - **Warnung**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die vor einem Zugriffsversuch auf eine nicht empfehlenswerte Webressource warnt.

   - **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 der Nachricht, die an den Administrator des lokalen Netzwerks gesendet wird, wenn der Zugriff nach Meinung des Benutzers irrtümlich blockiert wurde. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Zugriffsverbot auf Webseite**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

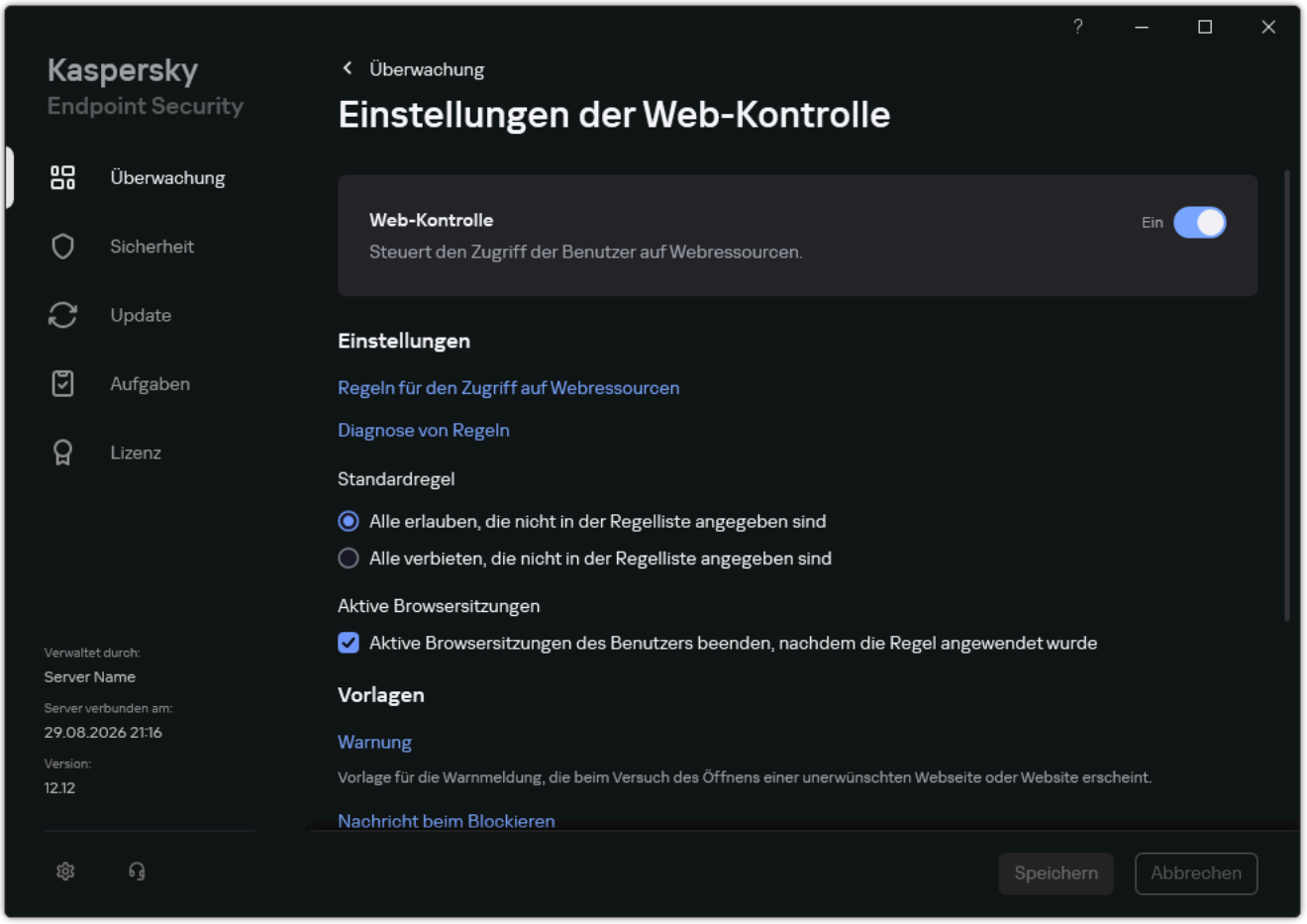
Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Auf Standard zurücksetzen** wiederherstellen.

6. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie die Nachrichtenvorlage der Web-Kontrolle über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Web-Kontrolle** aus.



Einstellungen der Web-Kontrolle

3. Konfigurieren Sie im Block **Vorlagen** die Vorlagen für Nachrichten der Web-Kontrolle:

   - **Warnung**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die vor einem Zugriffsversuch auf eine nicht empfehlenswerte Webressource warnt.

   - **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 der Nachricht, die an den Administrator des lokalen Netzwerks gesendet wird, wenn der Zugriff nach Meinung des Benutzers irrtümlich blockiert wurde. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Zugriffsverbot auf Webseite**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Zurücksetzen** wiederherstellen.

4. Speichern Sie die vorgenommenen Änderungen.

Regeln für das Erstellen von Adressmasken für Webressourcen

Die Verwendung einer *Adressmaske für eine Webressource* (im Folgenden „Adressmaske“) bietet sich an, wenn eine Zugriffsregel für Webressourcen erstellt wird, für die eine hohe Anzahl ähnlicher Adressen für Webressourcen angegeben werden soll. Eine korrekt formulierte Adressmaske kann eine Vielzahl von Webressourcen ersetzen.

Für das Erstellen einer Adressmaske sind folgende Regeln zu beachten:

1. Das Zeichen `*` ersetzt eine beliebige Abfolge aus null oder mehr Zeichen.

   Beispielsweise wird bei Angabe der Adressmaske `*abc*` die Zugriffsregel für Webressourcen auf alle Adressen angewendet, welche die Zeichenfolge `abc` enthalten. Beispiel: `http://www.example.com/page_0-9abcdef.html`.

2. Mithilfe einer Abfolge des Zeichens `*.` (auch *Domänenmaske* genannt) können Sie alle Domänen einer Adresse auswählen. Die Domänenmaske `*.` ersetzt einen beliebigen Domänennamen, einen Subdomänennamen oder eine leere Zeile.

   Beispiel: Die Maske `*.example.com` steht für die folgenden Adressen:

   - `http://pictures.example.com`. Die Domänenmaske `*.` steht für `pictures.`
   - `http://user.pictures.example.com`. Die Domänenmaske `*.` steht für `pictures.` und `user.`
   - `http://example.com`. Die Domänenmaske `*.` wird als Leerzeile interpretiert.

3. Die Zeichenfolge `www.` zu Beginn der Adressmaske wird wie `*.` behandelt.

   Beispiel: Die Adressmaske `www.example.com` wird wie `*.example.com` behandelt. Diese Maske schließt die Adressen `www2.example.com` und `www.pictures.example.com` ein.

4. Beginnt eine Adressmaske nicht mit dem Zeichen `*`, entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Präfix `*.`.

5. Endet eine Adressmaske mit einem anderen Zeichen als `/` oder `*`, so entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Postfix `/*`.

   Beispiel: Die Adressmaske `http://www.example.com` schließt Adressen der Form `http://www.example.com/abc` ein, wobei `a`, `b`, `c` für beliebige Zeichen stehen.

6. Endet eine Adressmaske mit dem Zeichen `/`, so entspricht der Inhalt dieser Adressmaske dem gleichen Inhalt mit dem Postfix `/*`.

7. Die Zeichenfolge `/*` am Ende einer Adressmaske wird wie `/*` oder als leere Zeile behandelt.

8. Eine Untersuchung von Adressen für Webressourcen nach einer Adressmaske erfolgt unter Berücksichtigung des Schemas (http oder https):

   - Enthält eine Adressmaske kein Netzwerkprotokoll, erstreckt sich die Adressmaske auf eine Adresse mit beliebigem Netzwerkprotokoll.

     Beispiel: Die Adressmaske `example.com` schließt die Adressen `http://example.com` und `https://example.com` ein.

- Enthält eine Adressmaske ein Netzwerkprotokoll, erstreckt sich die Adressmaske nur auf Adressen mit dem in der Adressmaske genannten Netzwerkprotokoll.

  Beispiel: Die Adressmaske `http://*.example.com` schließt die Adresse `http://www.example.com` ein, während die Adresse `https://www.example.com` nicht darunter fällt.

9. Eine Adressmaske, die in doppelten Anführungszeichen steht, wird ungeachtet zusätzlicher Substitutionen behandelt. Eine Ausnahme bildet das Zeichen `*`, falls es in der Adressmaske enthalten ist. Für Adressmasken, die in doppelten Anführungszeichen stehen, werden die Regeln 5 und 7 nicht ausgeführt (s. Beispiele 14 – 18 in folgender Tabelle).

10. Beim Vergleich mit der Adressmaske für eine Webressource bleiben Benutzername und Kennwort, Verbindungsport sowie Groß- und Kleinschreibung unberücksichtigt.

Praktische Beispiele für die Regeln zum Erstellen von Adressmasken

Nr.	Adressmaske	Zu untersuchende Adresse für eine Webressource	Die zu untersuchende Adresse entspricht 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 und 1.
7	www.example.com	https://www.example.com	Ja	Siehe Regeln 3, 2 und 1.
8	http://www.*.example.com	http://123.example.com	Ja	Siehe Regeln 3, 4 und 1.
9	www.example.com	http://www.example.com/abc	Ja	Siehe Regeln 3, 5 und 1.
10	example.com	http://www.example.com	Ja	Siehe Regeln 3 und 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 und 9.
17	„http://www.example.com/*“	http://www.example.com/abc	Ja	Siehe Regeln 1 und 9.
18	„www.example.com“	http://www.example.com; https://www.example.com	Ja	Siehe Regeln 9 und 8.
19	www.example.com/abc/123	http://www.example.com/abc	Nein	Eine Adressmaske enthält mehr Informationen als die Adresse einer Webressource.

Web-Kontrolle für virtuelle Maschinen

Die Web-Kontrolle kontrolliert den Datenverkehr sowohl auf dem Computer als auch auf einer virtuellen Maschine, die lokal auf dem Computer bereitgestellt wird. Dies funktioniert, ohne dass Kaspersky Endpoint Security auf der lokalen virtuellen Maschine installiert werden muss. Wenn der Benutzer also versucht, in einem Browser auf der *virtuellen Maschine* eine Website zu öffnen, die durch eine Regel der Web-Kontrolle gesperrt ist, verweigert die auf dem Host-Betriebssystem des *Computers* installierte App den Zugriff auf diese Website.

Die Funktionen der Web-Kontrolle unterscheiden sich je nach virtueller Maschine.

Oracle VM VirtualBox

Kaspersky Endpoint Security unterstützt die Regeln der Web-Kontrolle auf virtuellen Maschinen von Oracle VM VirtualBox ohne Einschränkungen. Die App kann den gesamten Datenverkehr der virtuellen Maschine kontrollieren. Wenn in den Regeln der Web-Kontrolle ein Filter nach Benutzern konfiguriert ist, funktioniert die App ordnungsgemäß, da alle Prozesse der virtuellen Maschinen vom lokalen Benutzer gestartet werden.

VMware Workstation

Kaspersky Endpoint Security unterstützt die Regeln der Web-Kontrolle auf virtuellen Maschinen von VMware Workstation mit Einschränkungen. Regeln, in denen ein Filter nach Benutzern konfiguriert ist, werden von der App nicht unterstützt. Die Prozesse der virtuellen Maschine werden unter dem Konto des Systembenutzers (SYSTEM) ausgeführt. Dadurch kann ein Benutzer nicht identifiziert werden, der versucht, die Website auf der virtuellen Maschine zu öffnen.

Microsoft Hyper-V

Regeln der Web-Kontrolle werden von Kaspersky Endpoint Security auf virtuellen Maschinen von Microsoft Hyper-V nicht unterstützt.

Variablen in Nachrichtenvorlagen der Web-Kontrolle

In Vorlagen für Nachrichten an Benutzer oder an den Administrator können Sie die folgenden Variablen verwenden:

- **Benutzername** – `%USER_NAME%`.

  Name des aktuellen Benutzerkontos auf dem Computer, auf dem die Nachricht erstellt wurde, im Format `<Gerätename>\<Benutzeralias>` (z. B. `DESKTOP-123\John.Smith`).

- **Adresse der Webseite** – `%CANONIC_REQUEST_URL%`.

  Adresse der blockierten Webressource.

- **Regelname** – `%RULE%`.

  Name der Regel, durch die eine Webressource blockiert wurde.

- **Empfängeradresse für die Nachricht** – `%COMPLAIN_EMAIL%`.

  E-Mail-Adresse für das Feedback über blockierte Webressourcen. Durch Klick auf die E-Mail-Adresse wird ein Fenster geöffnet, in dem der Benutzer eine Nachricht an den Administrator schreiben kann.

- **Name der Inhaltskategorie** – `%CONTENT_CATEGORY_LIST%`.

  Website-Kategorie, zu der die blockierte Ressource gehört (z. B. *Zahlungssysteme*).

- **Name der Datentypkategorie** – `%TYPE_CATEGORY_LIST%`.

  Kategorie für den Typ der Daten, die sich auf der blockierten Webressource befinden (z. B. *Bilddateien*).

- **Link zur angeforderten Webseite** – `%CONTINUE_PAGE%`.

  Link zur angeforderten Webseite (z. B. `http://www.example.com/pagename.html`).

- **Link zur Website** – `%CONTINUE_SITE%`.

  Link zur Website, die die angeforderte Webseite enthält (z. B. `http://www.example.com/`).

- **Link für den Zugriff auf Domänen** – `%CONTINUE_DOMAIN%`.

  Durch Klick auf diesen Link kann auf alle vorhandenen Webseiten des Domänennamens zugegriffen werden. Beispiel: Wenn die Adresse der blockierten Webseite `http://www.example.com` lautet, wird die Variable `%CONTINUE_DOMAIN%` durch den Link `http://*.example.com` ersetzt. Mit diesem Link können Sie auf alle Webadressen des zugrunde liegenden Domänennamens `http://www.example.com/` zugreifen, auch auf untergeordnete Domänen wie z. B. `http://start.example.com/*` oder `http://domain.domain.example.com/*`. Dabei steht das Zeichen `*` für eine beliebige Zeichenfolge (einschließlich einer leeren Zeichenfolge).

Gerätekontrolle

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.

Wenn die Gerätekontrolle aktiviert ist, leitet das Programm Informationen über angeschlossene Geräte an Kaspersky Security Center weiter. Die Liste der verbundenen Geräte können Sie in Kaspersky Security Center im Ordner **Erweitert** → **Datenverwaltung** → **Hardware** ansehen.

Ebenen für den Zugriff auf Geräte

Die „Gerätekontrolle“ verwaltet den Zugriff auf folgenden Ebenen:

- **Gerätetyp**. Beispielsweise Drucker, Wechseldatenträger, CD/DVD-Laufwerke.

Sie können den Zugriff auf Geräte wie folgt anpassen:

- Erlauben – .
- Blockieren – .
- Nach Regeln (nur Drucker und tragbare Geräte) – .
- Von Verbindungsschnittstelle abhängig (außer WLAN) – .
- Verbieten mit Ausnahmen (nur WLAN) – .

- **Schnittstellen**. Mithilfe einer *Verbindungsschnittstelle* können Geräte mit einem Computer verbunden werden (z. B. via USB oder FireWire). Wenn der Modus **Von Verbindungsschnittstelle abhängig** für den Gerätetyp ausgewählt ist, erlaubt oder verbietet die App den Zugriff auf das Gerät abhängig von der Verbindungsschnittstelle (z. B. USB).

  Sie können den Zugriff auf Geräte wie folgt anpassen:

  - Erlauben – .
  - Blockieren – .

- **Vertrauenswürdige Geräte**. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

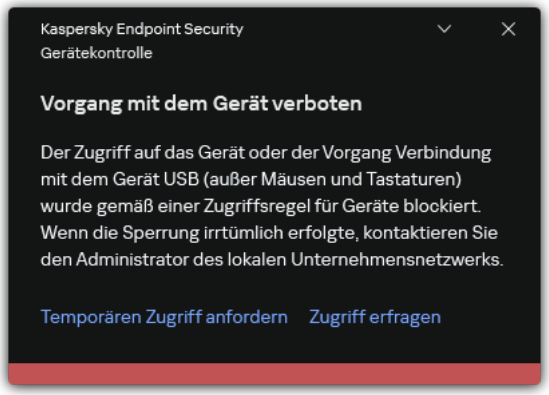
  Sie können vertrauenswürdige Geräte mithilfe der folgenden Daten hinzufügen:

  - **Geräte nach 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.
  - **Geräte nach Modell**. Jedes Gerät besitzt eine Vendor ID (VID) und eine 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.
  - **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 `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.
  - **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 `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `VID_05AC&PID_*`.

Die „Gerätekontrolle“ verwendet *Zugriffsregeln*, um den Zugriff von Benutzern auf Geräte zu regulieren. Außerdem kann die „Gerätekontrolle“ Ereignisse über die Verbindung/Trennung von Geräten speichern. Damit Ereignisse gespeichert werden, müssen Sie in der Richtlinie das Senden von Ereignissen anpassen.

Falls der Zugriff auf das Gerät von der Schnittstelle abhängig ist (Status), werden Ereignisse über die Verbindung/Trennung des Geräts nicht von Kaspersky Endpoint Security gespeichert. Damit das Programm Kaspersky Endpoint Security Ereignisse über die Verbindung/Trennung des Geräts speichert, erlauben Sie den Zugriff auf den entsprechenden Gerätetyp (Status) oder fügen Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

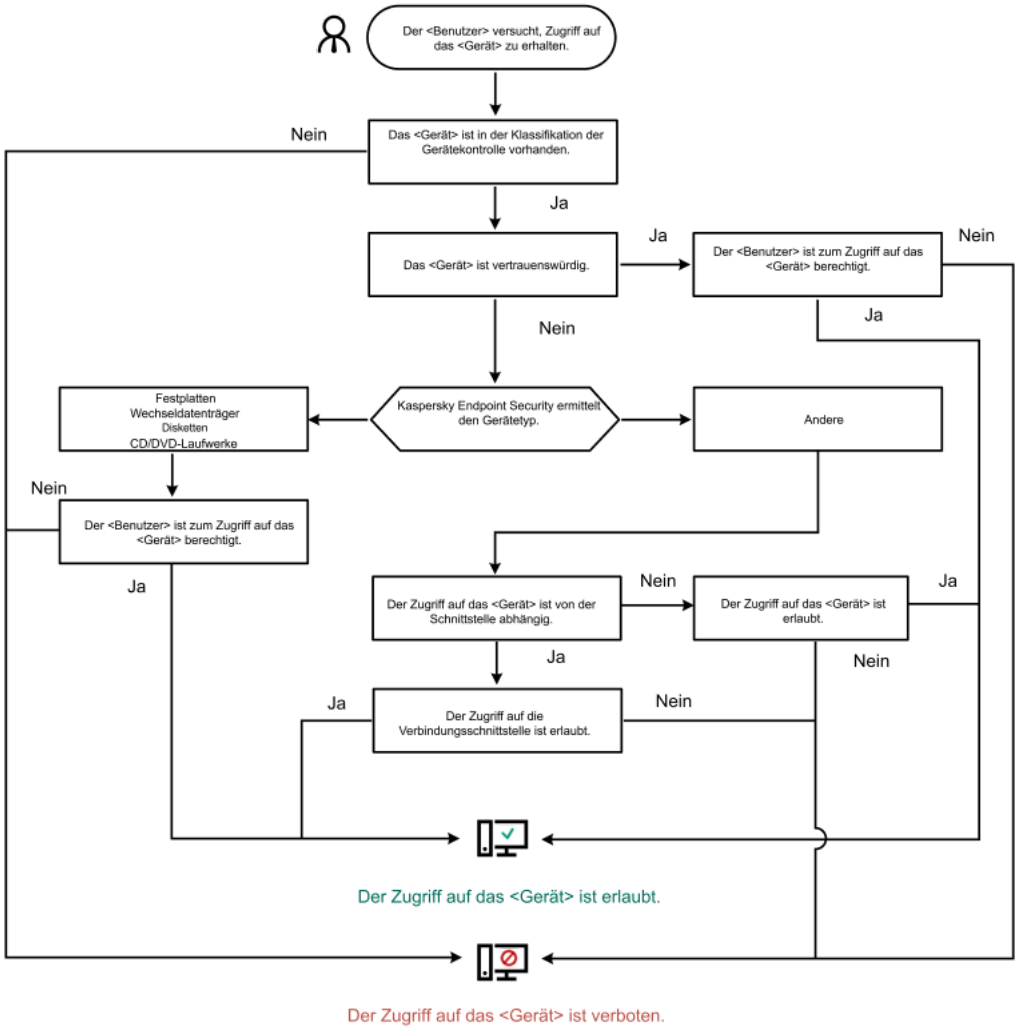
Wird mit dem Computer ein Gerät verbunden, auf das der Zugriff von der „Gerätekontrolle“ verboten ist, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Benachrichtigung an (s. Bild unten).



Benachrichtigung der „Gerätekontrolle“

Algorithmus der „Gerätekontrolle”

Kaspersky Endpoint Security entscheidet über den Zugriff auf ein Gerät, sobald dieses vom Benutzer an den Computer angeschlossen wird (s. folgende Abb.).



Algorithmus der „Gerätekontrolle”

Wenn ein Gerät verbunden ist und der Zugriff erlaubt ist, können Sie die Zugriffsregel ändern und den Zugriff verbieten. Wenn das nächste Mal auf das Gerät zugegriffen wird (Anzeige der Ordnerstruktur, Lesen, Schreiben), blockiert Kaspersky Endpoint Security den Zugriff. Geräte ohne Dateisystem werden erst blockiert, wenn sie zum nächsten Mal mit dem Computer verbunden werden.

Wenn der Benutzer eines Computers, auf dem das Programm Kaspersky Endpoint Security installiert ist, den Zugriff auf ein Gerät angefordert hat, das seiner Meinung nach irrtümlicherweise blockiert wurde, so übermitteln Sie ihm eine Anleitung für die Zugriffsanforderung.

Über Zugriffsregeln

Eine *Gerätezugriffsregel* ist eine Gruppe von Einstellungen, mit deren Hilfe Benutzer auf installierte oder an den Computer angeschlossene Geräte zugreifen können. Zu diesen Einstellungen gehören der Zugriff auf ein bestimmtes Gerät, ein Zugriffszeitplan sowie Lese- oder Schreibberechtigungen. Ein Gerät, das nicht zur Klassifikation der „Gerätekontrolle“ gehört, kann nicht hinzugefügt werden. Der Zugriff auf diese Geräte ist für alle Benutzer erlaubt.

Regeln für den Zugriff auf Geräte

Die Auswahl der Einstellungen für eine Zugriffsregel ist vom Gerätetyp abhängig (siehe folgende Tabelle).

Einstellungen für eine Zugriffsregel

Geräte	Zugangskontrolle	Zeitplan für den Zugriff auf ein Gerät	Zuweisung von Benutzern / einer Benutzergruppe	Priorität	Erlaubnis zum Lesen/Schreiben
Festplatten	✓	✓	✓	✓	✓
Wechseldatenträger (einschließlich USB-Sticks)	✓	✓	✓	✓	✓
Disketten	✓	✓	✓	✓	✓
CD/DVD-Laufwerke	✓	✓	✓	✓	✓
Tragbare Geräte (MTP)	✓	✓	✓	✓	✓
Lokale Drucker	✓	–	✓	✓	–
Netzwerkdrucker	✓	–	✓	✓	–
Modems	✓	–	–	–	–
Bandlaufwerke	✓	–	–	–	–
Multifunktionsgeräte	✓	–	–	–	–
Smartcard-Leser	✓	–	–	–	–
Windows CE USB ActiveSync-Geräte	✓	–	–	–	–
Externe Netzwerkadapter	✓	–	–	–	–
Bluetooth	✓	–	–	–	–
Kameras und Scanner	✓	–	–	–	–

Regeln für den Zugriff auf WLAN-Netzwerke

Eine Regel für den Zugriff auf WLAN-Netzwerke legt die Erlaubnis (Status ✓) oder das Verbot (Status ⊘) für die Verwendung von WLAN-Netzwerken fest. Sie können ein *vertrauenswürdiges WLAN-Netzwerk* (Status ▣) zu einer Regel hinzufügen. Verwendung eines vertrauenswürdigen WLAN-Netzwerks ohne Beschränkungen. Eine Regel für den Zugriff auf ein WLAN-Netzwerk erlaubt standardmäßig den Zugriff auf ein beliebiges WLAN-Netzwerk.

Regeln für den Zugriff auf Verbindungsschnittstellen

Wenn der Wert **Von Verbindungsschnittstelle abhängig** für die Zugriffsregel nach Gerätetyp ausgewählt ist, erlaubt oder verweigert die App den Zugriff auf das Gerät abhängig von der Verbindungsschnittstelle. Für alle Schnittstellen aus der Klassifikation der Komponente „Gerätekontrolle" sind standardmäßige Regeln erstellt, die den Zugriff auf die Schnittstellen erlauben.

Regeln für den Zugriff auf Schnittstellen legen nur die Erlaubnis (Status ✓) oder das Verbot (Status ⊘) für die Verbindung mit Geräten fest. Zugriffsregeln für Gerätetypen haben eine höhere Priorität als Zugriffsregeln für Verbindungsschnittstellen.

Tastatur und Maus können über die „Gerätekontrolle" nicht gesperrt werden. Wenn Sie den Zugriff auf die USB-Schnittstelle verbieten, kann der Benutzer eine über USB verbundene Tastatur und Maus weiterhin verwenden. Die Komponente Schutz vor modifizierten USB-Geräten dient dazu, Verbindungen mit infizierten USB-Geräten zu verhindern, die Tastaturen imitieren.

Abrufen von Informationen über installierte Geräte

Kaspersky Security Center erhält Informationen über installierte Geräte von folgenden Anbietern: Administrationsagent und Kaspersky Endpoint Security. Informationen über installierte Geräte werden für die Zugriffsverwaltung und die Erstellung einer Liste vertrauenswürdiger Geräte benötigt.

Informationen zur Computerhardware

Wenn der Administrationsagent auf einem Windows-Gerät installiert ist, sendet er die folgenden Informationen über die Hardware des Geräts an den Administrationsserver:

- Arbeitsspeicher
- Speichergeräte (einschließlich Festplatten)
- Hauptplatine
- Prozessor
- Netzwerkadapter
- Monitore
- GPU
- Soundkarte

Der Administrationsagent stellt diese Informationen bei jeder Synchronisierung mit Kaspersky Security Center bereit. Sie können die Hardware eines Computers in den Eigenschaften des Computers anzeigen (**Hardware-Registry**).

Hardwareinformationen

Kaspersky Endpoint Security stellt Informationen über installierte Hardware bereit: Drucker, Wechseldatenträger, tragbare Geräte (MTP) usw. Um Hardwareinformationen zu erhalten, müssen Sie eine aktive Richtlinie anwenden, die die Übertragung von Informationen über installierte Geräte erlaubt (diese Übertragung ist standardmäßig aktiviert).

So aktivieren Sie die Übertragung von Informationen über installierte Geräte in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Berichte und Speicher** aus.
5. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Einstellungen**.
6. Aktivieren Sie das Kontrollkästchen **Installierte Geräte**.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Übertragung von Informationen über installierte Geräte in der Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → KSC-Integration**.
5. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Erweiterte Einstellungen**.
6. Aktivieren Sie das Kontrollkästchen **Über installierte Geräte**.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Anschließend können Sie die Liste der installierten Geräte in der Konsole von Kaspersky Security Center anzeigen (**Datenverwaltung → Hardware**).

Zugriff auf Geräte nach Typ verwalten

Mit der Gerätekontrolle können Sie den Zugriff auf Geräte nach Typ verwalten. Beim Anschließen eines Geräts bestimmt das Betriebssystem den Gerätetyp. Den Gerätetyp können Sie im Geräte-Manager des Betriebssystems nachsehen. Um den Zugriff auf Geräte zu verwalten, müssen Sie Regeln konfigurieren. Eine *Gerätezugriffsregel* ist eine Gruppe von Einstellungen, mit deren Hilfe Benutzer auf installierte oder an den Computer angeschlossene Geräte zugreifen können. Zu diesen Einstellungen gehören der Zugriff auf ein bestimmtes Gerät, ein Zugriffszeitplan sowie Lese- oder Schreibberechtigungen. Ein Gerät, das nicht zur Klassifikation der „Gerätekontrolle“ gehört, kann nicht hinzugefügt werden. Der Zugriff auf diese Geräte ist für alle Benutzer erlaubt.

Standardmäßig erlaubt die Gerätekontrolle allen Benutzern den Zugriff auf alle Geräte.

Sie können den Zugriff auf Geräte wie folgt konfigurieren:

- **Erlauben**.

  Kaspersky Endpoint Security gewährt allen Benutzern vollständigen Zugriff auf Geräte.

- **Verbieten**.

  Kaspersky Endpoint Security blockiert Verbindungen mit Geräten. Das Programm erlaubt nur Verbindungen mit vertrauenswürdigen Geräten.

- **Von Verbindungsschnittstelle abhängig**.

  Kaspersky Endpoint Security ermittelt die Verbindungsschnittstelle der Geräte und beschränkt den Zugriff auf die Geräte je nach Status der Verbindungsschnittstelle. Das Programm erlaubt auch Verbindungen mit vertrauenswürdigen Geräten.

- **Nach Regeln**.

  Für einige Gerätetypen können Sie einzelnen Benutzern oder einer Benutzergruppe die Verwendung von Geräten erlauben, einen Zeitplan für den Zugriff auf Geräte einrichten und die Lese- und Schreibberechtigungen konfigurieren. Das Programm erlaubt auch Verbindungen mit vertrauenswürdigen Geräten.

Gehen Sie vorsichtig vor, wenn Sie den Zugriff auf Geräte des Typs **Festplatten** konfigurierten. Wenn Sie den Zugriff auf die Systemfestplatte blockieren, kann das Programm beim Starten des Betriebssystems einen Absturz (BSOD) verursachen.

Wenn ein Gerät nicht in das Klassifizierungsschema der Gerätekontrolle passt, kann der Zugriff auf dieses Gerät nicht eingeschränkt werden.

So verwalten Sie den Zugriff auf Geräte nach Typ (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.

6. Konfigurieren Sie Zugriffsregeln für Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Verbieten**, **Von Verbindungsschnittstelle abhängig**, **Nach Regeln**.

      Zur Auswahl des Zugriffsmodus **Nach Regeln** doppelklicken Sie, um die Eigenschaften der Zugriffsregel zu öffnen.

   b. Wenn Sie die den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** auswählen, müssen Sie auf der Registerkarte **Verbindungsschnittstellen** die Zugriffsregeln für Verbindungsschnittstellen konfigurieren.

   c. Bei Speichergeräten (z. B. Wechseldatenträger) können Sie die Zugriffsberechtigungen für einzelne Benutzer konfigurieren. Sie können auch einen Zeitplan für den Zugriff auf Geräte einrichten und Lese- und Schreibberechtigungen konfigurieren.

      Sie können Geräte zur vertrauenswürdigen Liste hinzufügen. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

   d. Konfigurieren Sie die Druckregeln (falls erforderlich).

   e. Konfigurieren Sie die Zugriffsregeln für Bluetooth-Geräte (falls erforderlich).

   f. Konfigurieren Sie die Regeln für die WLAN-Verbindung des Computers (falls erforderlich).

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Zugriff auf Geräte nach Typ (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.

5. Wählen Sie unter **Regeln für den Zugriff auf Geräte** die Registerkarte **Geräte und WLAN-Netzwerke** aus.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.

6. Konfigurieren Sie Zugriffsregeln für Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Je nach Schnittstelle**, **Benutzerdefiniert**.

      Wenn der Zugriffsmodus im Dropdown-Menü nicht vorhanden ist, doppelklicken Sie auf den Gerätetyp, um die Eigenschaften der Zugriffsregel zu öffnen.

   b. Wenn Sie die den Zugriffsmodus **Je nach Schnittstelle** auswählen, müssen Sie auf der Registerkarte **Verbindungsschnittstellen** die Zugriffsregeln für Verbindungsschnittstellen konfigurieren.

c. Bei Speichergeräten (z. B. Wechseldatenträger) können Sie die Zugriffsberechtigungen für einzelne Benutzer konfigurieren. Sie können auch einen Zeitplan für den Zugriff auf Geräte einrichten und Lese- und Schreibberechtigungen konfigurieren.

Sie können Geräte zur vertrauenswürdigen Liste hinzufügen. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

d. Konfigurieren Sie die Druckregeln (falls erforderlich).

e. Konfigurieren Sie die Zugriffsregeln für Bluetooth-Geräte (falls erforderlich).

f. Konfigurieren Sie die Regeln für die WLAN-Verbindung des Computers (falls erforderlich).

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So verwalten Sie den Zugriff auf Geräte (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf den Link **Geräte und WLAN-Netzwerke**.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.
4. Konfigurieren Sie Zugriffsregeln für Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Verbieten**, **Von Verbindungsschnittstelle abhängig**, **Nach Regeln**.

   Wenn der Zugriffsmodus im Dropdown-Menü nicht vorhanden ist, doppelklicken Sie auf den Gerätetyp, um die Eigenschaften der Zugriffsregel zu öffnen.

   b. Wenn Sie die den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** auswählen, müssen Sie auf der Registerkarte **Verbindungsschnittstellen** die Zugriffsregeln für Verbindungsschnittstellen konfigurieren.

   c. Bei Speichergeräten (z. B. Wechseldatenträger) können Sie die Zugriffsberechtigungen für einzelne Benutzer konfigurieren. Sie können auch einen Zeitplan für den Zugriff auf Geräte einrichten und Lese- und Schreibberechtigungen konfigurieren.

   Sie können Geräte zur vertrauenswürdigen Liste hinzufügen. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

   d. Konfigurieren Sie die Druckregeln (falls erforderlich).

   e. Konfigurieren Sie die Zugriffsregeln für Bluetooth-Geräte (falls erforderlich).

   f. Konfigurieren Sie die Regeln für die WLAN-Verbindung des Computers (falls erforderlich).
5. Speichern Sie die vorgenommenen Änderungen.

Wenn ein Benutzer versucht, auf ein Gerät zuzugreifen, blockiert das Programm den Zugriff gemäß den Regeln. Außerdem protokolliert Kaspersky Endpoint Security ein entsprechendes Ereignis. Wenn Sie einzelnen Geräten Zugriff gewähren möchten, können Sie diese Geräte zur Liste der vertrauenswürdigen Geräte hinzufügen.

Zugriff auf Geräte nach Verbindungsschnittstelle verwalten

Gehen Sie folgendermaßen vor, um eine Zugriffsregel für eine Schnittstelle zu ändern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Verbindungsschnittstellen**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.
4. Wählen Sie eine Zugriffsregel, die geändert werden soll.
5. Wählen Sie in der Spalte **Zugriff**, ob Sie den Zugriff auf die Schnittstelle erlauben oder verweigern möchten: **Erlauben** oder **Blockieren**.

   Wenn Sie den Zugriff auf die Schnittstelle **Serieller Anschluss** (COM) oder **Paralleler Anschluss** (LPT) geändert haben, müssen Sie den Computer neu starten, um die Zugriffsregel zu aktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

Differenzierung von Benutzerrechten für den Zugriff auf Geräte

Sie können die Benutzerzugriffsrechte nach Gerätetyp oder nach vertrauenswürdigen Geräten konfigurieren.

Differenzierung von Benutzerzugriffsrechten nach Gerätetyp

Mit der Gerätekontrolle können Sie die Benutzerzugriffsrechte für Daten auf *Speichergeräten* konfigurieren. Für solche Geräte können Sie Schreib- und Leseberechtigungen konfigurieren. Die Gerätekontrolle unterstützt die folgenden Typen von *Speichergeräten*:

- Festplatten
- Wechseldatenträger (einschließlich USB-Sticks)
- Disketten
- CD/DVD-Laufwerke
- Tragbare Geräte (MTP) – Zu den tragbaren Geräten (MTP) gehören beispielsweise mobile Geräte, Fotoapparate und Mediaplayer.

Auf diese Weise können Sie beispielsweise festlegen, dass Wechseldatenträger nur von der Gruppe Administratoren verwendet werden dürfen. Für andere Gerätetypen können Sie den Zugriff für alle Benutzer verbieten oder erlauben. Sie können auch Benutzerzugriffsrechte für die Verwendung von Druckern konfigurieren.

So konfigurieren Sie die Benutzerzugriffsrechte für Daten auf Speichergeräten (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.
5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.
6. Um Zugriffsregeln für Speichergeräte zu konfigurieren, doppelklicken auf die Regelliste.
7. Konfigurieren Sie die Zugriffsregel für Speichergeräte:

   a. Klicken Sie im Block **Zugriffsregeln** auf **Hinzufügen**.

   Dadurch wird ein Fenster geöffnet, in dem Sie eine neue Zugriffsregel für Speichergeräte hinzufügen können.

   b. Legen Sie im Feld **Priorität der Regel** die Priorität für das *Schreiben der Regel* fest. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben) und Priorität.

   Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

   Beispielsweise können Sie der Gruppe „Jeder" schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder" eine Priorität von 0 zu.

   Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

   c. Wählen Sie unter **Regel für Benutzer und Gruppen** die Benutzer oder Benutzergruppen aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   d. Klicken Sie auf **OK**.
8. Konfigurieren Sie unter **Zeitpläne für die ausgewählte Zugriffsregel** einen Zeitplan für den Zugriff auf Speichergeräte für die Benutzer.

   Sie können beispielsweise festlegen, dass Benutzer Speichergeräte nur während der Arbeitszeit verwenden dürfen.
9. Konfigurieren Sie die Benutzerberechtigungen für den Zugriff auf Speichergeräte im Dateimanager (**Lesen**/**Schreiben**).
10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Benutzerzugriffsrechte für Daten auf Speichergeräten (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Öffnen Sie im Block **Regeln für den Zugriff auf Geräte** in der Tabelle für Zugriffsregeln die Eigenschaften der Zugriffsregeln für Speichergeräte.
6. Wählen Sie im Block **Regeln für den Zugriff auf Geräte** die Variante **Benutzerdefiniert** aus.
7. Konfigurieren Sie die Zugriffsregel für Speichergeräte:

   a. Klicken Sie im Block **Benutzer und deren Rechte** auf **Hinzufügen**.

   Dadurch wird ein Fenster geöffnet, in dem Sie eine neue Zugriffsregel für Speichergeräte hinzufügen können.

   b. Legen Sie im Feld **Priorität** die Priorität für das *Schreiben der Regel* fest. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben) und Priorität.

   Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

   Beispielsweise können Sie der Gruppe „Jeder" schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder" eine Priorität von 0 zu.

   Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

   c. Wählen Sie unter **Benutzer oder Gruppe** die Benutzer oder Benutzergruppen aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   d. Konfigurieren Sie unter **Zugriffszeitplan** einen Zeitplan für den Zugriff auf Speichergeräte für die Benutzer.

   Sie können beispielsweise festlegen, dass Benutzer Speichergeräte nur während der Arbeitszeit verwenden dürfen.

   e. Konfigurieren Sie die Benutzerberechtigungen für den Zugriff auf Speichergeräte im Dateimanager (**Lesen**/**Schreiben**).

   f. Klicken Sie auf **Speichern**.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Benutzerzugriffsrechte für Daten auf Speichergeräten (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf den Link **Geräte und WLAN-Netzwerke**.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.
4. Um Zugriffsregeln für Speichergeräte zu konfigurieren, klicken Sie mit der rechten Maustaste auf die Regelliste.
5. Konfigurieren Sie die Zugriffsregel für Speichergeräte:

   a. Klicken Sie im Block **Benutzerrechte** auf **Hinzufügen**.

   Dadurch wird ein Fenster geöffnet, in dem Sie eine neue Zugriffsregel für Speichergeräte hinzufügen können.

   b. Legen Sie im Feld **Priorität** die Priorität für das *Schreiben der Regel* fest. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben) und Priorität.

   Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

   Beispielsweise können Sie der Gruppe „Jeder” schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren” Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder“ eine Priorität von 0 zu.

   Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

   c. Wählen Sie unter **Benutzer** die Benutzer oder Benutzergruppen aus. Sie können Benutzer in Active Directory auswählen oder einen lokalen Benutzernamen manuell eingeben. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   d. Klicken Sie auf **OK**.
6. Konfigurieren Sie unter **Zeitplan für den Zugriff auf Geräte** einen Zeitplan für den Zugriff auf Speichergeräte für die Benutzer.

   Sie können beispielsweise festlegen, dass Benutzer Speichergeräte nur während der Arbeitszeit verwenden dürfen.
7. Konfigurieren Sie die Benutzerberechtigungen für den Zugriff auf Speichergeräte im Dateimanager (**Lesen**/**Schreiben**).
8. Speichern Sie die vorgenommenen Änderungen.

Differenzierung von Benutzerrechten für den Zugriff auf vertrauenswürdige Geräte

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. Sie können die Benutzerzugriffsrechte in den Eigenschaften des vertrauenswürdigen Geräts konfigurieren.

Zugriff auf Mobilgeräte verwalten

Mit Kaspersky Endpoint Security können Sie den Zugriff auf Daten auf Android- und iOS-Mobilgeräten kontrollieren. Mobilgeräte gehören zur Kategorie der tragbaren Geräte (MTP). Um den Datenzugriff auf mobilen Geräten zu konfigurieren, müssen Sie daher die Zugriffseinstellungen für tragbare Geräte (MTP) bearbeiten.

Wenn ein mobiles Gerät mit dem Computer verbunden wird, ermittelt das Betriebssystem den Gerätetyp. Wenn auf dem Computer Programme wie Android Debug Bridge (ADB), iTunes oder ähnliche Programme installiert sind, bestimmt das Betriebssystem die mobilen Geräte als ADB- oder iTunes-Geräte. In den übrigen Fällen kann das Betriebssystem den Typ eines mobilen Gerätes als tragbares Gerät (MTP) für die Dateiübertragung, als PTP-Geräte (Kamera) für die Bildübertragung oder als anderes Gerät bestimmen. Der Gerätetyp hängt vom Modell des Mobilgeräts und vom ausgewählten USB-Verbindungsmodus ab. Mit Kaspersky Endpoint Security können Sie individuelle Zugriffsberechtigungen für Daten auf Mobilgeräten in ADB-Anwendungen, iTunes oder im Dateimanager konfigurieren. In allen anderen Fällen erlaubt die „Gerätekontrolle“ den Zugriff auf Mobilgeräte gemäß den Zugriffsregeln für tragbare Geräte (MTP).

Zugriff auf Mobilgeräte

Mobilgeräte gehören zur Kategorie der tragbaren Geräte (MTP) und haben darum die gleichen Einstellungen. Sie können einen der folgenden Zugriffsmodi für Mobilgeräte auswählen:

- **Erlauben**. Kaspersky Endpoint Security erlaubt Vollzugriff auf mobile Geräte. Auf mobilen Geräten können Sie über den Dateimanager oder über die ADB- und iTunes-App Dateien öffnen, erstellen, ändern, kopieren oder löschen. Außerdem können Sie den Geräteakku aufladen, indem Sie das Mobilgerät an einen USB-Anschluss des Computers anschließen.

- **Blockieren**. Kaspersky Endpoint Security schränkt den Zugriff auf Mobilgeräte im Dateimanager sowie in der App ADB und iTunes ein. Die App erlaubt nur den Zugriff auf vertrauenswürdige Mobilgeräte. Außerdem können Sie den Geräteakku aufladen, indem Sie das Mobilgerät an einen USB-Anschluss des Computers anschließen.

- **Von Verbindungsschnittstelle abhängig**. Kaspersky Endpoint Security erlaubt Verbindungen zu Mobilgeräten abhängig vom Status der USB-Verbindung (**Erlauben** oder **Blockieren**).

- **Nach Regeln**. Kaspersky Endpoint Security schränkt den Zugriff auf Mobilgeräte gemäß Regeln ein. In den Regeln können Sie Zugriffsrechte (Lesen/Schreiben) konfigurieren, Benutzer oder eine Gruppe von Benutzern auswählen, die Zugriff auf mobile Geräte haben sollen, und einen Zugriffszeitplan für mobile Geräte konfigurieren. Sie können den Zugriff auf Daten auf mobilen Geräten auch über die ADB- und iTunes-Anwendungen einschränken.

Zugriffsregeln für mobile Geräte konfigurieren

Zugriffsregeln für tragbare Geräte (MTP), ADB-Geräte und iTunes-Geräte werden unterschiedlich konfiguriert. Für tragbare Geräte (MTP) und ADB-Geräte können Sie Regeln für einzelne Benutzer oder Benutzergruppen konfigurieren und einen Zeitplan erstellen, nach dem die Regeln angewendet werden. Bei iTunes-Geräten ist dies nicht möglich. Hier können Sie den Datenzugriff über die iTunes-App nur für alle Benutzer zulassen oder verweigern.

So konfigurieren Sie den Zugriff auf Mobilgeräte über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.
4. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.
5. Konfigurieren Sie im Kontextmenü für den Gerätetyp **Tragbare Geräte (MTP)** den Zugriffsmodus für mobile Geräte: **Erlauben**, **Blockieren** oder **Von Verbindungsschnittstelle abhängig**.
6. Um die Zugriffsregeln für Mobilgeräte zu konfigurieren, doppelklicken Sie zum Öffnen der Regelliste.
7. Konfigurieren Sie die Zugriffsregel für Mobilgeräte:

   a. Klicken Sie im Block **Zugriffsregeln** auf **Hinzufügen**.

   Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel für Mobilgeräte geöffnet.

   b. Legen Sie im Feld **Priorität** die Schreibpriorität der Regel fest. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben/ADB-Zugriff) und Priorität.

   Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

   Beispielsweise können Sie der Gruppe „Jeder” schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren” Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder“ eine Priorität von 0 zu.

   Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

   c. Wählen Sie unter **Regel für Benutzer und Gruppen** die Benutzer oder Benutzergruppen aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   d. Klicken Sie auf **OK**.

8. Konfigurieren Sie unter **Zeitpläne für die ausgewählte Zugriffsregel**, einen Zeitplan für den Zugriff auf mobile Geräte für die Benutzer.

   Für ADB-Geräte kann kein separater Zugriffszeitplan konfiguriert werden. Sie können einen gemeinsamen Zugriffszeitplan für ADB-Geräte und tragbare Geräte (MTP) konfigurieren.

9. Konfigurieren Sie die Zugriffsberechtigungen der Benutzer auf Mobilgeräte im Dateimanager (**Lesen**/**Schreiben**).

10. Konfigurieren Sie den Zugriff auf Daten auf einem mobilen Gerät über die ADB-Anwendung mithilfe des Kontrollkästchens **Zugriff über ADB**.

    Ist das Kontrollkästchen deaktiviert und das Mobilgerät wird verbunden, wird die ADB-Anwendung daran gehindert, das Gerät zu erkennen.

11. Konfigurieren Sie unter **Zugriff über iTunes** den Zugriff auf Daten auf dem Mobilgerät über die iTunes-App.

    Kaspersky Endpoint Security wendet die Einstellungen für den Zugriff auf mobile Geräte über die iTunes-App für alle Benutzer an. Für iTunes-Geräte kann kein separater Zugriffszeitplan konfiguriert werden.

12. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Zugriffsregeln für mobile Geräte über Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.

5. Klicken Sie im Block **Regeln für den Zugriff auf Geräte** auf den Link **Geräte und WLAN-Netzwerke**.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle" vorhanden sind.

6. Wählen Sie den Gerätetyp **Tragbare Geräte (MTP)** aus.

   Dadurch werden die Zugriffsrechte für tragbare Geräte (MTP) geöffnet.

7. Konfigurieren Sie den Modus für den Zugriff auf mobile Geräte: **Erlauben**, **Blockieren**, **Je nach Schnittstelle** oder **Benutzerdefiniert**.

8. Verwenden Sie den Schalter **Zugriff via iTunes für alle Benutzer AKTIVIERT**, um den Zugriff auf Daten auf dem Mobilgerät über die iTunes-App zu konfigurieren.

   Kaspersky Endpoint Security wendet die Einstellungen für den Zugriff auf mobile Geräte über die iTunes-App für alle Benutzer an. Für iTunes-Geräte kann kein separater Zugriffszeitplan konfiguriert werden.

9. Wenn Sie den Modus **Benutzerdefiniert** auswählen, müssen Sie Zugriffsregeln für Geräte hinzufügen. Klicken Sie dazu unter **Benutzer und deren Rechte** auf **Hinzufügen** und konfigurieren Sie die Zugriffsregel für Mobilgeräte:

    a. Legen Sie im Feld **Priorität** die Schreibpriorität der Regel fest. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben/ADB-Zugriff) und Priorität.

    Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

    Beispielsweise können Sie der Gruppe „Jeder" schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder" eine Priorität von 0 zu.

    Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

    b. Wählen Sie unter **Benutzer oder Gruppe** die Benutzer oder Benutzergruppen für den Zugriff auf Mobilgeräte aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

    c. Konfigurieren Sie unter **Zugriffszeitplan**, einen Zeitplan für den Zugriff auf mobile Geräte für die Benutzer.

    > Für ADB-Geräte kann kein separater Zugriffszeitplan konfiguriert werden. Sie können einen gemeinsamen Zugriffszeitplan für ADB-Geräte und tragbare Geräte (MTP) konfigurieren.

    d. Konfigurieren Sie die Zugriffsberechtigungen der Benutzer auf Mobilgeräte im Dateimanager (**Lesen**/**Schreiben**).

    e. Konfigurieren Sie den Zugriff auf Daten auf einem mobilen Gerät über die ADB-Anwendung mithilfe des Kontrollkästchens **Zugriff über ADB**.

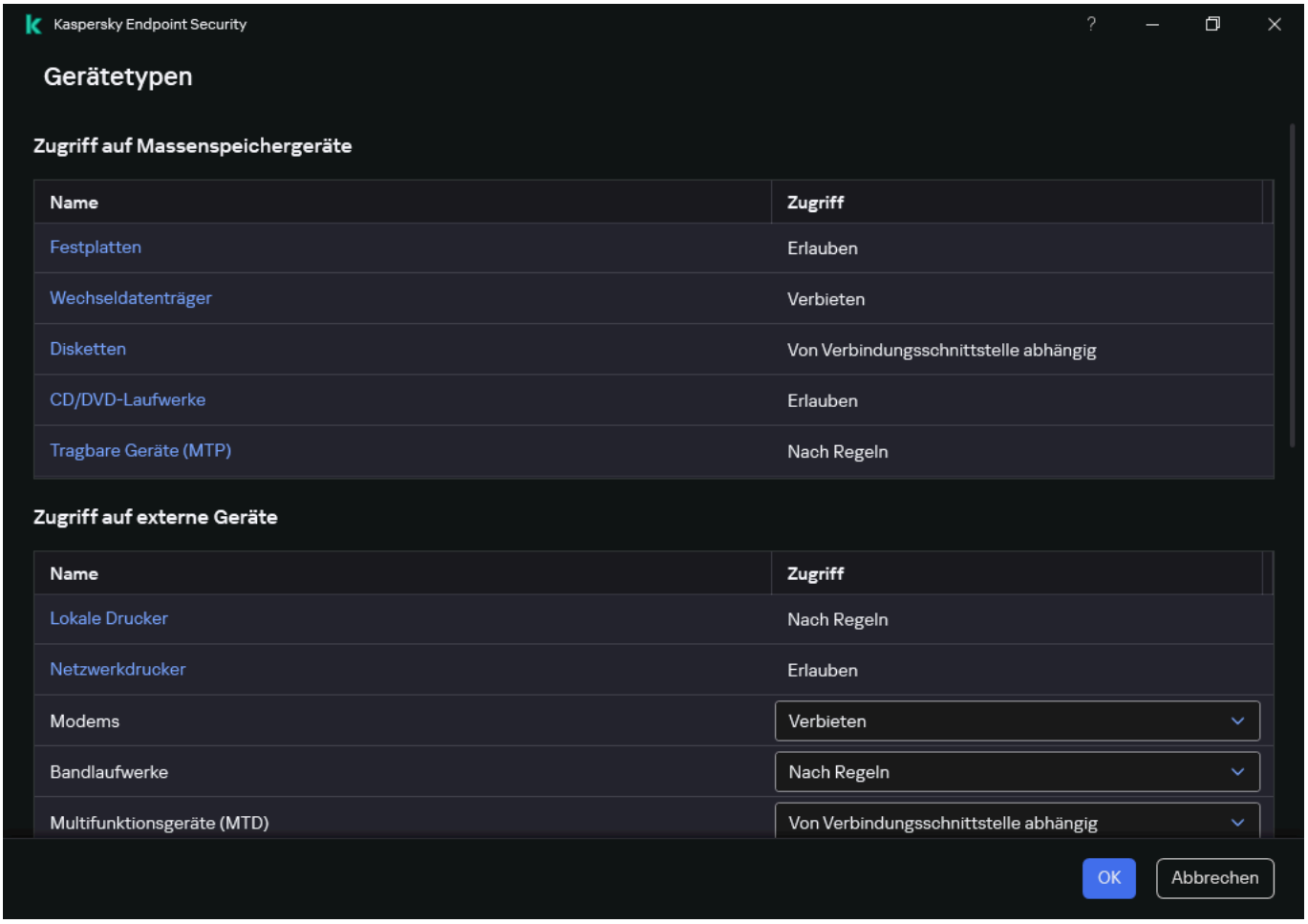
    Ist das Kontrollkästchen deaktiviert und das Mobilgerät wird verbunden, wird die ADB-Anwendung daran gehindert, das Gerät zu erkennen.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Zugriff auf Mobilgeräte über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Geräte und WLAN-Netzwerke**.

Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.



Gerätetypen in der Komponente „Gerätekontrolle“

4. Klicken Sie im Block **Zugriff auf Massenspeichergeräte** auf den Link **Tragbare Geräte (MTP)**.

   Dadurch wird ein Fenster mit den Zugriffsregeln für tragbare Geräte (MTP) geöffnet.

5. Konfigurieren Sie unter **Zugriff** den Zugriffsmodus für mobile Geräte: **Erlauben**, **Blockieren**, **Von Verbindungsschnittstelle abhängig** oder **Nach Regeln**.

6. Wenn Sie den Modus **Nach Regeln** auswählen, müssen Sie Zugriffsregeln für Geräte hinzufügen:

   a. Klicken Sie im Block **Benutzerrechte** auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel für Mobilgeräte geöffnet.

   b. Legen Sie im Feld **Priorität** die Schreibpriorität der Regel fest. Eine Regel umfasst die folgenden Attribute: Benutzerkonto, Zeitplan, Berechtigungen (Lesen/Schreiben/ADB-Zugriff) und Priorität.

      Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

      Beispielsweise können Sie der Gruppe „Jeder” schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren” Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder“ eine Priorität von 0 zu.

      Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

c. Aktivieren Sie unter **Status** die Zugriffsregel für Mobilgeräte.

d. Konfigurieren Sie unter **Zugriffsregeln** die Berechtigungen für den Benutzerzugriff auf Mobilgeräte.

- Konfigurieren Sie die Zugriffsberechtigungen der Benutzer auf Mobilgeräte im Dateimanager (**Lesen**/**Schreiben**).
- Konfigurieren Sie den Zugriff auf Daten auf einem mobilen Gerät über die ADB-Anwendung mithilfe des Kontrollkästchens **Zugriff über ADB**.

  Ist das Kontrollkästchen deaktiviert und das Mobilgerät wird verbunden, wird die ADB-Anwendung daran gehindert, das Gerät zu erkennen.

e. Wählen Sie unter **Benutzer** die Benutzer oder Benutzergruppen für den Zugriff auf Mobilgeräte aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

f. Konfigurieren Sie unter **Zeitplan für den Zugriff auf Geräte** einen Gerätezugriffsplan für die Benutzer.

> Für ADB-Geräte kann kein separater Zugriffszeitplan konfiguriert werden. Sie können einen gemeinsamen Zugriffszeitplan für ADB-Geräte und tragbare Geräte (MTP) konfigurieren.

g. Konfigurieren Sie unter **Zugriff über iTunes** den Zugriff auf Daten auf dem Mobilgerät über die iTunes-App.

> Kaspersky Endpoint Security wendet die Einstellungen für den Zugriff auf mobile Geräte über die iTunes-App für alle Benutzer an. Für iTunes-Geräte kann kein separater Zugriffszeitplan konfiguriert werden.

7. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird der Benutzerzugriff auf Mobilgeräte gemäß den Regeln eingeschränkt. Wenn Sie den Zugriff auf mobile Geräte in den ADB- und iTunes-Anwendungen untersagt haben und dann ein mobiles Geräte verbinden, werden die ADB- und iTunes-Anwendungen daran gehindert, das mobile Gerät zu erkennen.

Vertrauenswürdige Mobilgeräte

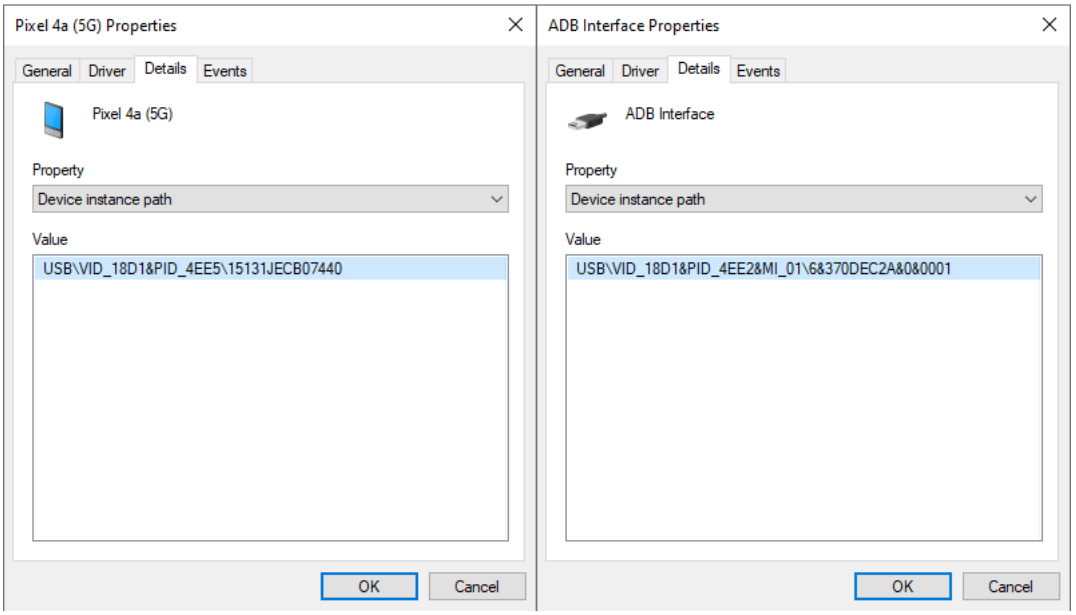
Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

Das Vorgehen zum Hinzufügen eines vertrauenswürdigen Mobilgeräts entspricht dem Vorgehen für andere Arten von vertrauenswürdigen Geräten. Sie können ein mobiles Gerät nach ID oder Gerätemodell hinzufügen.

Um ein vertrauenswürdiges mobiles Gerät nach ID hinzuzufügen, benötigen Sie eine eindeutige ID (Hardware ID – HWID). Diese ID finden Sie mithilfe von Betriebssystem-Tools in den Geräteeigenschaften (siehe folgende Abbildung). Dazu können Sie den Geräte-Manager verwenden. Die IDs von tragbaren Geräten (MTP) und ADB- bzw. iTunes-Geräten unterscheiden sich sogar für dasselbe mobile Gerät. Die ID eines tragbaren Geräts (MTP) kann wie folgt aussehen: `15131JECB07440`. Die ID eines ADB-Geräts kann wie folgt aussehen: `6&370DEC2A&0&0001`. Es bietet sich an, Geräte mithilfe von IDs hinzuzufügen, wenn Sie mehrere bestimmte Geräte hinzufügen möchten. Sie können auch Masken verwenden.

Wenn Sie ADB- oder iTunes-Programme installiert haben, nachdem ein Gerät mit dem Computer verbunden wurde, kann es sein, dass die einmalige Geräte-ID zurückgesetzt wird. Das bedeutet, dass Kaspersky Endpoint Security dieses Gerät als neu erkennt. Wenn das Gerät vertrauenswürdig ist, fügen Sie es erneut zur Liste der vertrauenswürdigen Geräte hinzu.

Um ein vertrauenswürdiges mobiles Gerät nach Gerätemodell hinzuzufügen, benötigen Sie die Vendor ID (VID) und Product ID (PID). Diese IDs finden Sie mithilfe von Betriebssystem-Tools in den Geräteeigenschaften (siehe Abbildung unten). Vorlage für die Eingabe einer VID und PID: `VID_18D1&PID_4EE5`. 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.



Geräte-ID im Geräte-Manager

Zugriff auf Bluetooth-Geräte verwalten

Mit Kaspersky Endpoint Security können Sie den Zugriff auf Bluetooth-Geräte verwalten. Zu Bluetooth-Geräten gehören beispielsweise auch drahtlose Tastaturen, Mäuse, Headsets und Drucker. Über Bluetooth können Sie beispielsweise auch mit einem mobilen Gerät kommunizieren.

Wenn Bluetooth-Geräte verbunden oder getrennt werden, erstellt das Programm möglicherweise mehrere Ereignisse für das Gerät. Der Grund dafür ist, dass das Betriebssystem ein Bluetooth-Gerät möglicherweise als mehrere Geräte unterschiedlichen Typs erkennt. Auch der Bluetooth-Adapter, über den das Gerät verbunden ist, wird von Kaspersky Endpoint Security als separates Gerät verwaltet. Aus diesem Grund erstellt das Programm für jedes erkannte Gerät ein Ereignis.

Für den Zugriff auf Bluetooth-Geräte gibt es die folgenden Modi:

- **Erlauben und nicht protokollieren**. Kaspersky Endpoint Security erlaubt die Verbindung mit beliebigen Bluetooth-Geräten und speichert im Ereignisprotokoll keine Informationen über die Verbindung. Sie können Bluetooth-Eingabegeräte (z. B. Tastaturen und Mäuse) verbinden, Daten über Bluetooth senden und andere Bluetooth-Geräte (wie Headsets und Kopfhörer) verwalten.
- **Erlauben**. Kaspersky Endpoint Security erlaubt die Verbindung mit beliebigen Bluetooth-Geräten. Sie können Bluetooth-Eingabegeräte (z. B. Tastaturen und Mäuse) verbinden, Daten über Bluetooth senden und andere Bluetooth-Geräte (wie Headsets und Kopfhörer) verwalten.
- **Blockieren**. Kaspersky Endpoint Security schränkt den Zugriff auf Bluetooth-Geräte ein. Sie können festlegen, dass nur Verbindungen mit Bluetooth-Eingabegeräten (Klasse Human Interface Devices) erlaubt werden sollen. Zu diesen Geräten gehören beispielsweise Tastaturen, Mäuse und Joysticks.

Es ist nicht möglich, eine Liste mit vertrauenswürdigen Bluetooth-Geräten zu erstellen. Wenn Sie den Zugriff auf Bluetooth-Geräte eingeschränkt haben, können Sie nur Bluetooth-Eingabegeräte verbinden.

So konfigurieren Sie den Zugriff auf Bluetooth-Geräte über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.
5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.
6. Konfigurieren Sie im Kontextmenü für den Gerätetyp **Bluetooth** den Zugriffsmodus für Bluetooth-Geräte: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.
7. Wenn Sie den Modus **Blockieren** auswählen, können Sie festlegen, dass nur die Verbindung von Bluetooth-Eingabegeräten (Tastaturen, Mäuse usw.) zugelassen wird. Aktivieren Sie dazu unter **Ausnahmen** das Kontrollkästchen **Eingabegeräte (Mäuse und Tastaturen)**.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie Zugriffsregeln für Bluetooth-Geräte über die Web Console und Cloud Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle → Gerätekontrolle**.

5. Klicken Sie im Block **Regeln für den Zugriff auf Geräte** auf den Link **Geräte und WLAN-Netzwerke**.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.

6. Wählen Sie den Gerätetyp **Bluetooth-Geräte** aus.

   Dadurch werden die Zugriffseinstellungen für Bluetooth-Geräte geöffnet.

7. Konfigurieren Sie den Zugriffsmodus für Bluetooth-Geräte: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

8. Wenn Sie den Modus **Blockieren** auswählen, können Sie festlegen, dass nur die Verbindung von Bluetooth-Eingabegeräten (Tastaturen, Mäuse usw.) zugelassen wird. Aktivieren Sie dazu unter **Ausnahmen** das Kontrollkästchen **Eingabegeräte (Mäuse und Tastaturen)**.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

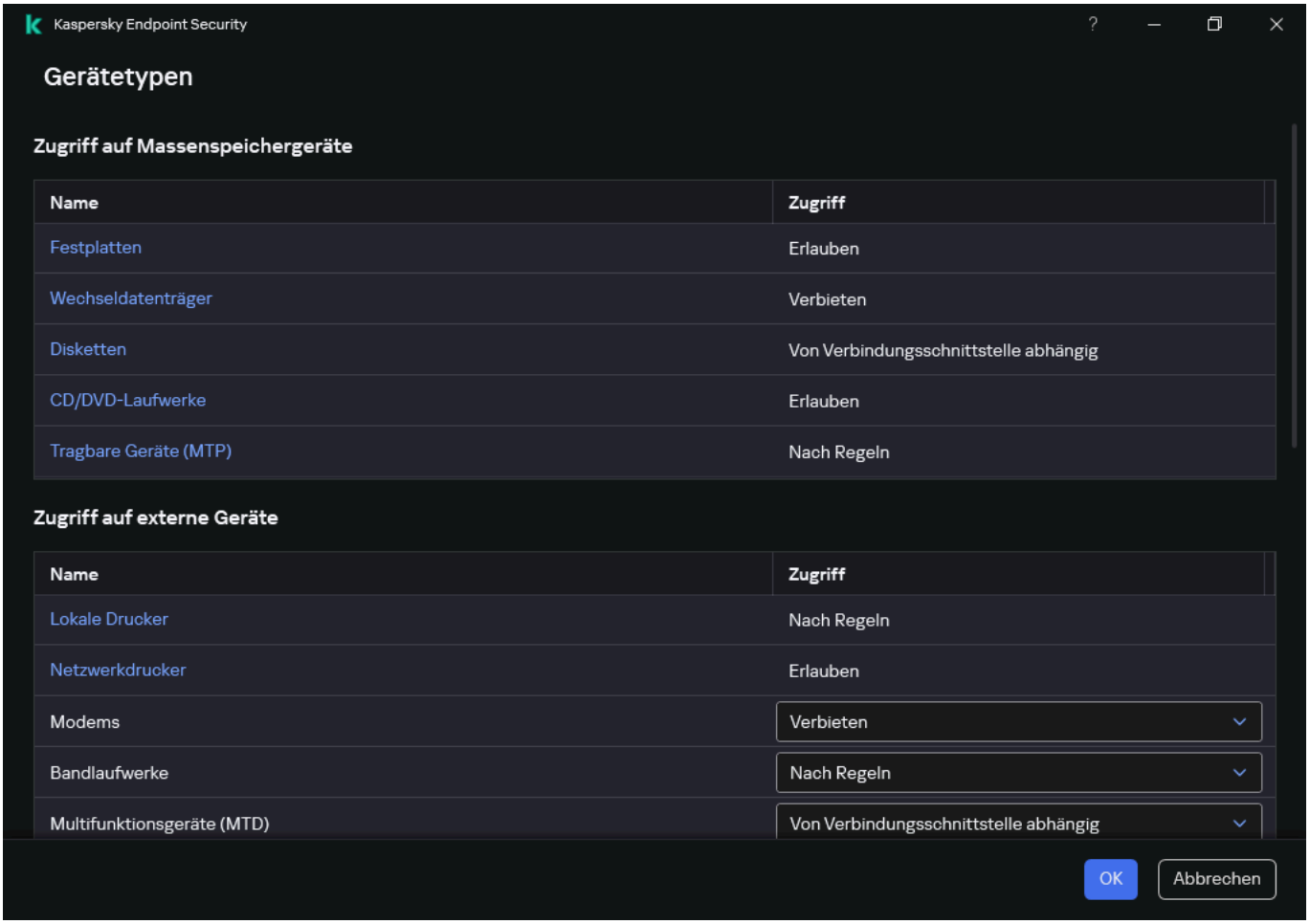
So konfigurieren Sie über die App-Benutzeroberfläche die Zugriffsregeln für Bluetooth-Geräte

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Gerätekontrolle** aus.

3. Klicken Sie im Block **Zugriffseinstellungen** auf **Geräte und WLAN-Netzwerke**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.



Gerätetypen in der Komponente „Gerätekontrolle“

4. Klicken Sie im Block **Zugriff auf externe Geräte** auf den Link **Bluetooth**.

   Dadurch werden die Zugriffseinstellungen für Bluetooth-Geräte geöffnet.

5. Konfigurieren Sie unter **Zugriff** den Zugriffsmodus für Bluetooth-Geräte: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

6. Wenn Sie den Modus **Blockieren** auswählen, können Sie festlegen, dass nur die Verbindung von Bluetooth-Eingabegeräten (Tastaturen, Mäuse usw.) zugelassen wird. Aktivieren Sie dazu unter **Ausnahmen** das Kontrollkästchen **Eingabegeräte (Mäuse und Tastaturen)**.

7. Speichern Sie die vorgenommenen Änderungen.

Druckerüberwachung

Die Drucksteuerung wird auf Arm-basierten Computern nicht unterstützt.

Mit der Druckerüberwachung können Sie den Benutzerzugriff auf lokale Drucker und Netzwerkdrucker konfigurieren.

Überwachung lokaler Drucker

Der Zugriff auf lokale Drucker lässt sich über Kaspersky Endpoint Security auf zwei Ebenen konfigurieren: *Verbinden* und *Drucken*.

Kaspersky Endpoint Security kontrolliert lokale Druckerverbindungen über die folgenden Schnittstellen: USB, Serielle Schnittstelle (COM), Paralleler Anschluss (LPT).

Kaspersky Endpoint Security kontrolliert das Verbinden lokaler Drucker an die COM- und LPT-Ports nur auf Schnittstellenebene. Um Druckerverbindungen über COM- und LPT-Ports zu verhindern, müssen Sie also den Zugriffsmodus Von Verbindungsschnittstelle abhängig für lokale Drucker auswählen und Verbindungen über COM- und LPT-Schnittstellen verbieten.

Für Drucker, die über USB verbunden werden, führt die App eine Kontrolle auf zwei Ebenen aus: Gerätetyp (lokale Drucker) und Verbindungsschnittstelle (USB).

Sie können einen der folgenden Modus für den Zugriff auf lokale Drucker über USB auswählen:

- **Erlauben**. Kaspersky Endpoint Security gewährt allen Benutzern vollständigen Zugriff auf lokale Drucker. Benutzer können Drucker verbinden und Dokumente mit den Mitteln des Betriebssystems drucken.

- **Blockieren**. Kaspersky Endpoint Security blockiert Verbindungen zu lokalen Druckern. Die App erlaubt nur Verbindungen zu vertrauenswürdigen Druckern.

- **Von Verbindungsschnittstelle abhängig**. Kaspersky Endpoint Security erlaubt Verbindungen zu lokalen Druckern abhängig vom Status der USB-Schnittstelle (**Erlauben** oder **Blockieren**).

- **Nach Regeln**. Um das Drucken zu steuern, müssen Sie *Druckerregeln* hinzufügen. In den Regeln können Sie Benutzer oder eine Gruppe von Benutzern auswählen, denen Sie den Zugriff auf das Drucken von Dokumenten auf lokalen Druckern erlauben oder verbieten.

Überwachung von Netzwerkdruckern

Mit Kaspersky Endpoint Security können Sie den Zugriff auf das Drucken auf Netzwerkdruckern konfigurieren. Sie können einen der folgenden Modi für den Zugriff auf Netzwerkdrucker auswählen:

- **Erlauben und nicht protokollieren**. Das Drucken auf Netzwerkdruckern wird von Kaspersky Endpoint Security nicht kontrolliert. Das Programm gewährt allen Benutzern Zugriff auf Drucker und speichert im Ereignisprotokoll keine Informationen über Druckvorgänge.

- **Erlauben**. Kaspersky Endpoint Security gewährt allen Benutzern Zugriff auf das Drucken auf Netzwerkdruckern.

- **Blockieren**. Kaspersky Endpoint Security beschränkt den Zugriff auf Netzwerkdrucker für alle Benutzer. Die App erlaubt nur den Zugriff auf vertrauenswürdige Drucker.

- **Nach Regeln**. Kaspersky Endpoint Security gewährt den Druckerzugriff gemäß den Regeln für das Drucken. In den Regeln können Sie Benutzer oder eine Gruppe von Benutzern auswählen, denen das Drucken von Dokumenten auf Netzwerkdruckern gestattet oder verweigert wird.

Druckerregeln für Drucker hinzufügen

So fügen Sie Regeln für das Drucken über die Verwaltungskonsole (MMC) hinzu

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Gerätekontrolle** aus.

4. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.

5. Konfigurieren Sie im Kontextmenü für die Gerätetypen **Lokale Drucker** und **Netzwerkdrucker** den Zugriffsmodus für die entsprechenden Drucker: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren** (nur für Netzwerkdrucker), oder **Von Verbindungsschnittstelle abhängig** (nur für lokale Drucker).

6. Um die Regeln für das Drucken auf lokalen Druckern und Netzwerkdruckern zu konfigurieren, doppelklicken Sie auf die Regellisten.

7. Wählen Sie **Nach Regeln** als Zugriffsmodus für Drucker aus.

8. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Druckerregel gelten soll.

   a. Klicken Sie auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer neuen Druckerregel geöffnet.

   b. Weisen Sie dem Regeleintrag eine Priorität zu. Ein Regeleintrag enthält die folgenden Attribute: Benutzerkonto, Aktion (erlauben/blockieren) und Priorität.

      Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

      Beispielsweise können Sie der Gruppe „Jeder" schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder" eine Priorität von 0 zu.

      Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

   c. Konfigurieren Sie unter **Aktion** den Benutzerzugriff für das Drucken auf dem Drucker.

   d. Klicken Sie auf **Benutzer und Gruppen** und wählen Sie die Benutzer oder Benutzergruppen für den Druckerzugriff aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   e. Klicken Sie auf **OK**.

9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Druckerregeln über Web Console und Cloud Console hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Klicken Sie im Block **Regeln für den Zugriff auf Geräte** auf den Link **Geräte und WLAN-Netzwerke**.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle" vorhanden sind.
6. Wählen Sie den Gerätetyp **Lokale Drucker** oder **Netzwerkdrucker** aus.

   Dadurch werden Regeln für den Druckerzugriff geöffnet.
7. Konfigurieren Sie den Zugriffsmodus für die entsprechenden Drucker: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren** (nur für Netzwerkdrucker), **Je nach Schnittstelle** (nur für lokale Drucker) oder **Benutzerdefiniert**.

8. Wenn Sie den Modus **Benutzerdefiniert** auswählen, müssen Sie Druckerregeln für lokale Drucker oder Netzwerkdrucker hinzufügen. Klicken Sie dazu in der Tabelle mit den Druckerregeln auf **Hinzufügen**.

   Dadurch werden die Einstellungen der neuen Druckerregel geöffnet.

9. Weisen Sie dem Regeleintrag eine Priorität zu. Ein Regeleintrag enthält die folgenden Attribute: Benutzerkonto, Aktion (erlauben/blockieren) und Priorität.

   Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

   Beispielsweise können Sie der Gruppe „Jeder" schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren" Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder" eine Priorität von 0 zu.

   Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

10. Konfigurieren Sie unter **Aktion** den Benutzerzugriff für das Drucken auf dem Drucker.

11. Wählen Sie unter **Benutzer oder Gruppe** die Benutzer oder Benutzergruppen für den Druckerzugriff aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

12. Speichern Sie die vorgenommenen Änderungen.

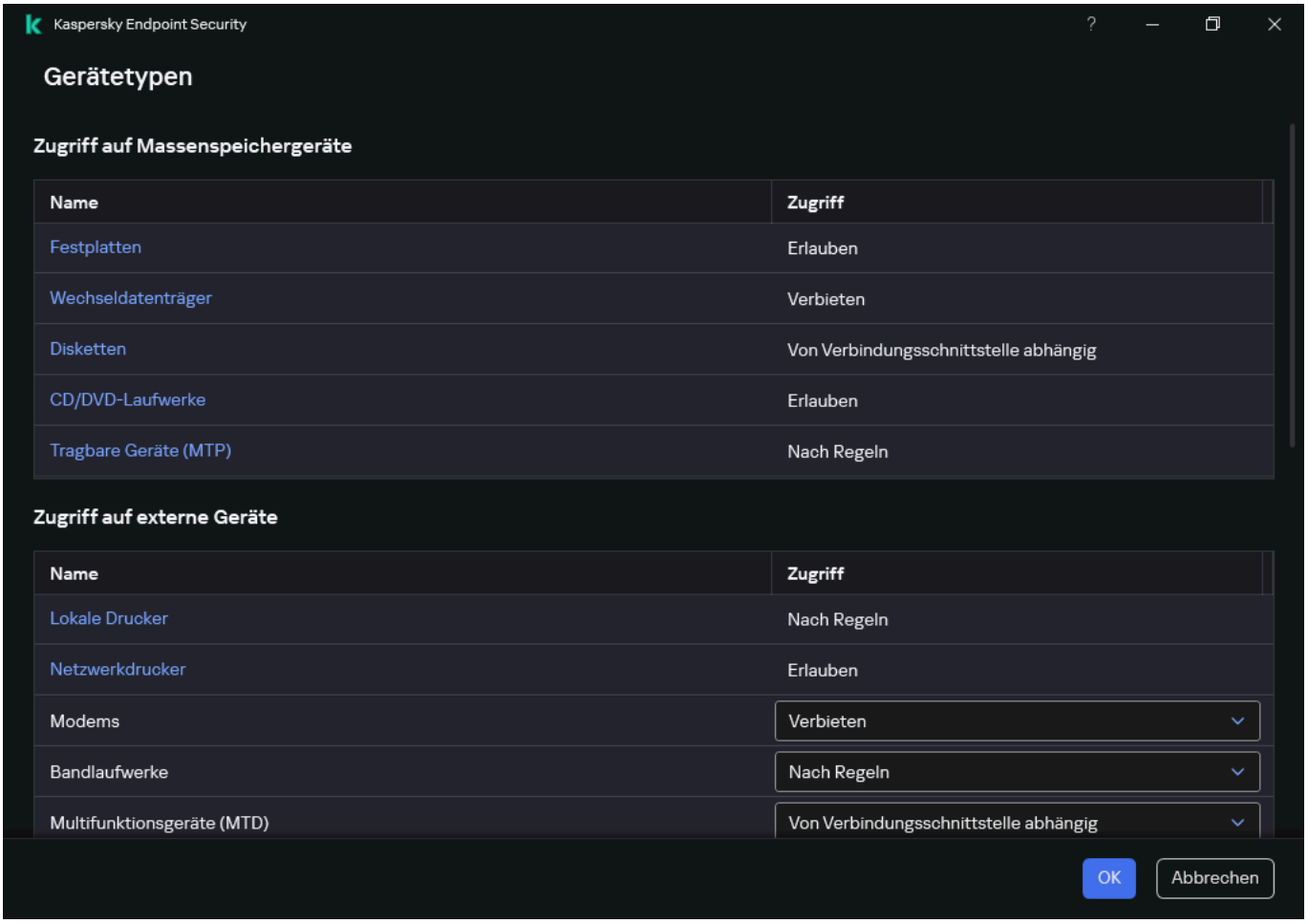
So fügen Sie Druckerregeln über die App-Oberfläche hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.

3. Klicken Sie im Block **Zugriffseinstellungen** auf **Geräte und WLAN-Netzwerke**.

Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.



Gerätetypen in der Komponente „Gerätekontrolle“

4. Klicken Sie unter **Zugriff auf externe Geräte** auf **Lokale Drucker** oder **Netzwerkdrucker**.

   Dadurch wird ein Fenster mit den Regeln für den Druckerzugriff geöffnet.

5. Konfigurieren Sie unter **Zugriff auf lokale Drucker** oder **Zugriff auf Netzwerkdrucker** den Zugriffsmodus für Drucker: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren** (nur für Netzwerkdrucker), **Von Verbindungsschnittstelle abhängig** (nur für lokale Drucker) oder **Nach Regeln**.

6. Wenn Sie den Modus **Nach Regeln** auswählen, müssen Sie Druckerregeln für die Drucker hinzufügen. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Druckerregel gelten soll.

   a. Klicken Sie auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer neuen Druckerregel geöffnet.

   b. Weisen Sie dem Regeleintrag eine Priorität zu. Ein Regeleintrag enthält die folgenden Attribute: Benutzerkonto, Berechtigungen (erlauben/blockieren) und Priorität.

      Eine Regel hat eine bestimmte Priorität. Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde, reguliert Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. In Kaspersky Endpoint Security können Sie eine Priorität von 0 bis 10.000 zuweisen. Je höher der Wert, desto höher die Priorität. Das bedeutet, dass ein Eintrag mit dem Wert 0 die niedrigste Priorität besitzt.

      Beispielsweise können Sie der Gruppe „Jeder” schreibgeschützte Leseberechtigungen und der Gruppe „Administratoren” Lese-/Schreibberechtigungen gewähren. Weisen Sie dazu für die Gruppe der Administratoren eine Priorität von 1 und für die Gruppe „Jeder“ eine Priorität von 0 zu.

Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Mit anderen Worten: Wenn ein Benutzer mehreren Gruppen hinzugefügt wurde und die Priorität aller Regeln gleich ist, regelt Kaspersky Endpoint Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

c. Konfigurieren Sie unter **Aktion** die Benutzerberechtigungen für den Druckerzugriff.

d. Wählen Sie unter **Benutzer und Gruppen** die Benutzer oder Benutzergruppen für den Druckerzugriff aus. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

7. Speichern Sie die vorgenommenen Änderungen.

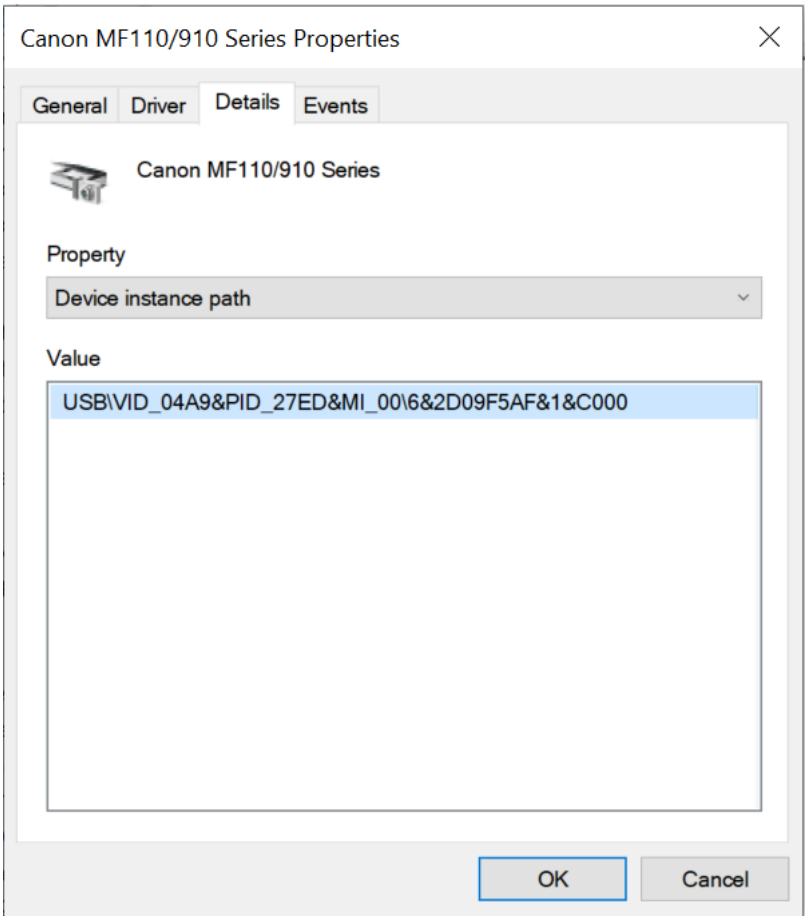
Vertrauenswürdige Drucker

Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

Das Vorgehen für das Hinzufügen vertrauenswürdiger Drucker entspricht dem Vorgehen für andere Arten von vertrauenswürdigen Geräten. Sie können lokale Drucker nach ID oder Gerätemodell hinzufügen. Netzwerkdrucker können nur nach Geräte-ID hinzugefügt werden.

Um einen vertrauenswürdigen lokalen Drucker nach ID hinzuzufügen, benötigen Sie eine eindeutige ID (Hardware ID – HWID)). Diese ID finden Sie mithilfe von Betriebssystem-Tools in den Geräteeigenschaften (siehe folgende Abbildung). Dazu können Sie den Device Manager verwenden. Die ID eines lokalen Druckers kann wie folgt aussehen: `6&2D09F5AF&1&C000`. Es bietet sich an, Geräte mithilfe von IDs hinzuzufügen, wenn Sie mehrere bestimmte Geräte hinzufügen möchten. Sie können auch Masken verwenden.

Um einen vertrauenswürdigen lokalen Drucker nach Gerätemodell hinzuzufügen, benötigen Sie die Vendor ID (VID) und Product ID (PID). Diese IDs finden Sie mithilfe von Betriebssystem-Tools in den Geräteeigenschaften (siehe Abbildung unten). Vorlage für die Eingabe einer VID und PID: `VID_04A9&PID_27FD`. 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.



Geräte-ID im Geräte-Manager

Um einen vertrauenswürdigen Netzwerkdrucker hinzuzufügen, benötigen Sie die Geräte-ID. Bei Netzwerkdruckern kann die Geräte-ID der Netzwerkname des Druckers (Name des freigegebenen Druckers), die IP-Adresse des Druckers oder die URL des Druckers sein.

Kontrolle von WLAN-Verbindungen

Mit der „Gerätekontrolle“ können Sie die WLAN-Verbindung des Computers (Laptops) verwalten. Öffentliche WLAN-Netzwerke sind möglicherweise unsicher. Die Verwendung solcher Netzwerke kann zu Datenverlust führen. Mit der „Gerätekontrolle“ können Sie verhindern, dass ein Benutzer eine WLAN-Verbindung herstellt, oder Sie können nur Verbindungen zu vertrauenswürdigen Netzwerken zulassen. Beispielsweise können Sie Verbindungen nur mit einem ausreichend sicheren Unternehmens-WLAN zulassen. Die Gerätekontrolle blockiert den Zugriff auf alle WLAN-Netzwerke, außer jenen, welche auf der Liste der vertrauenswürdigen WLAN-Netzwerke stehen.

Auf Computern unter Windows 11 müssen Sie die Standortdienste aktivieren, um die WLAN-Verbindungen zu überwachen. Dazu müssen Sie den Schalter **Standortdienste** in den Einstellungen des Betriebssystems aktivieren (**Einstellungen** → **Datenschutz & Sicherheit** → **Standort**). Wenn die Standortdienste deaktiviert sind, überwacht Kaspersky Endpoint Security die Verbindungen zu WLAN-Netzwerken nicht.

So beschränken Sie WLAN-Verbindungen über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.
4. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle“ vorhanden sind.
5. Wählen Sie im Kontextmenü für den Gerätetyp **WLAN** die „Gerätekontrolle“-Aktion aus, die beim Verbinden mit einem WLAN ausgeführt werden soll: **Erlauben** (), **Blockieren** () oder **Verbieten mit Ausnahmen** ().
6. Wenn Sie die Option **Verbieten mit Ausnahmen** ausgewählt haben, erstellen Sie eine Liste vertrauenswürdiger WLAN-Netzwerke:

   a. Doppelklicken Sie, um die Liste der vertrauenswürdigen WLAN-Netzwerke zu öffnen.

   b. Klicken Sie im Block **Vertrauenswürdige WLAN-Netzwerke** auf **Hinzufügen**.

   c. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster das vertrauenswürdige WLAN-Netzwerk (siehe Abbildung unten):

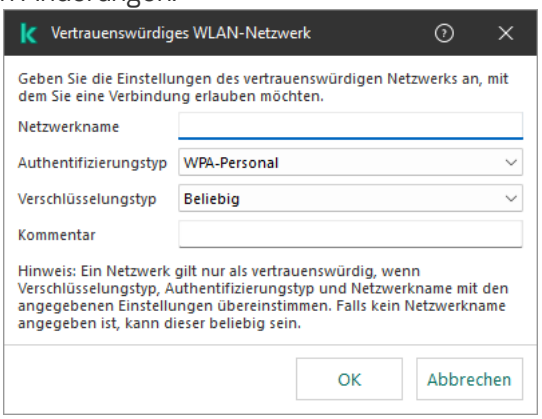
   - **Netzwerkname**. Name oder SSID (Service Set Identifier) des WLAN-Netzwerks.
   - **Authentifizierungstyp**. Authentifizierungstyp, der zur Verbindung mit dem WLAN-Netzwerk verwendet wird.

     Ab Kaspersky Endpoint Security für Windows Version 12.0 unterstützt die Anwendung das WPA3-Protokoll. Wenn auf einen Computer eine Richtlinie für Kaspersky Endpoint Security Version 12.2 angewendet wird, wird auf Computern mit Kaspersky Endpoint Security Version 11.11.0 und früher das Protokoll WPA2 ausgewählt; für die Versionen 12.0 bis 12.1 wird WPA2/WPA3 ausgewählt; für die Versionen 12.2 und höher wird WPA3 ausgewählt.
   - **Verschlüsselungstyp**. Verschlüsselungstyp, der zum Schutz des WLAN-Datenverkehrs verwendet wird.
   - **Kommentar**. Weitere Informationen über das hinzugefügte WLAN-Netzwerk.

   Die Einstellungen des vertrauenswürdigen WLAN-Netzwerks können Sie in den Router-Einstellungen anzeigen.

   Ein WLAN-Netzwerk wird als vertrauenswürdig betrachtet, wenn seine Einstellungen mit den in der Regel angegebenen Einstellungen übereinstimmen.

7. Speichern Sie die vorgenommenen Änderungen.



Einstellungen für ein vertrauenswürdiges WLAN-Netzwerk

So beschränken Sie WLAN-Verbindungen über Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.
5. Wählen Sie unter **Regeln für den Zugriff auf Geräte** die Registerkarte **Geräte und WLAN-Netzwerke** aus.

   Die Tabelle enthält Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponente „Gerätekontrolle" vorhanden sind.
6. Klicken Sie im Block **WLAN-Netzwerke** auf den Link **WLAN**.
7. Wählen Sie im folgenden Fenster aus, welche Aktion die Gerätekontrolle beim Verbinden mit einem WLAN ausführen soll: **Erlauben**, **Blockieren** oder **Blockieren mit Ausnahmen**.
8. Wenn Sie die Option **Blockieren mit Ausnahmen** ausgewählt haben, erstellen Sie eine Liste vertrauenswürdiger WLAN-Netzwerke:

   a. Doppelklicken Sie, um die Liste der vertrauenswürdigen WLAN-Netzwerke zu öffnen.

   b. Klicken Sie im Block **Vertrauenswürdige WLAN-Netzwerke** auf **Hinzufügen**.

   c. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster das vertrauenswürdige WLAN-Netzwerk (siehe Abbildung unten):

   - **Name**. Name oder SSID (Service Set Identifier) des WLAN-Netzwerks.
   - **Authentifizierungstyp**. Authentifizierungstyp, der zur Verbindung mit dem WLAN-Netzwerk verwendet wird.

     Ab Kaspersky Endpoint Security für Windows Version 12.0 unterstützt die Anwendung das WPA3-Protokoll. Wenn auf einen Computer eine Richtlinie für Kaspersky Endpoint Security Version 12.2 angewendet wird, wird auf Computern mit Kaspersky Endpoint Security Version 11.11.0 und früher das Protokoll WPA2 ausgewählt; für die Versionen 12.0 bis 12.1 wird WPA2/WPA3 ausgewählt; für die Versionen 12.2 und höher wird WPA3 ausgewählt.

- **Verschlüsselungstyp**. Verschlüsselungstyp, der zum Schutz des WLAN-Datenverkehrs verwendet wird.
- **Kommentar**. Weitere Informationen über das hinzugefügte WLAN-Netzwerk.

Die Einstellungen des vertrauenswürdigen WLAN-Netzwerks können Sie in den Router-Einstellungen anzeigen.

> Ein WLAN-Netzwerk wird als vertrauenswürdig betrachtet, wenn seine Einstellungen mit den in der Regel angegebenen Einstellungen übereinstimmen.

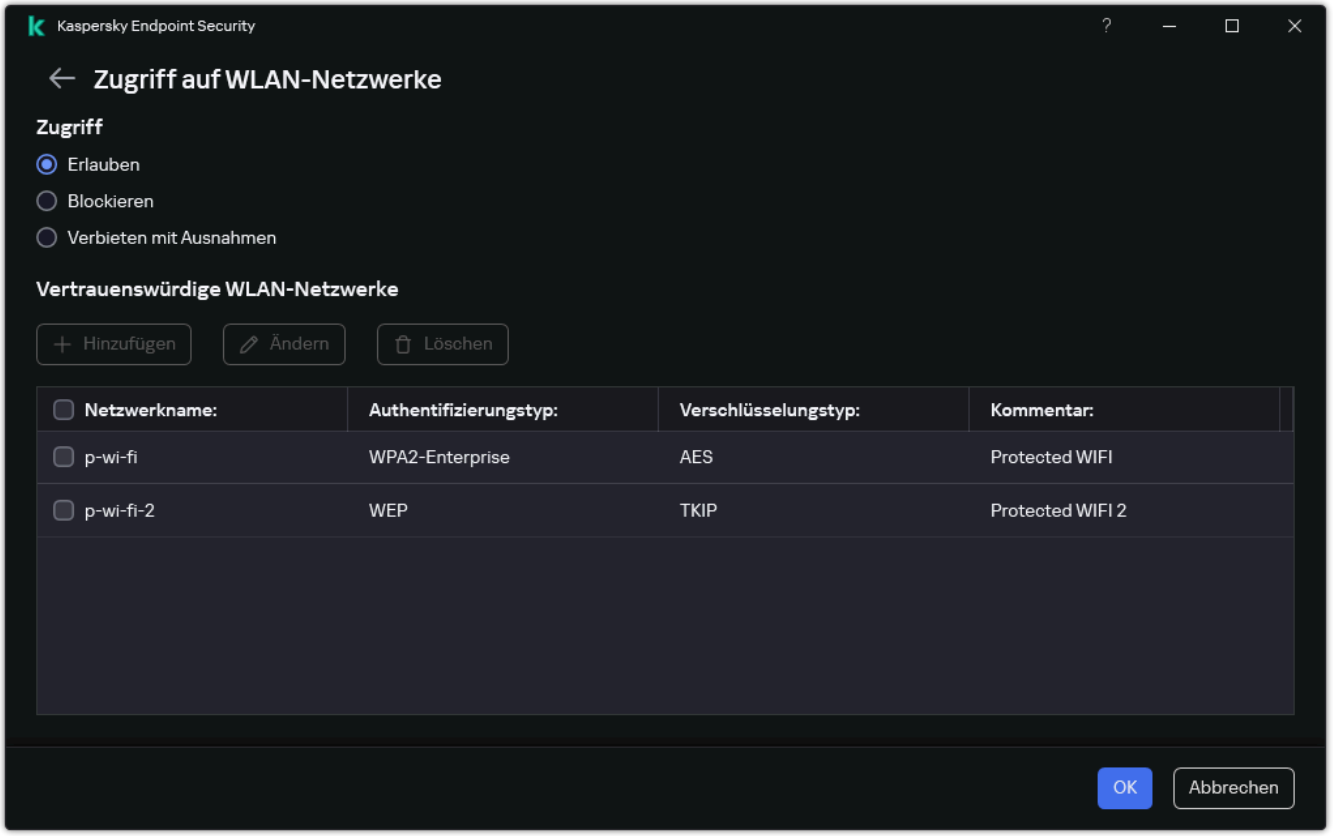
9. Speichern Sie die vorgenommenen Änderungen.

So beschränken Sie WLAN-Verbindungen über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Geräte und WLAN-Netzwerke**.

   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.
4. Klicken Sie im Block **Zugriff auf WLAN-Netzwerke** auf den Link **WLAN**.

   Das geöffnete Fenster zeigt die Regeln für den WLAN-Zugriff.



WLAN-Zugriffseinstellungen

5. Wählen Sie unter **Zugriff** die „Gerätekontrolle“-Aktion aus, die beim Verbinden mit einem WLAN ausgeführt werden soll: **Erlauben**, **Blockieren** oder **Verbieten mit Ausnahmen**.

6. Wenn Sie die Option **Verbieten mit Ausnahmen** ausgewählt haben, erstellen Sie eine Liste vertrauenswürdiger WLAN-Netzwerke:

   a. Klicken Sie im Block **Vertrauenswürdige WLAN-Netzwerke** auf **Hinzufügen**.

   b. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster das vertrauenswürdige WLAN-Netzwerk (siehe Abbildung unten):

   - **Netzwerkname**. Name oder SSID (Service Set Identifier) des WLAN-Netzwerks.
   - **Authentifizierungstyp**. Authentifizierungstyp, der zur Verbindung mit dem WLAN-Netzwerk verwendet wird.

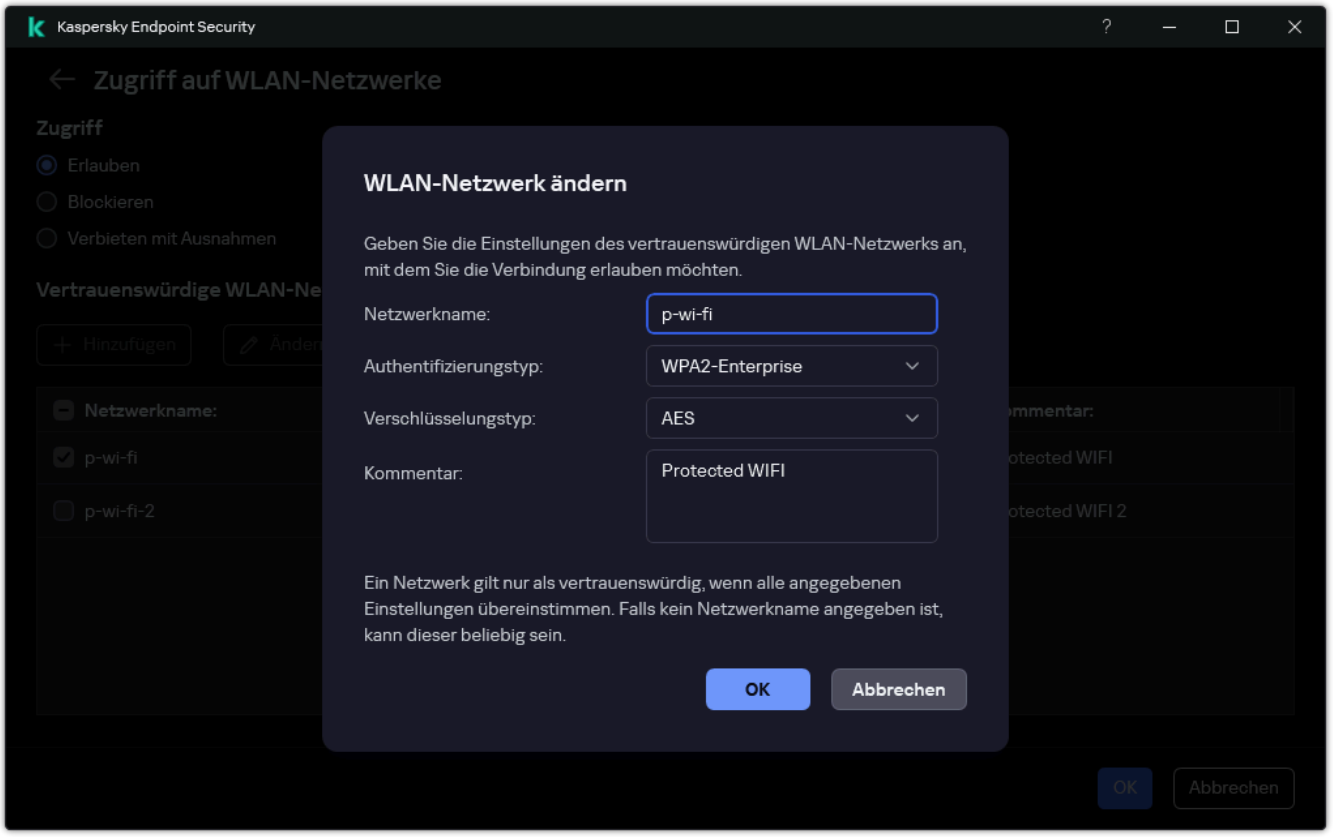
     Ab Kaspersky Endpoint Security für Windows Version 12.0 unterstützt die Anwendung das WPA3-Protokoll. Wenn auf einen Computer eine Richtlinie für Kaspersky Endpoint Security Version 12.2 angewendet wird, wird auf Computern mit Kaspersky Endpoint Security Version 11.11.0 und früher das Protokoll WPA2 ausgewählt; für die Versionen 12.0 bis 12.1 wird WPA2/WPA3 ausgewählt; für die Versionen 12.2 und höher wird WPA3 ausgewählt.

   - **Verschlüsselungstyp**. Verschlüsselungstyp, der zum Schutz des WLAN-Datenverkehrs verwendet wird.
   - **Kommentar**. Weitere Informationen über das hinzugefügte WLAN-Netzwerk.

   Die Einstellungen des vertrauenswürdigen WLAN-Netzwerks können Sie in den Router-Einstellungen anzeigen.

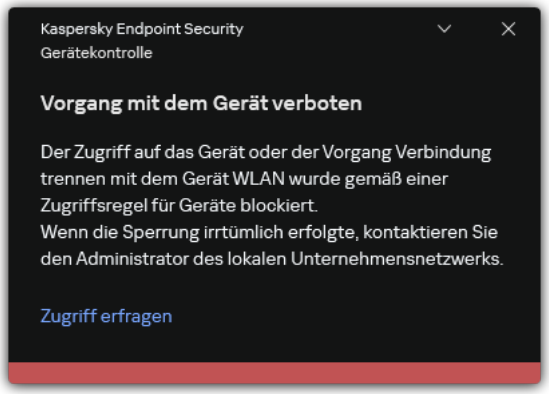
   Ein WLAN-Netzwerk wird als vertrauenswürdig betrachtet, wenn seine Einstellungen mit den in der Regel angegebenen Einstellungen übereinstimmen.

7. Speichern Sie die vorgenommenen Änderungen.



Einstellungen für ein vertrauenswürdiges WLAN-Netzwerk

Wenn ein Benutzer versucht, sich mit einem WLAN-Netzwerk zu verbinden, das nicht als vertrauenswürdig gilt, blockiert die App die Verbindung und zeigt eine Benachrichtigung an (siehe Abbildung unten).



Benachrichtigung der „Gerätekontrolle"

Überwachung der Nutzung von Wechseldatenträgern

Die Überwachung der Nutzung von Wechseldatenträgern umfasst:

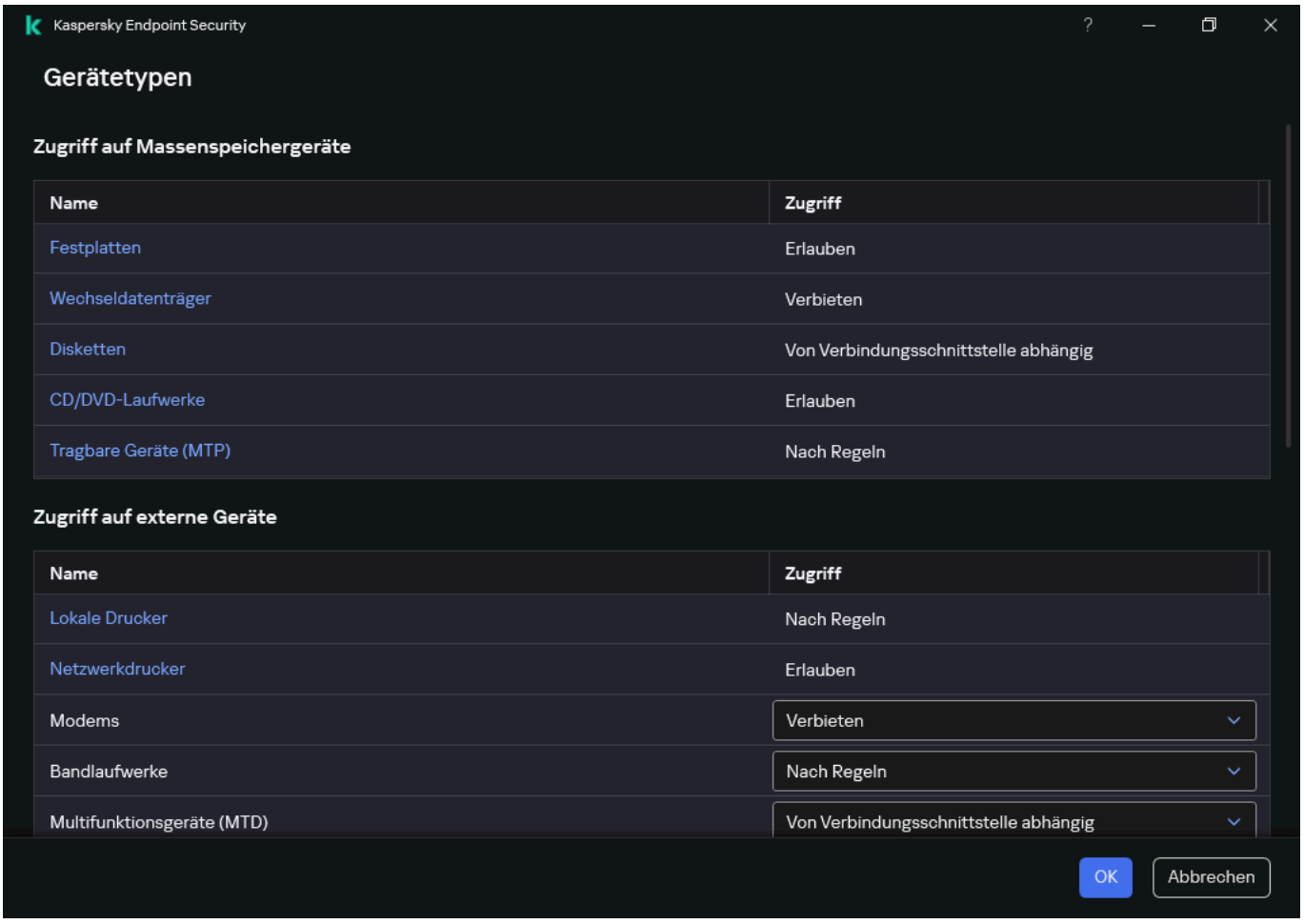
- Überwachung von Vorgängen mit Dateien auf Wechseldatenträgern.
- Überwachung der Verbindung und Trennung von vertrauenswürdigen Wechseldatenträgern.

  Kaspersky Endpoint Security kann das Verbinden und Trennen aller vertrauenswürdigen Geräte überwachen, nicht nur von Wechseldatenträgern. In den Benachrichtigungseinstellungen für die Komponente „Gerätekontrolle“ können Sie die Ereignisprotokollierung aktivieren. Ereignisse haben die Signifikanz *Informative Meldung*.

So aktivieren Sie die Überwachung der Nutzung von Wechseldatenträgern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Geräte und WLAN-Netzwerke**.

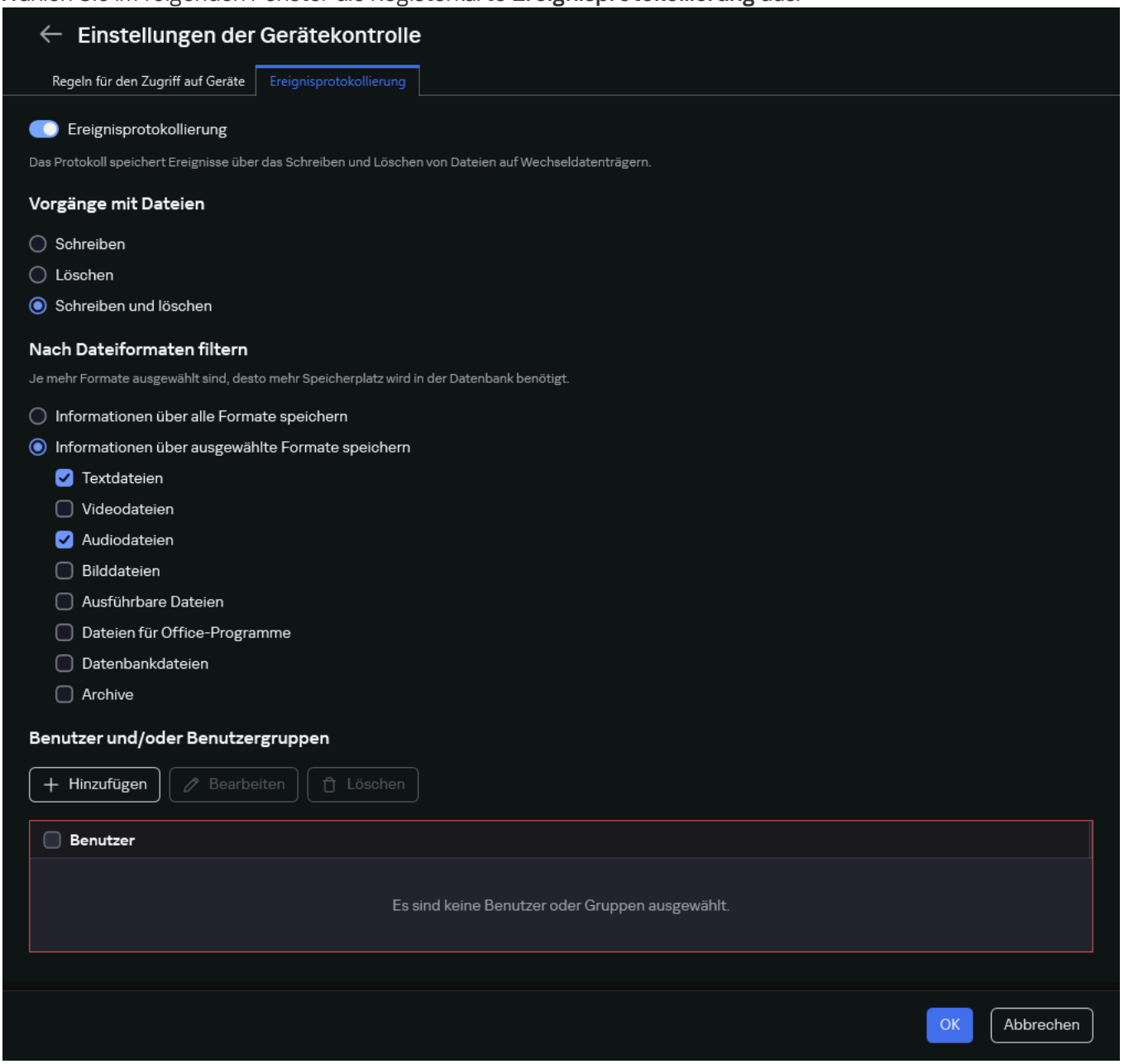
   Das geöffnete Fenster zeigt Zugriffsregeln für alle Geräte, die in der Klassifizierung der Komponenten für die Gerätekontrolle enthalten sind.



Gerätetypen in der Komponente „Gerätekontrolle“

4. Wählen Sie im Block **Zugriff auf Massenspeichergeräte** die Variante **Wechseldatenträger** aus.

5. Wählen Sie im folgenden Fenster die Registerkarte **Ereignisprotokollierung** aus.



Die Einstellungen zur Überwachung der Verwendung von Wechseldatenträgern

6. Aktivieren Sie den Schalter **Ereignisprotokollierung**.

7. Markieren Sie im Block **Vorgänge mit Dateien** die Operationen, die Sie überwachen möchten: **Schreiben**, **Löschen**.

8. Wählen Sie im Block **Nach Dateiformaten filtern** die Formate von Dateien aus, deren zugehörige Operationen von der Gerätekontrolle protokolliert werden sollen.

9. Wählen Sie die Benutzer oder Benutzergruppen aus, deren Verwendung von Wechsellaufwerken Sie überwachen möchten.

10. Speichern Sie die vorgenommenen Änderungen.

Wenn daher Benutzer Dateien speichern, die sich auf Wechseldatenträgern befinden, oder Dateien von Wechseldatenträgern löschen, so speichert Kaspersky Endpoint Security im Ereignisprotokoll Informationen über den ausgeführten Vorgang und sendet ein Ereignis an das Kaspersky Security Center. Ereignisse, die mit Dateien auf Wechseldatenträgern zusammenhängen, können Sie in der Kaspersky Security Center-Verwaltungskonsole im Arbeitsbereich für den Knoten **Administrationsserver** auf der Registerkarte **Ereignisse**

einsehen. Damit Ereignisse im lokalen Ereignisprotokoll von Kaspersky Endpoint Security angezeigt werden, muss das Kontrollkästchen **Dateivorgang ausgeführt** in den Benachrichtigungseinstellungen für die Komponente „Gerätekontrolle“ aktiviert werden.

Ändern der Cache-Dauer

Die Komponente „Gerätekontrolle“ registriert Ereignisse im Zusammenhang mit überwachten Geräten, wie das Anschließen und Trennen eines Geräts, das Lesen einer Datei von einem Gerät, das Schreiben einer Datei auf ein Gerät und andere Ereignisse. Gerätekontrolle erlaubt oder blockiert dann die Aktion entsprechend den Einstellungen von Kaspersky Endpoint Security.

Die Gerätekontrolle speichert Informationen über Ereignisse für einen bestimmten Zeitraum, den sogenannten *Caching-Zeitraum*. Wenn Informationen über ein Ereignis zwischengespeichert werden und dieses Ereignis wiederholt wird, ist es nicht notwendig, Kaspersky Endpoint Security darüber zu informieren oder eine weitere Aufforderung zur Gewährung des Zugriffs auf die entsprechende Aktion, wie z. B. das Anschließen eines Geräts, anzuzeigen. Dadurch wird die Arbeit mit einem Gerät komfortabler.

Ein Ereignis wird als doppeltes Ereignis betrachtet, wenn alle folgenden Ereigniseinstellungen mit dem Datensatz im Cache übereinstimmen:

- Geräte-ID
- SID des Benutzerkontos, auf das zugegriffen werden soll
- Gerätekategorie
- Mit dem Gerät ergriffene Maßnahmen
- App-Berechtigung für diese Aktion: erlaubt oder verweigert
- Pfad zum Prozess, der zur Durchführung der Aktion verwendet wurde
- Datei, auf die zugegriffen wird

Deaktivieren Sie Selbstschutz für Kaspersky Endpoint Security, bevor Sie den Cache-Zeitraum ändern. Aktivieren Sie den Selbstschutz, nachdem Sie den Cache-Zeitraum geändert haben.

So ändern Sie den Cache-Zeitraum:

1. Öffnen Sie den Registrierungseditor auf dem Computer.
2. Gehen Sie im Registrierungseditor zum folgenden Abschnitt:
   - Für 64-Bit-Betriebssysteme:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES.14.2\environment]`
   - Für 32-Bit-Betriebssysteme:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. Öffnen Sie `DeviceControlEventsCachePeriod` zur Bearbeitung.

4. Definieren Sie die Anzahl der Minuten, die die Gerätesteuerung Informationen über ein Ereignis speichern muss, bevor diese Informationen gelöscht werden.

Aktionen für vertrauenswürdige Geräte

Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

Sie können entweder einem einzelnen Benutzer, einer Benutzergruppe oder allen Benutzern des Unternehmens den Zugriff auf vertrauenswürdige Geräte gewähren.

Wenn in Ihrem Unternehmen beispielsweise die Verwendung von Wechseldatenträgern verboten ist, aber die Administratoren für ihre Arbeit Wechseldatenträger verwenden, können Sie die Verwendung von Wechseldatenträgern nur für die Gruppe der Administratoren erlauben. Dazu müssen Wechseldatenträger zur Liste der vertrauenswürdigen Geräte hinzugefügt werden und die Zugriffsrechte für Benutzer angepasst werden.

Es wird nicht empfohlen, mehr als 5000 vertrauenswürdige Geräte hinzuzufügen, da dies zu Systeminstabilität führen kann.

In Kaspersky Endpoint Security kann ein Gerät wie folgt zur Liste der vertrauenswürdigen Geräte hinzugefügt werden:

- Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitsteht, können Sie das Gerät mit dem Computer verbinden und es in den Programmeinstellungen zur Liste der vertrauenswürdigen Geräte hinzufügen. Um eine Liste der vertrauenswürdigen Geräte an alle Computer des Unternehmens zu verteilen, können Sie in der Richtlinie die Funktion zur Zusammenfassung der Listen mit den vertrauenswürdigen Geräten aktivieren und den Export-/Importvorgang verwenden.

- Wenn die Lösung Kaspersky Security Center in Ihrem Unternehmen bereitgestellt wurde, können Sie per Fernzugriff alle verbundenen Geräte ermitteln und in der Richtlinie eine Liste der vertrauenswürdigen Geräte erstellen. Die Liste der vertrauenswürdigen Geräte ist auf allen Geräten verfügbar, auf welche die Richtlinie an angewendet wird.

Kaspersky Endpoint Security kann die Verwendung vertrauenswürdiger Geräte steuern (Verbinden und Trennen). In den Benachrichtigungseinstellungen für die Komponente „Gerätekontrolle“ können Sie die Ereignisprotokollierung aktivieren. Ereignisse haben die Signifikanz *Informative Meldungen*.

Hinzufügen eines Geräts zur Liste der vertrauenswürdigen Geräte

Kaspersky Security Center erhält Informationen über Geräte, wenn auf den Computern Kaspersky Endpoint Security installiert ist, die Gerätekontrolle aktiviert ist und die Übertragung von Gerätedaten aktiviert ist. Ein Gerät, über das in Kaspersky Security Center keine Informationen vorliegen, kann nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

Wird ein Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt, wird der Zugriff auf das Gerät standardmäßig für alle Benutzer erlaubt (Benutzergruppe „Jeder“).

Mithilfe der folgenden Daten können Sie ein Gerät zur Liste der vertrauenswürdigen Geräte hinzufügen:

- **Geräte nach 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.

- **Geräte nach Modell**. Jedes Gerät besitzt eine Vendor ID (VID) und eine 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.

- **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 `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.

- **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 `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `VID_05AC&PID_*`.

So fügen Sie ein Gerät in der Verwaltungskonsole (MMC) zur Liste der vertrauenswürdigen Geräte hinzu

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Gerätekontrolle** aus.
5. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Vertrauenswürdige Geräte**.
6. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine gemeinsame Liste der vertrauenswürdigen Geräte für alle Computer des Unternehmens erstellen möchten.

   Die Listen mit vertrauenswürdigen Geräten der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Geräte der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Geräte der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.
7. Klicken Sie auf **Hinzufügen** und wählen Sie die Methode aus, mit der das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt werden soll.
8. Um die Geräte zu filtern, wählen Sie in der Dropdown-Liste **Gerätetyp** einen Gerätetyp aus (z. B. **Wechseldatenträger**).

   Geräte des Typs **Disketten** können in Kaspersky Endpoint Security nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

9. Geben Sie im Feld **Name / Modell** die Geräte-ID, das Modell (VID und PID) oder eine Maske ein. Die Eingabe ist von der ausgewählten Methode für das Hinzufügen abhängig.

   Das Hinzufügen von Geräten nach Modellmaske (VID und PID) funktioniert folgendermaßen: Wenn Sie eine Modellmaske eingeben, die mit keinem Modell übereinstimmt, prüft Kaspersky Endpoint Security, ob die Geräte-ID (HWID) mit der Maske übereinstimmt. Kaspersky Endpoint Security überprüft nur den Teil der Geräte-ID, der den Hersteller und den Gerätetyp angibt (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Wenn die Modellmaske diesem Teil der Geräte-ID entspricht, werden auf dem Computer zur Liste der vertrauenswürdigen Geräte jene Geräte hinzugefügt, die der Maske entsprechen. Gleichzeitig bleibt die Geräteliste in Kaspersky Security Center leer, wenn Sie auf die Schaltfläche **Upgrade** klicken. Damit die Geräteliste korrekt angezeigt wird, können Sie die Geräte mithilfe einer Maske für die Geräte-ID hinzufügen.

10. Um die Geräte zu filtern, geben Sie im Feld **Computer** den Namen des Computers oder eine Namensmaske des Computers ein, mit dem das Gerät verbunden ist.

    Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` steht als Platzhalter für ein beliebiges Einzelzeichen.

11. Klicken Sie auf **Upgrade**.

    In der Tabelle wird eine Liste der Geräte angezeigt, die den angegebenen Filterbedingungen entsprechen.

12. Aktivieren Sie die Kontrollkästchen für jene Geräte, die zur Liste der vertrauenswürdigen Geräte hinzugefügt werden sollen.

13. Geben Sie im Feld **Kommentar** an, weshalb das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt wird.

14. Klicken Sie rechts neben dem Feld **Für Benutzer und/oder Benutzergruppen erlauben** auf die Schaltfläche **Auswählen**.

    Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

    Für die Gruppe „Jeder“ ist der Zugriff auf vertrauenswürdige Geräte standardmäßig erlaubt.

15. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie ein Gerät in der Web Console zur Liste der vertrauenswürdigen Geräte hinzu

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.

5. Klicken Sie im folgenden Fenster auf den Link **Geräte**.

   Dadurch wird ein Fenster mit einer Liste der vertrauenswürdigen Geräte geöffnet.

6. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Vertrauenswürdige Geräte**.

7. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine gemeinsame Liste der vertrauenswürdigen Geräte für alle Computer des Unternehmens erstellen möchten.

   Die Listen mit vertrauenswürdigen Geräten der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Geräte der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Geräte der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.

8. Klicken Sie auf **Hinzufügen**.

   Daraufhin wird das Formular zum Hinzufügen eines vertrauenswürdigen Geräts geöffnet.

9. Wählen Sie unter **Benutzer oder Gruppe** die Benutzer aus, denen Sie den Zugriff auf vertrauenswürdige Geräte erlauben möchten.

   Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   Für die Gruppe „Jeder“ ist der Zugriff auf vertrauenswürdige Geräte standardmäßig erlaubt.

10. Um die Geräte zu filtern, wählen Sie in der Dropdown-Liste **Gerätetyp** einen Gerätetyp aus (z. B. **Wechseldatenträger**).

    Geräte des Typs **Disketten** können in Kaspersky Endpoint Security nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

11. Wenn Sie die genaue Geräte-ID oder das genaue Gerätemodell nicht kennen, aktivieren Sie das Kontrollkästchen **Maske verwenden**.

12. Wählen Sie aus, wie Sie das Gerät hinzufügen möchten: anhand der Geräte-ID oder des Modells (VID und PID).

    Das Hinzufügen von Geräten nach Modellmaske (VID und PID) funktioniert folgendermaßen: Wenn Sie eine Modellmaske eingeben, die mit keinem Modell übereinstimmt, prüft Kaspersky Endpoint Security, ob die Geräte-ID (HWID) mit der Maske übereinstimmt. Kaspersky Endpoint Security überprüft nur den Teil der Geräte-ID, der den Hersteller und den Gerätetyp angibt (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). Wenn die Modellmaske diesem Teil der Geräte-ID entspricht, werden auf dem Computer zur Liste der vertrauenswürdigen Geräte jene Geräte hinzugefügt, die der Maske entsprechen. Gleichzeitig wird in Kaspersky Security Center eine leere Geräteliste angezeigt. Damit die Geräteliste korrekt angezeigt wird, können Sie die Geräte mithilfe einer Maske für die Geräte-ID hinzufügen.

13. Um die Geräte zu filtern, geben Sie im Feld **Suche nach vertrauenswürdigen Geräten** den Namen des Computers oder eine Namensmaske des Computers ein, mit dem das Gerät verbunden ist.

    Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` steht als Platzhalter für ein beliebiges Einzelzeichen.

    In der Tabelle wird eine Liste der Geräte angezeigt, die den angegebenen Filterbedingungen entsprechen.

14. Aktivieren Sie die Kontrollkästchen für jene Geräte, die zur Liste der vertrauenswürdigen Geräte hinzugefügt werden sollen.

15. Geben Sie im Feld **Kommentar** an, weshalb das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt wird.

16. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So fügen Sie ein Gerät in der Programmoberfläche zur Liste der vertrauenswürdigen Geräte hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.

3. Klicken Sie im Block **Zugriffseinstellungen** auf **Vertrauenswürdige Geräte**.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.

4. Klicken Sie auf **Auswählen**.

   Dadurch wird die Liste der angeschlossenen Geräte geöffnet. Die Liste der Geräte hängt von dem Wert ab, der in der Dropdown-Liste **Angeschlossene Geräte anzeigen** ausgewählt ist.

5. Wählen Sie in der Geräteliste das Gerät aus, das Sie zur Liste der vertrauenswürdigen Geräte hinzufügen möchten.

   > Geräte des Typs **Disketten** können in Kaspersky Endpoint Security nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

6. Im Feld **Kommentar** können Sie alle relevanten Informationen über das vertrauenswürdige Gerät angeben.

7. Wählen Sie die Benutzer oder Benutzergruppen aus, denen Sie den Zugriff auf vertrauenswürdige Geräte erlauben möchten.

   Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

8. Speichern Sie die vorgenommenen Änderungen.

Wenn ein Gerät angeschlossen wird, überprüft Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte für den autorisierten Benutzer. Wenn das Gerät vertrauenswürdig ist, erlaubt Kaspersky Endpoint Security den Zugriff auf das Gerät mit allen Rechten, sogar wenn der Zugriff auf diesen Gerätetyp oder auf diese Schnittstelle verboten ist. Wenn das Gerät nicht vertrauenswürdig ist und der Zugriff verboten ist, können Sie Zugriff auf das blockierte Gerät anfordern.

Liste mit vertrauenswürdigen Geräten exportieren und importieren

Um die Liste der vertrauenswürdigen Geräte an alle Computer des Unternehmens zu verteilen, können Sie die Liste exportieren bzw. importieren.

Um beispielsweise eine Liste der vertrauenswürdigen Wechseldatenträger zu verteilen, gehen Sie wie folgt vor:

1. Verbinden Sie die Wechseldatenträger nacheinander mit dem Computer.

2. Fügen Sie die Wechseldatenträger in den Einstellungen von Kaspersky Endpoint Security zur Liste der vertrauenswürdigen Wechseldatenträger hinzu. Passen Sie bei Bedarf die Zugriffsrechte der Benutzer an. Sie können beispielsweise den Zugriff auf Wechseldatenträger nur den Administratoren erlauben.

3. Exportieren Sie in den Einstellungen von Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte (s. Anleitung unten).

4. Verteilen Sie die Datei mit der Liste der vertrauenswürdigen Geräte an die übrigen Computer des Unternehmens. Sie können die Datei beispielsweise in einem gemeinsamen Ordner ablegen.

5. Importieren Sie in den Einstellungen von Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte auf die übrigen Computern des Unternehmens (s. Anleitung unten).

Um die Liste mit vertrauenswürdigen Geräten zu importieren oder exportieren, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.

3. Klicken Sie im Block **Zugriffseinstellungen** auf **Vertrauenswürdige Geräte**.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.

4. Um die Liste der vertrauenswürdigen Geräte zu exportieren, gehen Sie wie folgt vor:

   a. Wählen Sie die vertrauenswürdigen Geräte aus, die Sie exportieren möchten.

   b. Klicken Sie auf **Export**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in welche Sie die Liste der vertrauenswürdigen Geräte exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die gesamte Liste der vertrauenswürdigen Geräte in die XLM-Datei.

5. Um die Liste der vertrauenswürdigen Geräte zu importieren, gehen Sie wie folgt vor:

   a. Wählen Sie in der Dropdown-Liste **Import** die entsprechende Aktion aus: **Importieren und zu vorhandenen Einträgen hinzufügen** oder **Importieren und vorhandene Einträge ersetzen**.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdigen Geräte importieren möchten.

   c. Öffnen Sie die Datei.

6. Speichern Sie die vorgenommenen Änderungen.

Wenn ein Gerät angeschlossen wird, überprüft Kaspersky Endpoint Security die Liste der vertrauenswürdigen Geräte für den autorisierten Benutzer. Wenn das Gerät vertrauenswürdig ist, erlaubt Kaspersky Endpoint Security den Zugriff auf das Gerät mit allen Rechten, sogar wenn der Zugriff auf diesen Gerätetyp oder auf diese Schnittstelle verboten ist.

Freigabe eines blockierten Geräts

Es kann vorkommen, dass Sie beim Anpassen der „Gerätekontrolle“ versehentlich den Zugriff auf ein erforderliches Gerät verbieten.

Falls in Ihrem Unternehmen die Lösung Kaspersky Security Center nicht verteilt wurde, können Sie das Gerät in den Einstellungen für Kaspersky Endpoint Security freigeben. Beispielsweise können Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzufügen oder die Gerätekontrolle vorübergehend deaktivieren.

Falls in Ihrem Unternehmen die Lösung Kaspersky Security Center verteilt wurde und auf die Computer eine Richtlinie angewendet wurde, können Sie das Gerät in der Verwaltungskonsole freigeben.

Online-Modus für die Freigabe

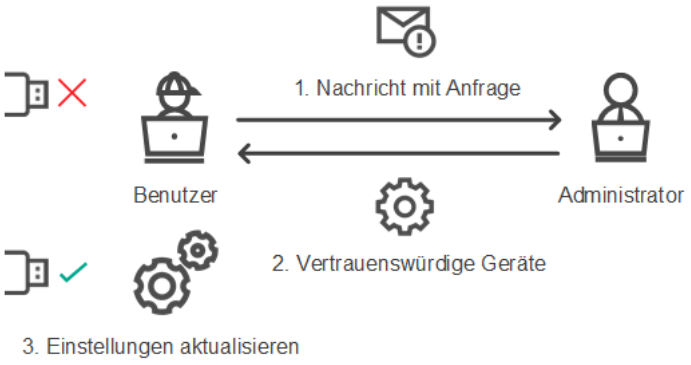
Die Freigabe eines blockierten Gerätes im Online-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. Der Computer muss die Möglichkeit haben, eine Verbindung zum Administrationsserver herzustellen.

Die Freigabe im Online-Modus umfasst die folgenden Schritte:

1. Der Benutzer sendet an den Administrator eine Nachricht mit einer Freigabeanfrage.
2. Der Administrator erhält in der Kaspersky Security Center-Konsole eine Nachricht mit der Anfrage.

   Die Kaspersky Security Center-Konsole verfügt über eine voreingestellte Ereignisauswahl *Benutzeranfragen*, mit sich der Nachrichten von Benutzern verfolgen lassen.
3. Der Administrator fügt das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

   Ein vertrauenswürdiges Gerät können Sie in der Richtlinie für die Administrationsgruppe hinzufügen oder in den lokalen Programmeinstellungen für einen bestimmten Computer.
4. Der Administrator aktualisiert die Einstellungen für Kaspersky Endpoint Security auf dem Benutzercomputer.



Schema für die Freigabe eines Gerätes im Online-Modus

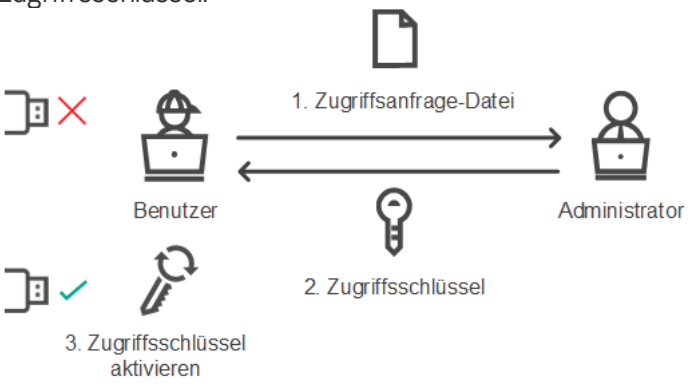
Offline-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Offline-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. In den Einstellungen der Richtlinie im Abschnitt **Gerätekontrolle** muss das Kontrollkästchen **Anfragen auf temporären Zugriff erlauben** aktiviert sein.

Falls ein blockiertes Gerät vorübergehend freigegeben werden soll, das Gerät aber nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden kann, können Sie das Gerät im Offline-Modus freigeben. Auf diese Weise können Sie ein blockiertes Gerät freigeben, falls Ihr Computer keinen Netzwerkzugang hat oder falls sich der Computer außerhalb des Unternehmensnetzwerks befindet.

Die Freigabe im Offline-Modus umfasst die folgenden Schritte:

1. Der Benutzer erstellt eine Zugriffsanfrage-Datei und sendet sie an den Administrator.
2. Der Administrator erstellt mithilfe der Zugriffsanfrage-Datei einen Zugriffsschlüssel und sendet ihn an den Benutzer.
3. Der Benutzer aktiviert den Zugriffsschlüssel.



Schema für die Freigabe eines Gerätes im Offline-Modus

Online-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Online-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. Der Computer muss die Möglichkeit haben, eine Verbindung zum Administrationsserver herzustellen.

Um als Benutzer den Zugriff auf ein blockiertes Gerät zu erfragen, gehen Sie wie folgt vor:

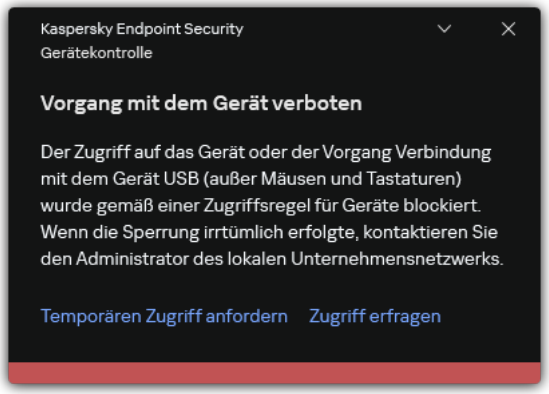
1. Verbinden Sie das Gerät mit dem Computer.

   Kaspersky Endpoint Security zeigt eine Benachrichtigung darüber an, dass der Zugriff auf das Gerät blockiert wurde (siehe folgende Abb.).

2. Klicken Sie auf den Link **Zugriff erfragen**.

   Dadurch wird ein Fenster mit einer Nachricht für den Administrator geöffnet. Die Nachricht enthält Informationen über das blockierte Gerät.

3. Klicken Sie auf **Senden**.



Benachrichtigung der „Gerätekontrolle"

Dann erhält der Administrator in der Kaspersky Security Center-Konsole das Ereignis *Nachricht an den Administrator über Zugriffsverbot auf Gerät*. Das Ereignis enthält unter anderem die folgenden Daten: Benutzername, Computername, Details zum Gerät, auf das der Benutzer zuzugreifen versucht, sowie andere Informationen. Sie können anpassen, wie der Administrator über solche Ereignisse benachrichtigt werden soll, z. B. per E-Mail-Benachrichtigung. Die Kaspersky Security Center-Konsole verfügt über eine voreingestellte Ereignisauswahl *Benutzeranfragen*, mit sich der Nachrichten von Benutzern verfolgen lassen.

Um den Zugriff zu erlauben, müssen Sie das Gerät zur vertrauenswürdigen Liste hinzufügen. Nachdem Sie die Einstellungen von Kaspersky Endpoint Security auf dem Computer aktualisiert haben, kann der Benutzer auf das Gerät zugreifen.

Offline-Modus für die Freigabe

Die Freigabe eines blockierten Gerätes im Offline-Modus ist nur verfügbar, wenn im Unternehmen die Lösung Kaspersky Security Center bereitgestellt wurde und auf den Computer eine Richtlinie angewendet wurde. In den Einstellungen der Richtlinie im Abschnitt **Gerätekontrolle** muss das Kontrollkästchen **Anfragen auf temporären Zugriff erlauben** aktiviert sein.

Um als Benutzer den Zugriff auf ein blockiertes Gerät zu erfragen, gehen Sie wie folgt vor:

1. Verbinden Sie das Gerät mit dem Computer.

   Kaspersky Endpoint Security zeigt eine Benachrichtigung darüber an, dass der Zugriff auf das Gerät blockiert wurde (siehe folgende Abb.).

2. Klicken Sie auf den Link **Temporären Zugriff anfordern**.

   Dadurch wird ein Fenster mit einer Liste der verbundenen Geräte geöffnet.

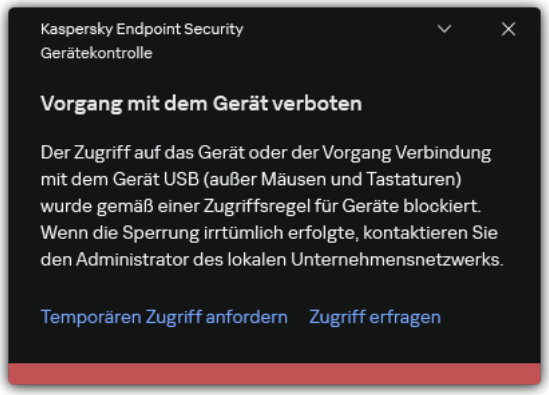
3. Wählen Sie in der Liste der angeschlossenen Geräte das Gerät aus, auf das Sie zugreifen möchten.

4. Klicken Sie auf **Zugriffsanfrage-Datei erstellen**.

5. Geben Sie im Feld **Zugriffsdauer** den Zeitraum an, für den Sie Zugriff auf das Gerät erhalten möchten.

6. Speichern Sie die Datei auf dem Computer.

   Dadurch wird eine Zugriffsanfrage-Datei mit der Erweiterung *.akey auf den Computer geladen. Senden Sie die Zugriffsanfrage-Datei für das Gerät auf beliebige Weise an den Administrator des lokalen Unternehmensnetzwerks.



Benachrichtigung der „Gerätekontrolle"

So erstellen Sie als Administrator über die Verwaltungskonsole (MMC) einen Zugriffsschlüssel für das gesperrte Gerät

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.

3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.

4. Wählen Sie in der Liste der Client-Computer den Computer aus, dessen Benutzer temporären Zugriff auf ein gesperrtes Gerät erhalten soll.

5. Wählen Sie im Kontextmenü des Computers den Punkt **Freigabe im Offline-Modus**.

6. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Gerätekontrolle**-Registerkarte aus.

7. Klicken Sie auf **Durchsuchen** und öffnen Sie die Zugriffsanfrage-Datei, die Sie vom Benutzer erhalten haben.

   Es werden Informationen über das blockierte Gerät angezeigt, auf das der Benutzer den Zugriff erfragt hat.

8. Ändern Sie erforderlichenfalls den Wert der Einstellung **Zugriffsdauer**.

   Für die Einstellung **Zugriffsdauer** ist standardmäßig der Wert festgelegt, der vom Benutzer bei der Erstellung der Zugriffsanfrage-Datei angegeben wurde.

9. Geben Sie einen Wert für **Aktivierungszeitraum** an.

   Diese Einstellung enthält den Zeitraum, während dem der Benutzer mithilfe des Zugriffsschlüssels den Zugriff auf das blockierte Gerät aktivieren kann.

10. Speichern Sie die Schlüsseldatei auf dem Computer.

So erstellen Sie als Administrator über die Web Console und Cloud Console einen Zugriffsschlüssel für das gesperrte Gerät

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Assets (Geräte)** aus.
2. Wählen Sie in der Liste der Client-Computer den Computer aus, dessen Benutzer temporären Zugriff auf ein gesperrtes Gerät erhalten soll.
3. Klicken Sie auf die Schaltfläche mit den Auslassungspunkten (...) über der Liste der Computer und klicken Sie anschließend auf die Schaltfläche **Zugriff auf das Gerät im autonomen Modus gewähren**.
4. Wählen Sie im folgenden Fenster den Abschnitt **Gerätekontrolle**.
5. Klicken Sie auf **Übersicht** und öffnen Sie die Zugriffsanfrage-Datei, die Sie vom Benutzer erhalten haben.

   Es werden Informationen über das blockierte Gerät angezeigt, auf das der Benutzer den Zugriff erfragt hat.
6. Ändern Sie erforderlichenfalls den Wert der Einstellung **Zugriffsdauer (Stunden)**.

   Für die Einstellung **Zugriffsdauer (Stunden)** ist standardmäßig der Wert festgelegt, der vom Benutzer bei der Erstellung der Zugriffsanfrage-Datei angegeben wurde.
7. Geben Sie den Zeitraum an, während dem der Zugriffsschlüssel auf dem Gerät aktiviert werden kann.

   Diese Einstellung enthält den Zeitraum, während dem der Benutzer mithilfe des Zugriffsschlüssels den Zugriff auf das blockierte Gerät aktivieren kann.
8. Speichern Sie die Schlüsseldatei auf dem Computer.

Dadurch wird der Zugriffsschlüssel für das blockierte Gerät auf den Computer geladen. Die Zugriffsschlüsseldatei hat die Erweiterung *.acode. Senden Sie den Zugriffsschlüssel für das blockierte Gerät auf beliebige Weise an den Benutzer.

Um als Benutzer den Zugriffsschlüssel zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffsanforderung** auf **Zugriff auf ein Gerät erfragen**.
4. Klicken Sie im angezeigten Fenster auf **Zugriffsschlüssel aktivieren**.
5. Wählen Sie im folgenden Fenster die Datei mit dem Zugriffsschlüssel für das Gerät aus, die Sie vom Administrator des lokalen Unternehmensnetzwerks erhalten haben.

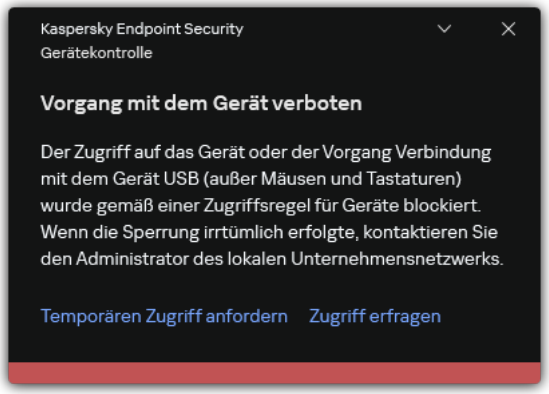
   Ein Fenster mit Informationen über die Freigabe wird geöffnet.
6. Klicken Sie auf **OK**.

Dadurch erhält der Benutzer für den vom Administrator festgelegten Zeitraum Zugriff auf das Gerät. Der Benutzer erhält einen kompletten Berechtigungssatz für den Zugriff auf das Gerät (Schreiben und Lesen). Wenn der Zugriffsschlüssel abläuft, wird der Zugriff auf das Gerät blockiert. Falls der Benutzer permanenten Zugriff auf das Gerät benötigt, fügen Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

Meldungsvorlagen für die Gerätekontrolle ändern

Versucht ein Benutzer, auf ein blockiertes Gerät zuzugreifen, so meldet Kaspersky Endpoint Security die Sperrung des Geräts oder das Verbot für einen Vorgang mit dem Geräteinhalt. Die Kaspersky-Experten haben eine Nachrichtenvorlage vorbereitet. In dieser Nachricht wird dem Benutzer erklärt, warum der Zugriff auf das Gerät gesperrt wurde (siehe folgende Abb.).

Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden. Wenn eine Nachricht generiert wird, ruft Kaspersky Endpoint Security den Wert der Variablen aus den Betriebssystemeinstellungen ab und fügt ihn passend zum Computer, Benutzer und Ereignis in die Nachricht ein.



Benachrichtigung der „Gerätekontrolle"

Ist der Benutzer der Meinung, die Zugriffsverweigerung auf ein Gerät oder das Verbot eines Vorgangs mit dem Geräteinhalt sei irrtümlich erfolgt, so kann der Benutzer eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden. Dafür ist im Text der Sperrmeldung ein Link vorgesehen. Dazu muss der Benutzer auf **Zugriff erfragen** oder **Temporären Zugriff anfordern** klicken und eine Nachricht an den Administrator senden, um die Situation zu beschreiben. Sie können auch eine Vorlage für die Nachricht an den Administrator erstellen. Dieser Nachricht können Sie Daten hinzufügen, die Ihre Entscheidung, den Zugriff auf das Gerät zuzulassen oder zu sperren, begründen. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Zugriffsverbot auf Gerät**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

So ändern Sie die Nachrichtenvorlagen der Gerätekontrolle über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Gerätekontrolle** aus.
4. Klicken Sie im Block **Einstellungen für Nachrichtenvorlagen** auf **Vorlagen**.

5. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die Vorlagen der Programmkontrolle:

   - **Nachricht beim Blockieren**. 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.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable** und wählen Sie die gewünschte Variable in der Liste aus.

   Sie können auch den Standardvorlagentext wiederherstellen.

6. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie die Nachrichtenvorlagen der Gerätekontrolle über die Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **Gerätekontrolle**.

5. Konfigurieren Sie im Block **Vorlagen für Nachrichten** die Nachrichtenvorlagen für die „Programmkontrolle“:

   - **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.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

   Sie können auch den Standardvorlagentext wiederherstellen.

6. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie die Nachrichtenvorlagen der Gerätekontrolle über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Programmkontrolle** aus.

3. Konfigurieren Sie im Block **Vorlagen für Nachrichten** die Nachrichtenvorlagen für die „Programmkontrolle“:

   - **Nachricht beim Blockieren**. 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.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

   Sie können auch den Standardvorlagentext wiederherstellen.

4. Speichern Sie die vorgenommenen Änderungen.

Anti-Bridging

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 reguliert die Herstellung von Netzwerkverbindungen und verwendet dazu *Verbindungsregeln*.

Für die folgenden vordefinierten Gerätetypen sind bereits Verbindungsregeln vorhanden:

- Netzwerkadapter;
- WLAN-Adapter;
- Modems.

Wenn eine Verbindungsregel aktiviert ist, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Wird eine neue Verbindung hergestellt, so wird die aktive Verbindung blockiert, falls für beide Verbindungen der in der Regel angegebene Gerätetyp verwendet wird;
- Verbindungen werden blockiert, wenn Sie mithilfe von Gerätetypen, für die Regeln mit einer niedrigeren Priorität verwendet werden, hergestellt wurden oder hergestellt werden sollen.

Anti-Bridging aktivieren

Die Funktion Anti-Bridging ist standardmäßig deaktiviert.

So aktivieren Sie Anti-Bridging:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Anti-Bridging**.

4. Verwenden Sie den Schalter **Anti-Bridging aktivieren**, um diese Funktion zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

Nachdem die Funktion Anti-Bridging aktiviert wurde, blockiert Kaspersky Endpoint Security die bereits bestehenden Verbindungen gemäß der Verbindungsregeln.

Status einer Verbindungsregel ändern

Im den Status einer Verbindungsregel zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Anti-Bridging**.
4. Wählen Sie im Block **Regeln für Geräte** die Regel aus, deren Status Sie ändern möchten.
5. Verwenden Sie die Schalter in der Spalte **Kontrolle**, um die Regel zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

Priorität einer Verbindungsregel ändern

Im die Priorität einer Verbindungsregel zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Gerätekontrolle** aus.
3. Klicken Sie im Block **Zugriffseinstellungen** auf **Anti-Bridging**.
4. Wählen Sie im Block **Regeln für Geräte** die Regel aus, deren Priorität Sie ändern möchten.
5. Verwenden Sie die Schaltflächen **Aufwärts** / **Abwärts**, um die Priorität der Verbindungsregel festzulegen.

   Je höher die Position einer Regel in der Tabelle ist, desto höher ist ihre Priorität. Die Funktion Anti-Bridging blockiert alle Verbindungen, unter Ausnahme der Verbindung, die mithilfe des Gerätetyps hergestellt wurde, für welchen die Regel mit der höchsten Priorität verwendet wird.
6. Speichern Sie die vorgenommenen Änderungen.

Adaptive Kontrolle von Anomalien

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Adaptive Kontrolle von Anomalien“ überwacht und blockiert Aktionen, die für Computer des Unternehmensnetzwerks untypisch sind. Zur Überwachung von untypischen Aktionen verwendet die „Adaptive Kontrolle von Anomalien“ eine Auswahl von Regeln (z. B. die Regel *Start von Windows PowerShell aus einem Office-Programm*). Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für schädliche Aktivitäten erstellt. Sie können ein Verhalten der „Adaptiven Kontrolle von Anomalien“ für jede einzelne Regeln auswählen und beispielsweise den Start von PowerShell-Skripten erlauben, um die Lösung von Unternehmensaufgaben zu automatisieren. Kaspersky Endpoint Security aktualisiert den Regelsatz aus den Programm-Datenbanken. Die Aktualisierung des Regelsatzes muss manuell bestätigt werden.

„Adaptive Kontrolle von Anomalien“ anpassen

Die Anpassung der „Adaptiven Kontrolle von Anomalien“ umfasst folgende Schritte:

1. Training der „Adaptiven Kontrolle von Anomalien“.

   Nachdem die „Adaptive Kontrolle von Anomalien“ aktiviert ist, funktionieren die Regeln im *Lernmodus*. Im Verlauf des Trainings überwacht die „Adaptive Kontrolle von Anomalien“ die Auslösung von Regeln und sendet Auslöseereignisse an Kaspersky Security Center. Jede Regel hat eine eigene Dauer für den Lernmodus. Die Dauer des Lernmodus wird von den Kaspersky-Experten vorgegeben. Gewöhnlich dauert der Lernmodus 2 Wochen.

   Wenn eine Regel während des Trainings nie ausgelöst wurde, betrachtet die „Adaptive Kontrolle von Anomalien“ die mit dieser Regel verbundenen Aktionen als untypisch. Kaspersky Endpoint Security blockiert alle Aktionen, die mit dieser Regel zusammenhängen.

   Wenn während des Trainings eine Regel ausgelöst wurde, protokolliert Kaspersky Endpoint Security die Ereignisse im Bericht über ausgelöste Regeln und in der Datenverwaltung **Auslöser der Regel im Smart-Training-Status**.

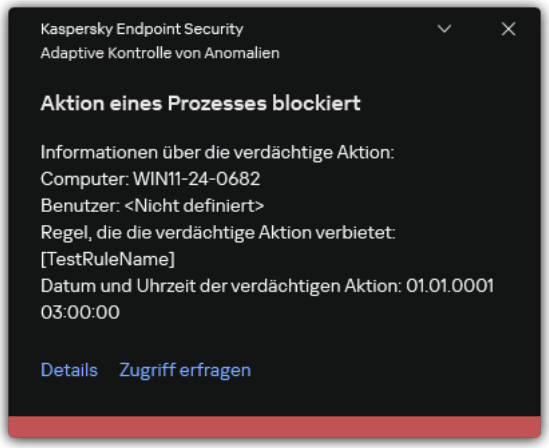
2. Analyse des Berichts über ausgelöste Regeln.

   Der Administrator analysiert den Bericht über ausgelöste Regeln oder den Inhalt der Datenverwaltung **Auslöser der Regel im Smart-Training-Status**. Anschließend kann der Administrator das Verhalten der „Adaptiven Kontrolle von Anomalien“ bei einer Auslösung der Regel festlegen: blockieren oder erlauben. Außerdem kann der Administrator die Regelauslösung weiterhin überwachen und die Dauer des Lernmodus für das Programm verlängern. Ergreift der Administrator keine Maßnahmen, so läuft das Programm ebenfalls im Lernmodus weiter. Die Dauer des Lernmodus beginnt von vorne.

Die Adaptive Kontrolle von Anomalien über die folgenden Kanäle in Echtzeit konfiguriert werden:

- Die „Adaptive Kontrolle von Anomalien“ beginnt automatisch, jene Aktionen zu blockieren, die mit Regeln zusammenhängen, die im Lernmodus nicht ausgelöst wurden.
- Kaspersky Endpoint Security fügt neue Regeln hinzu oder löscht veraltete Regeln.
- Der Administrator analysiert den Bericht über ausgelöste Regeln und den Inhalt des Repositorys **Auslöser der Regel im Smart-Training-Status** und konfiguriert anschließend die „Adaptive Kontrolle von Anomalien“. Es wird empfohlen, den Bericht über ausgelöste Regeln und den Inhalt des Speichers **Auslöser der Regel im Smart-Training-Status** zu überprüfen.

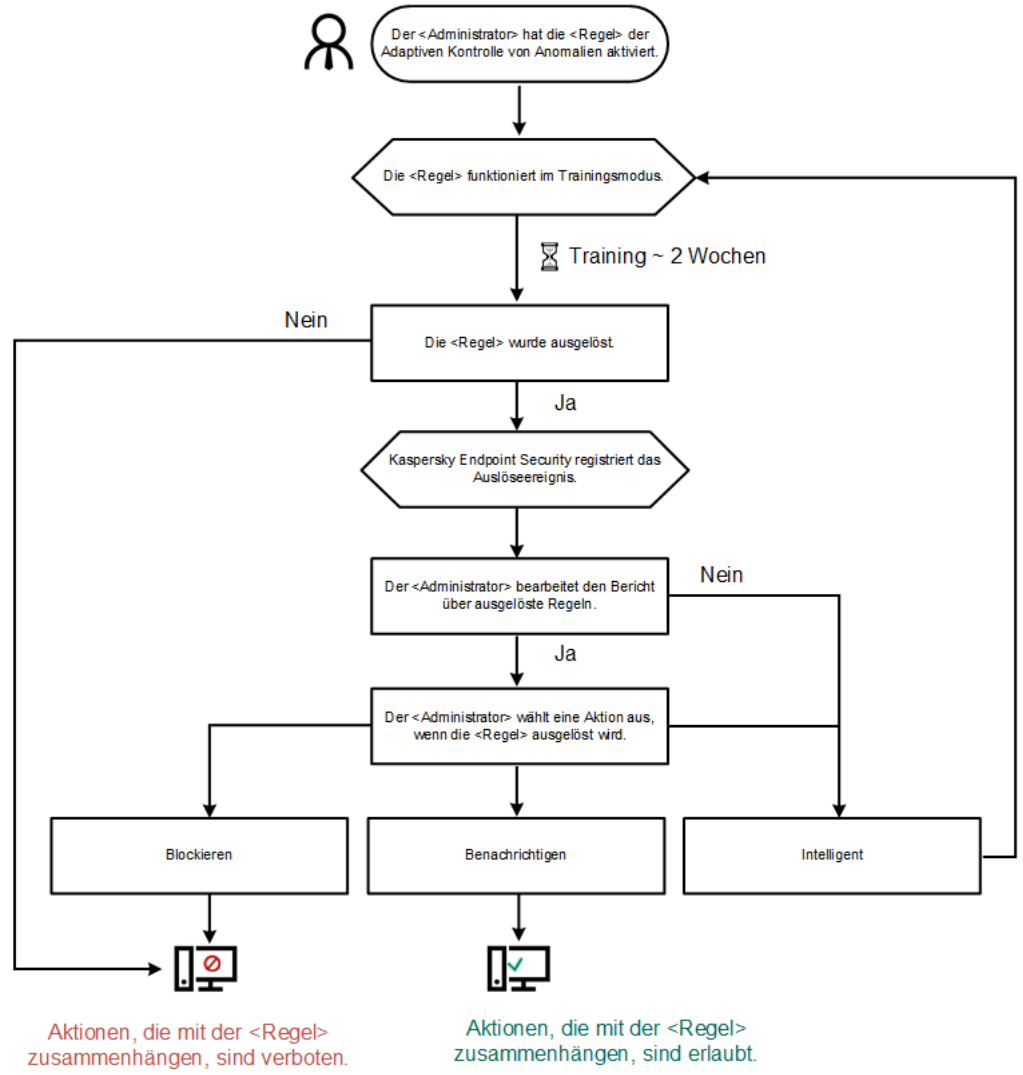
Wenn ein Schadprogramm versucht, eine Aktion auszuführen, blockiert Kaspersky Endpoint Security die Aktion und zeigt eine Benachrichtigung an (siehe Abbildung unten).



Benachrichtigung der „Adaptiven Kontrolle von Anomalien“

Algorithmus der „Adaptiven Kontrolle von Anomalien"

Um über die Ausführung einer Aktion, die mit einer Regeln verbunden ist, zu entscheiden, nutzt Kaspersky Endpoint Security den folgenden Algorithmus (siehe Abbildung unten).



Algorithmus der „Adaptiven Kontrolle von Anomalien"

Training der „Adaptiven Kontrolle von Anomalien"

Die Adaptive Kontrolle von Anomalien verwendet bestimmte Regeln (Verhaltensmuster). Nachdem die „Adaptive Kontrolle von Anomalien" aktiviert ist, funktionieren die Regeln im *Lernmodus*. Im Verlauf des Trainings überwacht die „Adaptive Kontrolle von Anomalien" die Auslösung von Regeln und sendet Auslöseereignisse an Kaspersky Security Center. Die Adaptive Kontrolle von Anomalien blockiert die Programmaktivität auf dem Computer nicht, sondern informiert nur den Administrator. Die Aktion, die beim Auslösen einer Regel der Adaptiven Kontrolle von Anomalien ausgeführt wird, kann auch manuell ausgewählt werden.

So zeigen Sie die Liste mit den Regeln der Adaptiven Kontrolle von Anomalien an (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.

3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.

5. Aktivieren Sie das Kontrollkästchen **Adaptive Kontrolle von Anomalien**.

6. Sehen Sie sich unter **Einstellungen der Regeln für die Adaptive Kontrolle von Anomalien** die Liste der Regeln an.

   Standardmäßig funktionieren alle Regeln im Modus **Intelligent**.

7. Bestätigen Sie bei Bedarf, dass die Regel der Adaptiven Kontrolle von Anomalien aktualisiert werden soll.

8. Wählen Sie bei Bedarf eine Aktion aus, die beim Auslösen einer Regel der Adaptiven Kontrolle von Anomalien ausgeführt werden soll:

   - **Blockieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so blockiert Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

   - **Informieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

9. Deaktivieren Sie bei Bedarf die Regeln, die Sie nicht verwenden möchten.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So zeigen Sie die Regeln der Adaptiven Kontrolle von Anomalien an (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien**.

5. Aktivieren Sie den Schalter **Adaptive Kontrolle von Anomalien AKTIVIERT**.

6. Sehen Sie sich unter **Regeln** die Liste der Regeln an.

   Standardmäßig funktionieren alle Regeln im Modus **Intelligent**.

7. Bestätigen Sie bei Bedarf, dass die Regel der Adaptiven Kontrolle von Anomalien aktualisiert werden soll.

8. Wählen Sie bei Bedarf eine Aktion aus, die beim Auslösen einer Regel der Adaptiven Kontrolle von Anomalien ausgeführt werden soll:

   - **Blockieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so blockiert Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

   - **Informieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

9. Deaktivieren Sie bei Bedarf die Regeln, die Sie nicht verwenden möchten.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So zeigen Sie die Liste mit den Regeln der Adaptiven Kontrolle von Anomalien an (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.

3. Aktivieren Sie den Schalter **Adaptive Kontrolle von Anomalien**.

4. Klicken Sie im Block **Regeln** auf den Link **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet. Standardmäßig funktionieren alle Regeln im Modus **Intelligent**.

5. Bestätigen Sie bei Bedarf, dass die Regel der Adaptiven Kontrolle von Anomalien aktualisiert werden soll.

6. Wählen Sie bei Bedarf eine Aktion aus, die beim Auslösen einer Regel der Adaptiven Kontrolle von Anomalien ausgeführt werden soll:

   - **Blockieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so blockiert Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

   - **Informieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

7. Deaktivieren Sie bei Bedarf die Regeln, die Sie nicht verwenden möchten.

8. Speichern Sie die vorgenommenen Änderungen.

Jede Regel hat eine eigene Dauer für den Lernmodus. Die Dauer des Lernmodus wird von den Kaspersky-Experten vorgegeben. Gewöhnlich dauert der Lernmodus 2 Wochen.

Wenn eine Regel während des Trainings nie ausgelöst wurde, betrachtet die Adaptive Kontrolle von Anomalien solches Verhalten als untypisch und ändert den Status der Regel in **Intelligentes Blockieren**. Das Programm blockiert künftig alle Aktivitäten, die dieser Regel entsprechen.

Wenn eine Regel während des Trainings ausgelöst wird, gehen Sie wie folgt vor: Konfigurieren Sie manuell die Aktion, die das Programm mit der erkannten, dieser Regel entsprechenden Aktivität ausführen soll. Wenn Sie beim Auslösen der Regel keine Aktion auswählen, wird die Adaptive Kontrolle von Anomalien im Trainingsmodus fortgesetzt.

Regel der Adaptiven Kontrolle von Anomalien aktivieren und deaktivieren

Um eine Regeln der Adaptiven Kontrolle von Anomalien zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. Wählen Sie in der Tabelle einen Regelsatz aus (z. B. *Aktivität von Office-Software*) und erweitern Sie den Satz.
5. Wählen Sie eine Regel aus (z. B. *Start von Windows PowerShell aus einem Office-Programm*).
6. Verwenden Sie den Schalter in der Spalte **Status**, um die „Adaptive Kontrolle von Anomalien“ zu aktivieren oder zu deaktivieren.
7. Speichern Sie die vorgenommenen Änderungen.

Aktion für den Fall, dass eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst wird, ändern

Um die Aktion für den Fall, dass eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst wird, zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. Wählen Sie eine Regel in der Tabelle aus.
5. Klicken Sie auf **Bearbeiten**.

   Das Eigenschaftenfenster der „Adaptive Kontrolle von Anomalien“-Regel wird geöffnet.

6. Wählen Sie im Block **Aktion** eine der folgenden Optionen aus:

   - **Intelligent**. Wenn diese Option ausgewählt ist, funktioniert die Regel der Adaptiven Kontrolle von Anomalien für einen bestimmten Zeitraum im Lernmodus. Der Zeitraum wird von den Kaspersky-Experten festgelegt. Wenn in diesem Modus eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst wird, erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Eintrag im Speicher **Auslöser der Regel im Smart-Training-Status** des Kaspersky Security Center-Administrationsservers. Nachdem der Zeitraum für den Lernmodus abgelaufen ist, blockiert Kaspersky Endpoint Security die Aktivität, die unter eine Regel der „Adaptiven Kontrolle von Anomalien“ fällt, und erstellt im Bericht einen Eintrag, der Informationen über diese Aktivität enthält.

   - **Blockieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so blockiert Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

   - **Informieren**. Wenn diese Aktion ausgewählt wurde und es wird eine Regel der Adaptiven Kontrolle von Anomalien ausgelöst, so erlaubt Kaspersky Endpoint Security die Aktivität, die unter diese Regel fällt, und erstellt einen Berichtseintrag, der Informationen über diese Aktivität enthält.

7. Speichern Sie die vorgenommenen Änderungen.

Um eine Ausnahme für eine „Adaptive Kontrolle von Anomalien“-Regel zu löschen, gehen Sie wie folgt vor:

Für die Regeln der Adaptiven Kontrolle von Anomalien können maximal 1.000 Ausnahmen erstellt werden. Es wird davon abgeraten, mehr als 200 Ausnahmen zu erstellen. Um die Anzahl der verwendeten Ausnahmen zu reduzieren, können in den Ausnahmeeinstellungen Masken angegeben werden.

Eine Ausnahme für eine Regel der „Adaptiven Kontrolle von Anomalien“ enthält eine Beschreibung der Quell- und Zielobjekte. *Quellobjekt* – Objekt, das Aktionen ausführt. *Zielobjekt* – Objekt, mit dem Aktionen ausgeführt werden. Beispiel: Sie haben die Datei `file.xlsx` geöffnet. Als Ergebnis wird eine Bibliotheksdatei mit der DLL-Erweiterung in den Computerspeicher geladen. Diese Bibliothek wird von einem Browser verwendet (ausführbare Datei namens `browser.exe`). In diesem Beispiel ist `file.xlsx` das Quellobjekt, Excel der Quellprozess, `browser.exe` das Zielobjekt, und der Browser der Zielprozess.

Um eine Ausnahme für eine Regel der „Adaptiven Kontrolle von Anomalien“ zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.

3. Klicken Sie im Block **Regeln** auf **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.

4. Wählen Sie eine Regel in der Tabelle aus.

5. Klicken Sie auf **Bearbeiten**.

   Das Eigenschaftenfenster der „Adaptive Kontrolle von Anomalien“-Regel wird geöffnet.

6. Klicken Sie im Block **Ausnahmen** auf **Hinzufügen**.

   Das Eigenschaftenfenster der Ausnahme wird geöffnet.

7. Wählen Sie den Benutzer aus, für den Sie eine Ausnahme konfigurieren möchten.

   Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

   > Die „Adaptive Kontrolle von Anomalien" unterstützt keine Ausnahmen für Benutzergruppen. Wenn Sie eine Benutzergruppe auswählen, wendet Kaspersky Endpoint Security die Ausnahme nicht an.

8. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Ausnahme ein.

9. Geben Sie die Einstellungen des Quellobjekts oder des Quellprozesses an, die von dem Objekt gestartet wurden:

   - **Quellprozess**. Pfad oder Pfadmaske für eine Datei oder für einen Ordner mit Dateien (z. B. `C:\Dir\File.exe` oder `Dir\*.exe`).
   - **Hash des Quellprozesses**. SHA256-Hash der Datei.
   - **Quellobjekt**. Pfad oder Pfadmaske für eine Datei oder für einen Ordner mit Dateien (z. B. `C:\Dir\File.exe` oder `Dir\*.exe`). Beispiel: Pfad der Datei `document.docm`, welche die Zielprozesse mithilfe eines Skripts oder Makros startet.

     Sie können auch andere Objekte für eine Ausnahme angeben, beispielsweise eine Webadresse, ein Makro, einen Befehl in der Befehlszeile, einen Registrierungspfad und andere. Geben Sie das Objekt gemäß der folgenden Vorlage an: `object://<object>` wobei `<object>` für den Namen des Objekts steht. Beispiele: `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Sie können auch Masken verwenden, beispielsweise `object://*C:\Windows\temp\*`.
   - **Hash des Quellobjekts**. SHA256-Hash der Datei.

   Die Regel für die „Adaptive Kontrolle von Anomalien" erstreckt sich nicht auf die Aktionen, die von dem Objekt ausgeführt werden, oder auf Prozesse, die von dem Objekt gestartet werden.

10. Geben Sie die Einstellungen des Zielobjekts oder der Zielprozesse an, die mit dem Objekt ausgeführt wurden.

    - **Zielprozess**. Pfad oder Pfadmaske für eine Datei oder für einen Ordner mit Dateien (z. B. `C:\Dir\File.exe` oder `Dir\*.exe`).
    - **Hash des Zielprozesses**. SHA256-Hash der Datei.
    - **Zielobjekt**. Befehl zum Starten des Zielprozesses. Geben Sie den Befehl nach dem Muster `object://<command>` an. Beispiel: `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Sie können auch Masken verwenden, beispielsweise `object://*C:\Windows\temp\*`.
    - **Hash des Zielobjekts**. SHA256-Hash der Datei.

    Die Regel für die „Adaptive Kontrolle von Anomalien" erstreckt sich nicht auf die Aktionen mit dem Objekt oder auf die Prozesse, die mit dem Objekt ausgeführt werden.

11. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Ausnahmen für die Regeln der „Adaptiven Kontrolle von Anomalien”

So exportieren oder importieren Sie die Liste der Ausnahmen für ausgewählte Regeln:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Regeln aus, deren Ausnahmen Sie exportieren möchten.
   b. Klicken Sie auf **Export**.
   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.
   e. Speichern Sie die Datei.
5. So importieren Sie die Ausnahmeliste:
   a. Klicken Sie auf **Import**.
   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.
   c. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.
6. Speichern Sie die vorgenommenen Änderungen.

Updates für die Regeln der Adaptiven Kontrolle von Anomalien übernehmen

Neue Regeln der „Adaptiven Kontrolle von Anomalien“ können zur Regeltabelle hinzugefügt werden und vorhandene Regeln der „Adaptiven Kontrolle von Anomalien“ können abhängig vom Ergebnis des Updates der Antiviren-Datenbanken aus der Regeltabelle gelöscht werden. Kaspersky Endpoint Security markiert zu löschende und hinzuzufügende Regeln der „Adaptiven Kontrolle von Anomalien“ in der Tabelle, falls das Update für diese Regeln nicht übernommen wurde.

Bis ein Update übernommen wurde, zeigt Kaspersky Endpoint Security die Regeln der Adaptiven Kontrolle von Anomalien, die aufgrund des Updates gelöscht werden, in der Tabelle mit dem Status *Deaktiviert* an. Die Einstellungen dieser Regeln können nicht geändert werden.

Um ein Update für die Regeln der Adaptiven Kontrolle von Anomalien zu übernehmen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.
3. Klicken Sie im Block **Regeln** auf **Regeln bearbeiten**.

   Die Regelliste für Adaptive Kontrolle von Anomalien wird geöffnet.
4. Klicken Sie im angezeigten Fenster auf **Updates bestätigen**.

   Die Schaltfläche **Updates bestätigen** ist verfügbar, wenn ein Update für die Regeln der Adaptiven Kontrolle von Anomalien vorliegt.
5. Speichern Sie die vorgenommenen Änderungen.

Meldungsvorlagen für die Adaptiven Kontrolle von Anomalien ändern

Wenn ein Benutzer versucht, eine Aktion auszuführen, die durch Regeln der „Adaptiven Kontrolle von Anomalien“ verboten ist, so meldet Kaspersky Endpoint Security, dass potentiell gefährliche Aktionen blockiert wurden. Wenn der Benutzer der Meinung ist, die Sperrung sei irrtümlich erfolgt, kann er aus der Sperrmeldung eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden.

Für Nachrichten, die den Administrator über das Blockieren potenziell schädlicher Aktionen informieren, stehen spezielle Vorlagen zur Verfügung. Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden. Wenn eine Nachricht generiert wird, ruft Kaspersky Endpoint Security den Wert der Variablen aus den Betriebssystemeinstellungen ab und fügt ihn passend zum Computer, Benutzer und Ereignis in die Nachricht ein.

Gehen Sie folgendermaßen vor, um eine Meldungsvorlage zu ändern:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien** aus.
3. Konfigurieren Sie im Block **Vorlagen** die Vorlagen für Nachrichten der Adaptiven Kontrolle von Anomalien:

   - **Nachricht beim Blockieren**. Vorlage der Nachricht an den Benutzer. Diese Nachricht wird angezeigt, wenn eine Regel der „Adaptiven Kontrolle von Anomalien“ ausgelöst wird, die eine untypische Aktion blockiert.
   - **Nachricht an den Administrator**. Vorlage der Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn eine Aktion nach Meinung des Benutzers irrtümlich blockiert wurde. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über das Verbot einer Programmaktion**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

   Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Zurücksetzen** wiederherstellen.
4. Speichern Sie die vorgenommenen Änderungen.

Überwachungstools der „Adaptiven Kontrolle von Anomalien“

Die „Adaptive Kontrolle von Anomalien“ umfasst mehrere Überwachungstools. Der Hauptzweck der Überwachung der „Adaptiven Kontrolle von Anomalien“ besteht darin, die Komponente während des Trainings zu konfigurieren.

Berichte der „Adaptiven Kontrolle von Anomalien“

Die „Adaptive Kontrolle von Anomalien“ verwendet die folgenden Berichte:

- **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“**. Der Bericht enthält Informationen über den Status der Regeln der Adaptiven Kontrolle von Anomalien (*Aus*, *Smart Training*, *Smarte Blockierung*, *Benachrichtigen*, *Blockieren*). Mit diesem Bericht können Sie den Trainingsstand der Adaptiven Kontrolle von Anomalien analysieren und ermitteln, für wie viele Regeln der Modus *Smart Training* in den normalen Funktionsmodus (z. B. *Smarte Blockierung*) geändert wurde.
- **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“**. Der Bericht enthält Informationen zu Regelauslösern. Der Bericht enthält auch Informationen zum Auslösemodus für Regeln: *Blockieren* (einschließlich *Smarte Blockierung*) oder *Benachrichtigen*. Mit diesem Bericht können Sie die Aktivität der „Adaptiven Kontrolle von Anomalien“ auf Benutzercomputern auswerten.

So zeigen Sie Berichte der „Adaptiven Kontrolle von Anomalien“ an (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien**.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um einen Bericht über den Status von Regeln der „Adaptiven Kontrolle von Anomalien“ anzuzeigen, klicken Sie auf den Link **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“**.
   - Wenn Sie einen Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“ anzeigen möchten, klicken Sie auf den Link **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“**.
5. Der Vorgang zur Berichterstellung wird gestartet.

Der Bericht wird in einem neuen Fenster angezeigt.

So zeigen Sie Berichte der „Adaptiven Kontrolle von Anomalien“ an (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle → Adaptive Kontrolle von Anomalien**.
5. Führen Sie im Block **Regeln** eine der folgenden Aktionen aus:
   - Wenn Sie den Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“ anzeigen möchten, wählen Sie **Bericht anzeigen → Status der Regel** aus.
   - Wenn Sie den Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“ anzeigen möchten, klicken Sie auf **Bericht anzeigen → Erkennungen**.
6. Der Vorgang zur Berichterstellung wird gestartet.

Der Bericht wird in einem neuen Fenster angezeigt.

Um Berichte in der Kaspersky Security Center-Konsole zu erstellen, müssen Sie die Datenübertragung an den Administrationsserver aktivieren. Die Datenübertragung ist standardmäßig aktiviert.

So aktivieren Sie die Datenübertragung für die „Adaptive Kontrolle von Anomalien“ (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Berichte und Speicher** aus.

4. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Einstellungen**.
5. Aktivieren Sie die folgenden Kontrollkästchen:
   - **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“**.
   - **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“**.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Datenübertragung für die „Adaptive Kontrolle von Anomalien“ (in der Web Console)

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **KSC-Integration**.
5. Aktivieren Sie unter **Datenübertragung an den Administrationsserver** die folgenden Kontrollkästchen:
   - **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“**.
   - **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“**.
6. Speichern Sie die vorgenommenen Änderungen.

Speicher Auslöser der Regel im Smart-Training-Status

Im Trainingsmodus sendet die Adaptive Kontrolle von Anomalien Informationen über ausgelöste Regeln an einen separaten Speicher (**Auslöser der Regel im Smart-Training-Status**). Informationen über ausgelöste Regeln werden im Speicher als Ereignisliste angezeigt. Um die „Adaptive Kontrolle von Anomalien“ anzupassen, können Sie entweder das ungewöhnliche Verhalten auf dem Computer bestätigen oder eine Ausnahme für die Regel hinzufügen.

Ereignisse in der „Adaptiven Kontrolle von Anomalien“

Die Adaptive Kontrolle von Anomalien protokolliert Ereignisse, bei denen Regeln ausgelöst werden, in den Modi *Blockieren* (einschließlich *Smarte Blockierung*) und *Benachrichtigen*. Dazu sind folgende Ereignisse vorgesehen:

Aktion eines Prozesses blockiert

Aktion eines Prozesses übersprungen

Ereignisse enthalten Informationen über die verdächtige Aktivität, einschließlich Dateiprüfsummen, beteiligte Benutzer, Zeitpunkt der Regelauslösung und Computername. Wenn die Ereignisanalyse ergibt, dass die Aktivität zulässig ist, können Sie sofort Ausnahmen für die Regel hinzufügen.

Programmkontrolle

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 „Programmkontrolle“ wird mit folgenden Schritten angepasst:

1. Programmkategorien erstellen

   Der Administrator erstellt Kategorien für die Programme, die er verwalten möchte. Die Programmkategorien gelten unabhängig von der Administrationsgruppe für alle Computer des Unternehmensnetzwerks. Um eine Kategorie zu erstellen, können Sie beispielsweise folgende Kriterien verwenden: KL-Kategorie (z. B. *Browser* oder another category), Datei-Hash und Programmhersteller.

2. Programmkontrolle-Regeln erstellen.

   Der Administrator erstellt Regeln der „Programmkontrolle“ in der Richtlinie für die Administrationsgruppe. Eine Regel enthält Programmkategorien und einen Startstatus für die Programme aus diesen Kategorien: verboten oder erlaubt. 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.

3. Modus der „Programmkontrolle“ auswählen.

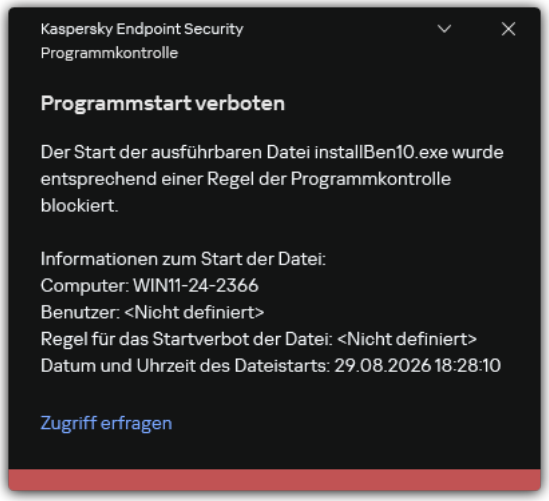
   Der Administrator wählt einen Modus für die Arbeit mit den Programmen aus, die zu keiner Regel gehören: Denyliste und Allowliste.

Wenn der Benutzer versucht, ein verbotenes Programm zu starten, blockiert Kaspersky Endpoint Security den Programmstart und zeigt eine Benachrichtigung an (s. Abb. unten).

Die Einstellungen der „Programmkontrolle“ können im *Testmodus* überprüft werden. In diesem Modus führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Der Start von Programmen (auch von verbotenen Programmen) wird erlaubt.
- Beim Start eines verbotenen Programms wird eine entsprechende Benachrichtigung angezeigt und Informationen werden zum Bericht auf dem Benutzercomputer Informationen hinzugefügt.

- Daten über den Start verbotener Programme werden an Kaspersky Security Center gesendet.



Benachrichtigung der „Programmkontrolle"

Modi der „Programmkontrolle"

Die Komponente „Programmkontrolle" bietet zwei Modi:

- **Deny-Liste**. In diesem Modus erlaubt die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" verboten sind.

  Dieser Modus ist für die Programmkontrolle standardmäßig ausgewählt.

- **Allow-Liste**. In diesem Modus verbietet die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" erlaubt und nicht verboten sind.

  Wenn eine extrem genaue Erlaubnisregel für die Programmkontrolle erstellt wurde, verbietet die Komponente den Start aller neuen Programme, die noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüft wurden, gewährleistet dabei aber die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Programme, die von Benutzern für dienstliche Zwecke benötigt werden.

  Beachten Sie die Tipps für die Anpassung von Regeln der Programmkontrolle im Allowlist-Modus.

Diese Modi für die Programmkontrolle können sowohl auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security als auch mithilfe von Kaspersky Security Center angepasst werden.

Allerdings verfügt Kaspersky Security Center über Tools, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht verfügbar sind und für folgende Aufgaben dienen:

- Programmkategorien erstellen

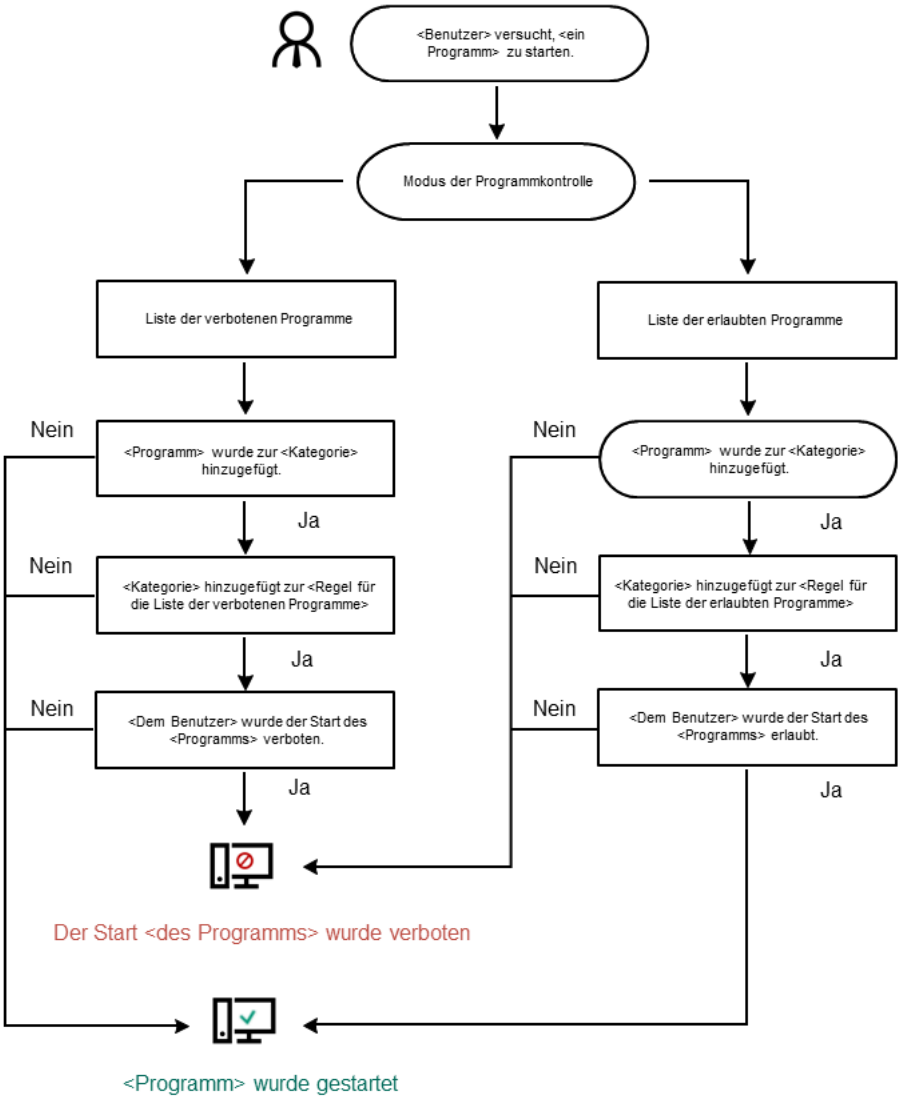
  Die Regeln der Programmkontrolle, die in der Verwaltungskonsole von Kaspersky Security Center erstellt wurden, beruhen auf den von Ihnen erstellten Programmkategorien, und nicht wie in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security auf ein- und ausschließenden Bedingungen.

- Empfang von Informationen über die Programme, die auf den Computern des lokalen Unternehmensnetzwerks installiert sind

Deshalb wird empfohlen, die Komponente „Programmkontrolle" mithilfe von Kaspersky Security Center anzupassen.

Algorithmus der „Programmkontrolle”

Kaspersky Endpoint Security verwendet einen Algorithmus, um über den Start eines Programms zu entscheiden (s. Abb. unten).



Algorithmus der „Programmkontrolle”

Funktionelle Beschränkungen der Programmkontrolle

Die Funktion der Komponente „Programmkontrolle“ ist in folgenden Fällen beschränkt:

- Beim Programm-Upgrade wird der Import von Einstellungen für die Komponente „Programmkontrolle“ nicht unterstützt.
- Wenn keine Verbindung mit den KSN-Servern besteht, empfängt Kaspersky Endpoint Security die Informationen über die Reputation von Programmen und Modulen nur aus den lokalen Datenbanken.

  Die Liste der Programme, die Kaspersky Endpoint Security der KL-Kategorie **Andere Programme\Programme, die laut KSN-Reputation vertrauenswürdig sind** zuordnet, kann unterschiedlich sein, je nachdem, ob eine Verbindung zu den KSN-Servern besteht oder nicht.

- Kaspersky Security Center kann Informationen über maximal 150.000 verarbeitete Dateien in der Datenbank speichern. Wenn diese Anzahl von Einträgen erreicht ist, werden neue Dateien nicht mehr verarbeitet. Um die Inventarisierung fortzusetzen, müssen von dem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, Dateien gelöscht werden, die bisher bei der Inventarisierung in der Datenbank für Kaspersky Security Center aufgezeichnet worden sind.
- Der Start von Skripten wird von der Komponente nicht kontrolliert, wenn ein Skript nicht über die Befehlszeile an den Interpreter übermittelt wird.

  Ist der Start des Interpreters durch Regeln der Programmkontrolle erlaubt, so blockiert die Komponente ein Skript nicht, das aus diesem Interpreter gestartet wurde.

  Wenn die Regeln der Programmkontrolle mindestens den Start von einem der Skripte verbieten, die in der Interpreter-Befehlszeile angegeben sind, so blockiert die Komponente alle Skripte, die in der Interpreter-Befehlszeile angegeben sind.

- Der Start von Skripten aus Interpretern wird von der Komponente nicht kontrolliert, wenn der Interpreter vom Programm Kaspersky Endpoint Security nicht unterstützt wird.

  Kaspersky Endpoint Security unterstützt folgende Interpreter:

  - Java
  - PowerShell

  Es werden folgende Interpretertypen unterstützt:

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe

- %SystemRoot%\system32\cscript.exe
- %SystemRoot%\system32\wscript.exe
- %SystemRoot%\system32\msiexec.exe
- %SystemRoot%\system32\mshta.exe
- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

Abrufen von Informationen über installierte Programme

Um optimale Regeln der Programmkontrolle zu erstellen, sollte bekannt sein, welche Programme auf den Computern des lokalen Unternehmensnetzwerks eingesetzt werden. Dazu können Sie folgende Informationen erhalten:

- Hersteller, Versionen und Sprachversionen der Programme, die im lokalen Unternehmensnetzwerk verwendet werden
- Häufigkeit von Programm-Updates
- im Unternehmen geltende Richtlinien für die Nutzung von Programmen (Dies können Sicherheitsrichtlinien oder administrative Richtlinien sein.)
- Speicherort für Programmpakete

Informationen zum Programm anzeigen

Informationen über installierte Programme werden vom Kaspersky Security Center-Administrationsagenten bereitgestellt. Informationen über installierte Programme sind in der Kaspersky Security Center-Konsole im Ordner **Programm-Registry** verfügbar. Der Administrationsagent aktualisiert die Informationen bei jeder Synchronisierung mit Kaspersky Security Center. Details zu den Informationen, die der Administrationsagent sendet, finden Sie in der Hilfe zu Kaspersky Security Center.

Um das Fenster mit den Programmeigenschaften im Ordner „Programm-Registry" zu öffnen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert** → **Programmverwaltung** → **Programm-Registry** aus.
3. Wählen Sie ein Programm aus.
4. Wählen Sie im Kontextmenü des Programms den Punkt **Eigenschaften** aus.

Informationen über ausführbare Dateien anzeigen

Sie können die Auslastung der Datenbank bei der Abfrage von Informationen über ausführbare Dateien reduzieren. Unser Tipp: Führen Sie die Aufgabe *Inventarisierung* auf mehreren Referenzcomputern aus, auf denen Ihre Standardsoftware installiert ist.

Informationen über ausführbare Dateien werden von Kaspersky Endpoint Security bereitgestellt. Um Hardwareinformationen zu erhalten, müssen Sie eine aktive Richtlinie anwenden, welche die Übertragung von Informationen über installierte Programme aktiviert (diese Übertragung ist standardmäßig aktiviert).

So aktivieren Sie die Übertragung von Programminformationen in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Berichte und Speicher** aus.
4. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gestartete Programme**.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über die Web Console und Cloud Console die Übertragung von Programminformationen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **KSC-Integration**.
5. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Erweiterte Einstellungen**.
6. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Über gestartete Programme**.
7. Speichern Sie die vorgenommenen Änderungen.

Eine Liste der ausführbaren Dateien können Sie auch abrufen, indem Sie die Aufgabe *Inventarisierung* von Kaspersky Endpoint Security verwenden. Die Liste der ausführbaren Dateien können Sie in der Kaspersky Security Center-Konsole im Ordner **Ausführbare Dateien** einsehen.

Bevor Sie die Aufgabe *Inventarisierung* ausführen, stellen Sie sicher, dass die Datenbank den Empfehlungen für Kaspersky Security Center entspricht. Details zu den Einschränkungen der Datenbank finden Sie in der Hilfe zu Kaspersky Security Center.

So führen Sie die Aufgabe Inventarisierung über die Verwaltungskonsole (MMC) aus

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Inventarisierung** aus.

Schritt 2. Inventarisierungsbereich

Erstellen Sie eine Liste mit Ordnern, die Kaspersky Endpoint Security nach ausführbaren Dateien durchsuchen soll. Konfigurieren Sie die Inventarisierungseinstellungen (s. folgende Tabelle).

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie eine Benutzerkonto für den Start der Aufgabe *Inventarisierung* aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos. Wenn zum Inventarisierungsbereich Netzlaufwerke oder andere Objekte gehören, auf die der Zugriff beschränkt ist, wählen Sie ein Benutzerkonto mit den erforderlichen Zugriffsrechten aus.

Schritt 5. Zeitplan des Aufgabenstarts anpassen

Konfigurieren Sie den Aufgabenzeitplan, z. B. mit der Option „manuell“.

Schritt 6. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgabe ein, z. B. *Baseline-Inventarisierung*.

Schritt 7. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen. Daraufhin wird auf den Benutzercomputern eine Suche nach ausführbaren Dateien ausgeführt, wobei der festgelegte Zeitplan berücksichtigt wird.

So führen Sie die Aufgabe Inventarisierung aus (in der Web Console und Cloud Console)

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

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

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein (beispielsweise *Baseline-Inventarisierung*).

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Um die Aufgabe zu konfigurieren, gehen Sie zu den Aufgabeneigenschaften (siehe folgende Tabelle).

8. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

9. Klicken Sie auf **Starten**.

   Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen. Daraufhin werden die Benutzercomputer nach ausführbaren Dateien durchsucht, wobei der festgelegte Zeitplan berücksichtigt wird.

So öffnen Sie das Eigenschaftenfenster einer ausführbaren Datei im Ordner Ausführbare Dateien:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert → Programmverwaltung → Ausführbare Dateien** aus.

3. Wählen Sie eine ausführbare Datei aus.

4. Wählen Sie im Kontextmenü der ausführbaren Datei den Punkt **Eigenschaften** aus.

Allgemeine Informationen über das Programm und dessen ausführbare Dateien sowie eine Liste der Computer, auf denen ein Programm installiert ist, finden Sie im Eigenschaftenfenster des ausgewählten Programms im Ordner **Programm-Registry** oder **Ausführbare Dateien**.

Informationen über installierte Anwendungen und ausführbare Dateien aktualisieren

Die Nutzung der Datenbank für ausführbare Dateien durch die Komponente „Programmkontrolle“ wurde in Kaspersky Endpoint Security optimiert. Kaspersky Endpoint Security aktualisiert die Datenbank automatisch, nachdem die Datei vom Computer gelöscht wurde. Dadurch ist die Datenbank immer auf dem neuesten Stand, und die Ressourcen von Kaspersky Security Center werden geschont. Damit die Datenbank der installierten Anwendungen stets aktuell bleibt, muss das Senden von Anwendungsinformationen an den Administrationsserver aktiviert sein (standardmäßig aktiviert).

Inventarisierungseinstellungen

Einstellung	Beschreibung
Inventarisierungsbereiche	Liste der Objekte, die zum Inventarisierungsbereich gehören.
Inventarisierung von DLL-Modulen	Kaspersky Endpoint Security durchsucht den Inventarisierungsbereich nach DLL-Modulen und sendet Informationen an Kaspersky Security Center. Wenn die Inventarisierung von DLL-Modulen aktiviert ist, dauert die Inventarisierungsaufgabe erheblich länger und die Größe der Datenbank steigt.
Inventarisierung von Skriptdateien	Kaspersky Endpoint Security durchsucht den Inventarisierungsbereich nach Skripten und sendet Informationen an Kaspersky Security Center. Wenn die Inventarisierung von Skript-Dateien aktiviert ist, dauert die Inventarisierungsaufgabe erheblich länger und die Größe der Datenbank steigt.
Nur ausführen, wenn der Computer inaktiv ist	Schiebt den Start der Aufgabe auf, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde. Mit dieser Zeitplanoption können Sie die Computerressourcen schonen, während der Computer verwendet wird.
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.
Datei überspringen, wenn Untersuchung länger dauert als (Sek.) n Sek	Ausführungszeit der Aufgabe begrenzen. Nach Ablauf des festgelegten Zeitraums bricht Kaspersky Endpoint Security die Aufgabe ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Endpoint Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.
Archive untersuchen	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Programmpakete untersuchen	Verteilungspakete für Drittanbieter-Programme untersuchen.
Große zusammengesetzte Dateien nicht entpacken	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.

So aktivieren Sie den Modus „Blockierte Programme“

Im Modus *Blockierte Programme* erlaubt die Programmkontrolle den Benutzern den Start aller Programme, unter Ausnahme von Programmen, die durch Programmkontrolle-Regeln verboten sind. Das heißt: Wenn keine Verbotsregel vorhanden ist, erlaubt die Programmkontrolle den Start des Programms. Dieser Modus ist für die Programmkontrolle standardmäßig ausgewählt.

Bevor Sie den Modus *Blockierte Programme* aktivieren, sollten Sie die Programmkontrolle-Regeln unbedingt testen. Dazu können Sie den Testmodus aktivieren.

So aktivieren Sie den Modus „Blockierte Programme“ (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Programmkontrolle** aus.
5. Aktivieren Sie das Kontrollkästchen **Programmkontrolle**.
6. Verwenden Sie im Block **Einstellungen der Programmkontrolle** die Dropdown-Liste **Kontrollmodus**, um **Deny-Liste** auszuwählen.
7. Wählen Sie aus der Dropdown-Liste **Aktion** die Aktion für die Programmkontrolle aus:
   - **Regeln testen**. Programme, deren Ausführung durch die Regeln verhindert wird, werden durch die Programmkontrolle nicht blockiert. Die Programmkontrolle generiert aber Ereignisse über die Ausführung von Programmen, die andernfalls blockiert würden.
   - **Regeln anwenden**. Die Programmkontrolle sperrt die blockierten Programme und generiert entsprechende Ereignisse.
8. Wählen Sie den Status für die Programmkontrolle-Regeln aus:
   - **Ein**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.
   - **Aus**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.
   - **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, auf welche die Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

Fügen Sie bei Bedarf Regeln für die Programmkontrolle hinzu.

9. Konfigurieren Sie die erweiterten Einstellungen der Programmkontrolle:

   - **Laden von DLL-Modulen überwachen (führt zu erheblich erhöhter Systemauslastung)**. 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.

   - **Strenge Überprüfung für digitale Signaturen verwenden**. 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 Trusted Root Certificate Store von Windows signiert sind. Solche Programme gehören nicht zur vertrauenswürdigen Zone. Die Schutzkomponenten überwachen die Aktivität solcher Programme.

   - **Nachricht beim Blockieren**. 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.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie den Modus „Blockierte Programme" (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.

5. Aktivieren Sie den Schalter **Programmkontrolle AKTIVIERT**.

6. Wählen Sie im Block **Funktionsmodus** die Variante **Alle blockieren, die nicht in der Regelliste angegeben sind** aus.

7. Wählen Sie im Block **Aktion** die Aktion für die Programmkontrolle aus:

   - **Informieren**. Programme, deren Ausführung durch die Regeln verhindert wird, werden durch die Programmkontrolle nicht blockiert. Die Programmkontrolle generiert aber Ereignisse über die Ausführung von Programmen, die andernfalls blockiert würden.

   - **Regeln anwenden**. Die Programmkontrolle sperrt die blockierten Programme und generiert entsprechende Ereignisse.

8. Wählen Sie den Status für die Programmkontrolle-Regeln aus:

   - **Aktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.

   - **Deaktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.

   - **Testmodus**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, auf welche die Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

   Fügen Sie bei Bedarf Regeln für die Programmkontrolle hinzu.

9. Konfigurieren Sie die erweiterten Einstellungen der Programmkontrolle:

   - **Laden von DLL-Modulen überwachen**. 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.

- **Strenge Überprüfung für digitale Signaturen verwenden**. 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 Trusted Root Certificate Store von Windows signiert sind. Solche Programme gehören nicht zur vertrauenswürdigen Zone. Die Schutzkomponenten überwachen die Aktivität solcher Programme.

- **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.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie den Modus „Blockierte Programme“ (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Programmkontrolle** aus.
3. Aktivieren Sie den Schalter **Programmkontrolle**.
4. Wählen Sie im Block **Modus „Kontrolle des Programmstarts“** die Variante **Deny-Liste. Alle Programme sind erlaubt, außer denen in der Regelliste** aus.
5. Wählen Sie im Block **Aktion beim Start von Programmen, die durch Regeln blockiert werden** die Aktion für die Programmkontrolle aus:

   - **Informieren (Testmodus) und Ereignisse protokollieren im Bericht**. Programme, deren Ausführung durch die Regeln verhindert wird, werden durch die Programmkontrolle nicht blockiert. Die Programmkontrolle generiert aber Ereignisse über die Ausführung von Programmen, die andernfalls blockiert würden.

   - **Blockieren**. Die Programmkontrolle sperrt die blockierten Programme und generiert entsprechende Ereignisse.

6. Wählen Sie den Status für die Programmkontrolle-Regeln aus:

   - **Aktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.

   - **Deaktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.

   - **Testmodus**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, auf welche die Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

Fügen Sie bei Bedarf Regeln für die Programmkontrolle hinzu.

7. Konfigurieren Sie die erweiterten Einstellungen der Programmkontrolle:

- **Laden von DLL-Modulen überwachen**. 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.

- **Strenge Überprüfung von digitalen Signaturen verwenden**. 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 Trusted Root Certificate Store von Windows signiert sind. Solche Programme gehören nicht zur vertrauenswürdigen Zone. Die Schutzkomponenten überwachen die Aktivität solcher Programme.

- **Vorlagen für Nachrichten über Programmblockierung**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert.

- **Vorlage für die Nachricht, die beim Blockieren eines Programmstarts erscheint**. Vorlage für die Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn ein Programm nach Meinung des Benutzers irrtümlich blockiert wurde.

8. Speichern Sie die vorgenommenen Änderungen.

Künftig werden verbotene Programme durch die Programmkontrolle blockiert. Außerdem generiert Kaspersky Endpoint Security die Ereignisse *Programmstart verboten*. Anhand dieser Ereignisse können den Bericht *Bericht über verbotene Anwendungen* in der Kaspersky Security Center-Konsole erstellen. In der Zusammenfassung des Berichts finden Sie eine Liste der Programme und Computer, von denen die Programmkontrolle-Regel ausgelöst wurde.

Programmkontrolle auf Basis eines Baseline-Computers

Sie können einen Baseline-Computer verwenden, um ein Image mit einer Auswahl von erforderlichen Programmen zu erstellen. Mit diesem Image können Sie anschließend das Betriebssystem und die Programme auf anderen Computern bereitstellen. Es ist nicht immer möglich, das Image auf dem neuesten Stand zu halten. Mit der Programmkontrolle können Sie eine Liste mit zulässigen Programme verwalten. Als Grundlage gilt ein Baseline-Computer. Die Programmkontrolle ermittelt automatisch, welche Programme auf dem Baseline-Computer installiert sind, und aktualisiert die Kategorie. Auf diese Weise erhalten die Computer eine aktuelle Liste der zulässigen Programme.

Die auf einem Baseline-Computer basierende Konfiguration der Programmkontrolle umfasst folgende Schritte:

1. Eine automatisch aktualisierte Kategorie erstellen. Wenn Sie eine neue Kategorie erstellen, wählen Sie zuerst die Kategorie **Kategorie für ausführbare Dateien aus einem bestimmten Ordner** und dann Ihren Baseline-Computer aus.

   So erstellen Sie eine automatisch aktualisierte Kategorie (in der Verwaltungskonsole (MMC))

   1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
   2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert** → **Programmverwaltung** → **Programmkategorien** aus.
   3. Klicken Sie im Arbeitsbereich auf **Neue Kategorie**.

      Dadurch wird der Assistent für neue Programmkategorien gestartet.
   4. Folgen Sie den Anweisungen des Assistenten für neue Programmkategorien.

Schritt 1. Kategorietyp auswählen

Wählen Sie die Option **Kategorie für ausführbare Dateien von ausgewählten Geräten** als Kategorietyp aus.

Schritt 2. Geben Sie den Namen der Benutzerkategorie ein.

Geben Sie bei diesem Schritt einen Namen für die Programmkategorie an.

Schritt 3. Einstellungen

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Kategorie für ausführbare Dateien der gewählten Geräte** ausgewählt haben.

Klicken Sie bei diesem Schritt auf **Hinzufügen** und geben Sie die Computer an, deren ausführbare Dateien Kaspersky Security Center in die Programmkategorie aufnehmen soll. Kaspersky Security Center fügt der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzu, die sich im Ordner **Ausführbare Dateien** befinden.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Algorithmus zur Berechnung der Hash-Funktion. Um einen Algorithmus auszuwählen, muss mindestens eines der folgenden Kontrollkästchen aktiviert werden:
  - **SHA256 für Dateien in dieser Kategorie berechnen (unterstützt ab Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.
  - **MD5 für Dateien in dieser Kategorie berechnen (unterstützt bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.
- Das Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center die Programmkategorie regelmäßig bereinigt und zu der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzufügt, die sich im Ordner **Ausführbare Dateien** befinden.

  Ist das Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren** deaktiviert ist, so nimmt Kaspersky Security Center nach der Erstellung der Programmkategorie in dieser Kategorie keine Änderungen vor.

Schritt 4. Filter

Konfigurieren Sie bei diesem Schritt einen Filter für Dateien.

Sie können den Dateityp angeben, den Sie zum Erstellen der Programmkategorie verwenden möchten.

- **Alle Dateien**. Die Kategorie umfasst alle Dateien. Dieser Status gilt als Standard.
- **Nur Dateien außerhalb der Programmkategorien**. Die Kategorie umfasst nur Dateien, die nicht zu Programmkategorien gehören.

Sie können Ordner von ausgewählten Computern angeben, die Dateien enthalten, die Sie zum Erstellen der Programmkategorie verwenden möchten.

- **Alle Ordner**. Die Kategorie umfasst alle Ordner. Dieser Status gilt als Standard.
- **Angegebener Ordner**. Die Kategorie umfasst nur den angegebenen Ordner. Bei Auswahl dieser Option müssen Sie einen Ordnerpfad angeben.

Schritt 5. Benutzerkategorie erstellen

Schließen Sie den Assistenten ab.

So erstellen Sie eine Kategorie, zu der automatisch Inhalte hinzugefügt werden (in der Web Console und Cloud Console)

1. Klicken Sie im Web Console-Hauptfenster auf **Vorgänge** → **Drittanbieteranwendungen** → **Programmkategorien**.

   Dadurch wird die Liste der Programmkategorien geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Dadurch wird der Assistent für neue Programmkategorien gestartet.

3. Konfigurieren Sie die allgemeinen Einstellungen der Programmkategorie:

   - Name der Kategorie.
   - Methode zum Erstellen einer Kategorie. Wählen Sie die Option **Kategorie für ausführbare Dateien von ausgewählten Geräten** als Kategorietyp aus.

   Weiter zum nächsten Schritt

4. Konfigurieren Sie die erweiterten Einstellungen der Programmkategorie:

   - Geben Sie die Computer an, von denen Kaspersky Security Center ausführbare Dateien zu der Programmkategorie hinzufügen soll. Kaspersky Security Center fügt der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzu, die sich im Ordner **Ausführbare Dateien** befinden.
   - Wählen Sie einen Algorithmus zur Berechnung der Hash-Funktion aus.
   - Konfigurieren Sie ein Intervall für die Synchronisierung der Daten mit dem Speicher des Administrationsservers.
   - Konfigurieren Sie einen Filter für Dateien.

5. Schließen Sie den Assistenten ab.

Wenn Sie eine automatisch aktualisierte Kategorie erstellen, kann es sinnvoll sein, die Dateien in mehrere Kategorien zu unterteilen. Beispiel: Betriebssystemdateien und Dateien aus dem Ordner Program Files. Dazu können Sie in den Einstellungen der Kategorie einen Filter verwenden und bestimmte Ordner auswählen.

2. Modus der Programmkontrolle auswählen. Sie müssen verhindern, dass Programme ausgeführt werden, die nicht ausdrücklich erlaubt sind. Wählen Sie dazu den Modus *Blockierte Programme* aus.

3. Eine Regel für die Programmkontrolle erstellen. Wählen Sie in den Regeleinstellungen die Kategorie aus, zu der die ausführbaren Dateien des Baseline-Computers gehören.

   So konfigurieren Sie die Programmkontrolle basierend auf einem Baseline-Computer (in der Verwaltungskonsole (MMC))

   1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
   2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
   3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
   4. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Programmkontrolle** aus.

5. Aktivieren Sie das Kontrollkästchen **Programmkontrolle**.

6. Verwenden Sie im Block **Einstellungen der Programmkontrolle** die Dropdown-Liste **Kontrollmodus**, um **Deny-Liste** auszuwählen.

7. Wählen Sie aus der Dropdown-Liste **Aktion** die Aktion für die Programmkontrolle aus:

   - **Regeln testen**. Programme, deren Ausführung durch die Regeln verhindert wird, werden durch die Programmkontrolle nicht blockiert. Die Programmkontrolle generiert aber Ereignisse über die Ausführung von Programmen, die andernfalls blockiert würden.

   - **Regeln anwenden**. Die Programmkontrolle sperrt die blockierten Programme und generiert entsprechende Ereignisse.

8. Klicken Sie in der Liste für die Programmkontrolle-Regeln auf **Hinzufügen**.

   Der Assistent zum Hinzufügen einer Programmkontrolle-Regel wird gestartet.

9. Wählen Sie in der Dropdown-Liste **Kategorie** eine automatisch aktualisierte Kategorie basierend auf dem Baseline-Computer aus.

10. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Programmkontrolle-Regel gelten soll.

11. Konfigurieren Sie die erweiterten Einstellungen der Programmkontrolle-Regel:

    - **Für andere Benutzer verbieten**. Das Programm verhindert den Start von Programmen, die zur ausgewählten Kategorie gehören, für alle Benutzer, die nicht auf der Liste stehen.

    - **Vertrauenswürdige Programme mit Update-Funktionen**. Programme, die zur ausgewählten Kategorie gehören, werden von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet. Solche Programme sind berechtigt, andere ausführbare Dateien zu erstellen, deren Start künftig zugelassen wird.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Programmkontrolle basierend auf einem Baseline-Computer (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.

5. Aktivieren Sie den Schalter **Programmkontrolle AKTIVIERT**.

6. Wählen Sie im Block **Funktionsmodus** die Variante **Alle blockieren, die nicht in der Regelliste angegeben sind** aus.

7. Wählen Sie im Block **Aktion** die Aktion für die Programmkontrolle aus:

   - **Informieren**. Programme, deren Ausführung durch die Regeln verhindert wird, werden durch die Programmkontrolle nicht blockiert. Die Programmkontrolle generiert aber Ereignisse über die Ausführung von Programmen, die andernfalls blockiert würden.

   - **Regeln anwenden**. Die Programmkontrolle sperrt die blockierten Programme und generiert entsprechende Ereignisse.

8. Klicken Sie in der Liste für die Programmkontrolle-Regeln auf **Hinzufügen**.

   Der Assistent zum Hinzufügen einer Programmkontrolle-Regel wird gestartet.

9. Wählen Sie unter **Kategorien/Programme** basierend auf dem Baseline-Computer eine automatisch aktualisierte Kategorie aus.

10. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Programmkontrolle-Regel gelten soll.

11. Konfigurieren Sie die erweiterten Einstellungen der Programmkontrolle-Regel:

    - **Benutzer**. Das Programm verhindert den Start von Programmen, die zur ausgewählten Kategorie gehören, für alle Benutzer, die nicht auf der Liste stehen.

    - **Vertrauenswürdige Programme mit Update-Funktionen**. Programme, die zur ausgewählten Kategorie gehören, werden von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet. Solche Programme sind berechtigt, andere ausführbare Dateien zu erstellen, deren Start künftig zugelassen wird.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Programmkontrolle basierend auf einem Baseline-Computer (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Programmkontrolle** aus.

3. Aktivieren Sie den Schalter **Programmkontrolle**.

4. Wählen Sie im Block **Modus „Kontrolle des Programmstarts“** die Variante **Deny-Liste. Alle Programme sind erlaubt, außer denen in der Regelliste** aus.

5. Wählen Sie im Block **Aktion beim Start von Programmen, die durch Regeln blockiert werden** die Aktion für die Programmkontrolle aus:

   - **Informieren (Testmodus) und Ereignisse protokollieren im Bericht**. Programme, deren Ausführung durch die Regeln verhindert wird, werden durch die Programmkontrolle nicht blockiert. Die Programmkontrolle generiert aber Ereignisse über die Ausführung von Programmen, die andernfalls blockiert würden.

   - **Blockieren**. Die Programmkontrolle sperrt die blockierten Programme und generiert entsprechende Ereignisse.

6. Klicken Sie in der Liste für die Programmkontrolle-Regeln auf **Hinzufügen**.

   Der Assistent zum Hinzufügen einer Programmkontrolle-Regel wird gestartet.

7. Wählen Sie unter **Kategorie** basierend auf dem Baseline-Computer eine automatisch aktualisierte Kategorie aus.

8. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Programmkontrolle-Regel gelten soll.

9. Konfigurieren Sie die erweiterten Einstellungen der Programmkontrolle-Regel:

   - **Für andere Benutzer verbieten**. Das Programm verhindert den Start von Programmen, die zur ausgewählten Kategorie gehören, für alle Benutzer, die nicht auf der Liste stehen.

   - **Vertrauenswürdige Programme mit Update-Funktionen**. Programme, die zur ausgewählten Kategorie gehören, werden von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet. Solche Programme sind berechtigt, andere ausführbare Dateien zu erstellen, deren Start künftig zugelassen wird.

10. Speichern Sie die vorgenommenen Änderungen.

Regeln der Programmkontrolle verwalten

Kaspersky Endpoint Security steuert den Start von Anwendungen durch Benutzer anhand von Regeln. Eine Regel der Programmkontrolle enthält Auslösebedingungen und legt die Aktionen fest, die von der Programmkontrolle beim Auslösen der Regel ausgeführt werden (Erlaubnis oder Verbot des Programmstarts durch Benutzer).

Auslösebedingungen für eine Regel

Eine regelauslösende Bedingung hat folgenden Zusammenhang: „Art der Bedingung – Bedingungskriterium – Bedingungswert“. Basierend auf den Auslösebedingungen für eine Regel wendet Kaspersky Endpoint Security die Regel auf ein Programm an (oder wendet die Regel nicht an).

Die folgenden Arten von Bedingungen werden in Regeln verwendet:

- *Einschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel auf ein Programm an, wenn das Programm mindestens eine einschließende Bedingung erfüllt.

- *Ausschließende Bedingungen*. Kaspersky Endpoint Security wendet die Regel nicht auf ein Programm an, wenn das Programm mindestens eine ausschließende Bedingung oder keine einschließende Bedingung erfüllt.

Auslösebedingungen für eine Regel werden mithilfe von Kriterien definiert. Um in Kaspersky Endpoint Security Bedingungen zu erstellen, werden folgende Kriterien verwendet:

- Pfad des Ordners mit der ausführbaren Programmdatei oder Pfad der ausführbaren Programmdatei

- Metadaten: Name der ausführbaren Programmdatei, Version der ausführbaren Programmdatei, Programmname, Programmversion, Programmhersteller

- Hash der ausführbaren Programmdatei

- Zertifikat: Herausgeber, Subjekt, Fingerabdruck

- Zugehörigkeit eines Programms zu einer KL-Kategorie
- Speicherort der ausführbaren Programmdatei auf dem Wechseldatenträger

Für jedes Kriterium, das in einer Bedingung verwendet wird, muss ein Wert angegeben werden. Entsprechen die Parameter eines zu startenden Programms den Werten von Kriterien, die in einer einschließenden Bedingung angegeben sind, so wird die Regel ausgelöst. In diesem Fall führt die Programmkontrolle die Aktion aus, die in der Regel angegeben ist. Entsprechen die Programmparameter den Werten von Kriterien, die in einer ausschließenden Bedingung angegeben sind, so überwacht die Programmkontrolle den Start des Programms nicht.

Wenn Sie ein Zertifikat als Auslösebedingung für eine Regel ausgewählt haben, müssen Sie sicherstellen, dass dieses Zertifikat dem vertrauenswürdigen Systemspeicher auf dem Computer hinzugefügt wurde. Überprüfen Sie auch die Einstellungen für die Nutzung des vertrauenswürdigen Systemspeichers in der Anwendung.

Entscheidungen der Komponente „Programmkontrolle“ beim Auslösen einer Regel

Wenn eine Regel ausgelöst wird, verfährt die Programmkontrolle nach der Regel und erlaubt oder verbietet den Benutzern (Benutzergruppen) den Programmstart. Sie können konkrete Benutzer oder Benutzergruppen wählen, denen der Start von Programmen, für welche eine Regel ausgelöst wird, erlaubt oder verboten werden soll.

In einer *Verbotsregel* ist kein Benutzer angegeben, dem der Start von Programmen erlaubt ist, welche die Regel erfüllen.

In einer *Erlaubnisregel* ist kein Benutzer angegeben, dem der Start von Programmen verboten ist, welche die Regel erfüllen.

Eine Verbotsregel besitzt eine höhere Priorität als eine Erlaubnisregel. Wenn für eine Benutzergruppe beispielsweise eine Erlaubnisregel der Programmkontrolle festgelegt ist, für einen Benutzer dieser Gruppe aber eine Verbotsregel der Programmkontrolle vorliegt, so wird der Start des Programms für diesen Benutzer verboten.

Status einer Regel

Für die Regeln der Programmkontrolle gibt es folgende Statusvarianten:

- **Aktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.
- **Deaktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.
- **Testmodus**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche die Regel gilt, erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

Auslösebedingung für die Regel der „Programmkontrolle“ hinzufügen

Um das Anlegen von Regeln der Programmkontrolle zu vereinfachen, können Sie Programmkategorien erstellen.

Es wird empfohlen, die Kategorie „Programme für die Arbeit“ zu erstellen und eine Standardauswahl von Programmen in diese Kategorie aufzunehmen, die im Unternehmen eingesetzt werden. Falls bestimmte Benutzergruppen unterschiedliche Programmsets einsetzen, können Sie für jede Benutzergruppe eine separate Programmkategorie erstellen.

Um über die Verwaltungskonsole eine Programmkategorie zu erstellen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert** → **Programmverwaltung** → **Programmkategorien** aus.
3. Klicken Sie im Arbeitsbereich auf **Neue Kategorie**.

   Der Assistent zum Erstellen einer benutzerdefinierten Kategorie wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer neuen Kategorie.

Schritt 1. Kategorietyp auswählen

Wählen Sie bei diesem Schritt einen der folgenden Typen für die Programmkategorien aus:

- Manuell zu erweiternde Kategorie. Informationen über ausführbare Dateien werden zur Kategorie manuell hinzugefügt – Wenn Sie diese Art von Kategorie ausgewählt haben, können Sie bei den Schritten *Bedingungen für die Aufnahme von Anwendungen in Programmkategorien festlegen* und *Bedingungen für den Ausschluss von Anwendungen aus Programmkategorien festlegen* die Kriterien festlegen, nach denen ausführbare Dateien in die Kategorie aufgenommen werden sollen.
- Kategorie für ausführbare Dateien von ausgewählten Geräten. Diese ausführbaren Dateien werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt – Wenn Sie diese Art von Kategorie ausgewählt haben, können Sie beim Schritt *Einstellungen* einen Computer angeben, dessen ausführbare Dateien automatisch in diese Kategorie aufgenommen werden sollen.
- Kategorie für ausführbare Dateien aus einem bestimmten Ordner. Ausführbare Dateien von Anwendungen, die sich in dem angegebenen Ordner befinden, werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt – Wenn Sie diese Art von Kategorie ausgewählt haben, können Sie beim Schritt *Ordner der Datenverwaltung* einen Ordner angeben, aus dem ausführbare Dateien automatisch in die Kategorie aufgenommen werden sollen.

Wenn eine automatisch zu erweiternde Kategorie erstellt wird, führt Kaspersky Security Center die Inventarisierung für Dateien der folgenden Formate aus: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, SCR.

Schritt 2. Geben Sie den Namen der Benutzerkategorie ein.

Geben Sie bei diesem Schritt einen Namen für die Programmkategorie an.

Schritt 3. Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest.

Wenn Sie den Programmkontrolle-Regeln eine große Anzahl von Bedingungen hinzufügen (z. B. Datei-Hashes), steigt der Ressourcenverbrauch des Computers an. Ab einer Gesamtzahl von 50.000 Bedingungen können Leistungsprobleme auftreten. Zur Leistungsoptimierung wird empfohlen, die Anzahl der Bedingungen zu überprüfen und zu reduzieren.

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Manuell zu erweiternde Kategorie** ausgewählt haben.

Wählen Sie bei diesem Schritt in der Dropdown-Liste **Hinzufügen** die Bedingungen aus, nach denen Programme in diese Kategorie aufgenommen werden sollen:

- **Aus der Liste ausführbarer Dateien**. Fügen Sie Programme aus der Liste für ausführbare Dateien auf dem Client-Gerät zu der benutzerdefinierten Kategorie hinzu.
- **Aus den Dateieigenschaften**. Geben Sie präzise Daten für die ausführbaren Dateien an. Diese Daten dienen als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie.
- **Metadaten der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Metadaten dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Prüfsummen der Dateien in dem Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Hash-Werte dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Zertifikate für die Dateien aus dem Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien, die mit Zertifikaten signiert sind, enthält. Kaspersky Security Center gibt die Zertifikate dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

  Es wird davon abgeraten, Bedingungen zu verwenden, in denen der Parameter **Fingerabdruck eines Zertifikats** nicht angegeben ist.

- **Metadaten der Dateien des msi-Installers**. Wählen Sie ein MSI-Paket aus. Die Metadaten der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.
- **Prüfsummen der Dateien des msi-Installers für das Programm**. Wählen Sie ein MSI-Paket aus. Die Hashs der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.
- **Aus der KL-Kategorie**. Geben Sie eine KL-Kategorie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie *Office-Anwendungen* gehören beispielsweise Programme aus der Microsoft Office-Suite, Adobe Acrobat und andere.

  Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Pfad des Programms festlegen (Masken unterstützt)**. Wählen Sie einen Ordner auf dem Client-Gerät aus. Kaspersky Security Center nimmt die ausführbaren Dateien aus diesem Ordner in die benutzerdefinierte Kategorie auf.
- **Zertifikat aus Datenverwaltung auswählen**. Wählen Sie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie die Zertifikate aus, mit denen die ausführbaren Dateien signiert sind.

  Es wird davon abgeraten, Bedingungen zu verwenden, in denen der Parameter **Fingerabdruck eines Zertifikats** nicht angegeben ist.

  Sie können den Zertifikatspeicher auswählen. Die Programmkontrolle wenden Regeln standardmäßig nur für Programme an, die mit einem Zertifikat aus dem vertrauenswürdigen Zertifikatspeicher des Systems signiert sind. Diese Option wird durch das Kontrollkästchen **Strenge Überprüfung für digitale Signaturen verwenden** aktiviert.
- **Datenträgertyp**. Geben Sie den Typ des Massenspeichergerätes (alle Festplatten und Wechseldatenträger oder nur Wechseldatenträger) als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie an.

Schritt 4. Legen Sie die Bedingungen für den Ausschluss der Programme aus der Kategorie fest.

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Manuell zu erweiternde Kategorie** ausgewählt haben.

Die Programme, die bei diesem Schritt angegeben werden, werden auch dann aus der Kategorie ausgeschlossen, wenn diese Programme beim Schritt „Legen Sie die Bedingungen für die Aufnahme der Programme in die Kategorie fest“ angegeben wurden.

Wählen Sie bei diesem Schritt in der Dropdown-Liste **Hinzufügen** die Bedingungen aus, nach denen Programme aus dieser Kategorie ausgeschlossen werden sollen:

- **Aus der Liste ausführbarer Dateien**. Fügen Sie Programme aus der Liste für ausführbare Dateien auf dem Client-Gerät zu der benutzerdefinierten Kategorie hinzu.
- **Aus den Dateieigenschaften**. Geben Sie präzise Daten für die ausführbaren Dateien an. Diese Daten dienen als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie.
- **Metadaten der Dateien im angegebenen Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Metadaten dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Prüfsummen der Dateien in dem Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien enthält. Kaspersky Security Center gibt die Hash-Werte dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.
- **Zertifikate für die Dateien aus dem Ordner**. Wählen Sie einen Ordner auf dem Client-Gerät aus, welcher ausführbare Dateien, die mit Zertifikaten signiert sind, enthält. Kaspersky Security Center gibt die Zertifikate dieser ausführbaren Dateien als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an.

- **Metadaten der Dateien des msi-Installers**. Wählen Sie ein MSI-Paket aus. Die Metadaten der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.

- **Prüfsummen der Dateien des msi-Installers für das Programm**. Wählen Sie ein MSI-Paket aus. Die Hashs der ausführbaren Dateien, die sich in diesem MSI-Paket befinden, werden von Kaspersky Security Center als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie angegeben.

- **Aus der KL-Kategorie**. Geben Sie eine KL-Kategorie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie an. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie *Office-Anwendungen* gehören beispielsweise Programme aus der Microsoft Office-Suite, Adobe Acrobat und andere.

  Sie können alle KL-Kategorien auswählen, um eine erweiterte Liste mit vertrauenswürdigen Programme zu erstellen.

- **Pfad des Programms festlegen (Masken unterstützt)**. Wählen Sie einen Ordner auf dem Client-Gerät aus. Kaspersky Security Center nimmt die ausführbaren Dateien aus diesem Ordner in die benutzerdefinierte Kategorie auf.

- **Zertifikat aus Datenverwaltung auswählen**. Wählen Sie als Bedingung für das Hinzufügen von Programmen zu der benutzerdefinierten Kategorie die Zertifikate aus, mit denen die ausführbaren Dateien signiert sind.

- **Datenträgertyp**. Geben Sie den Typ des Massenspeichergerätes (alle Festplatten und Wechseldatenträger oder nur Wechseldatenträger) als Bedingung für die Aufnahme von Programmen in die benutzerdefinierte Kategorie an.

Schritt 5. Einstellungen

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Kategorie für ausführbare Dateien der gewählten Geräte** ausgewählt haben.

Klicken Sie bei diesem Schritt auf **Hinzufügen** und geben Sie die Computer an, deren ausführbare Dateien Kaspersky Security Center in die Programmkategorie aufnehmen soll. Kaspersky Security Center fügt der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzu, die sich im Ordner **Ausführbare Dateien** befinden.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Algorithmus zur Berechnung der Hash-Funktion. Um einen Algorithmus auszuwählen, muss mindestens eines der folgenden Kontrollkästchen aktiviert werden:

  - **SHA256 für Dateien in dieser Kategorie berechnen (unterstützt ab Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

  - **MD5 für Dateien in dieser Kategorie berechnen (unterstützt bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

- Das Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center die Programmkategorie regelmäßig bereinigt und zu der Programmkategorie alle ausführbaren Dateien von den angegebenen Computern hinzufügt, die sich im Ordner **Ausführbare Dateien** befinden.

  Ist das Kontrollkästchen **Daten mit der Datenverwaltung des Administrationsservers synchronisieren** deaktiviert ist, so nimmt Kaspersky Security Center nach der Erstellung der Programmkategorie in dieser Kategorie keine Änderungen vor.

Schritt 6. Ordner der Datenverwaltung

Dieser Schritt ist verfügbar, wenn Sie den Kategorietyp **Kategorie für ausführbare Dateien aus dem angegebenen Ordner** ausgewählt haben.

Geben Sie bei diesem Schritt den Ordner an, den Kaspersky Security Center nach ausführbaren Dateien durchsuchen soll, um diese automatisch zu der Programmkategorie hinzuzufügen.

Bei diesem Schritt können Sie außerdem die folgenden Einstellungen anpassen:

- Das Kontrollkästchen **Dynamic Link Libraries (.dll) in diese Kategorie aufnehmen**. Aktivieren Sie das Kontrollkästchen, damit dynamische Programmbibliotheken (Dateien mit dem Format DLL) in die Programmkategorie aufgenommen werden.

  Wenn Dateien im DLL-Format in die Programmkategorie aufgenommen werden, kann sich die Leistungsfähigkeit von Kaspersky Security Center vermindern.

- Das Kontrollkästchen **Skriptdateien in diese Kategorie aufnehmen**. Aktivieren Sie das Kontrollkästchen, damit Skripte in die Programmkategorie aufgenommen werden.

  Wenn Skripte in die Programmkategorie aufgenommen werden, kann die Leistungsfähigkeit von Kaspersky Security Center sinken.

- Algorithmus zur Berechnung der Hash-Funktion. Um einen Algorithmus auszuwählen, muss mindestens eines der folgenden Kontrollkästchen aktiviert werden:

  - **SHA256 für Dateien in dieser Kategorie berechnen (unterstützt ab Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

  - **MD5 für Dateien in dieser Kategorie berechnen (unterstützt bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**.

- Das Kontrollkästchen **Untersuchung des Ordners auf Änderungen erzwingen**. Aktivieren Sie dieses Kontrollkästchen, damit Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, regelmäßig nach ausführbaren Dateien durchsucht.

  Ist das Kontrollkästchen **Untersuchung des Ordners auf Änderungen erzwingen** deaktiviert, durchsucht Kaspersky Security Center den Ordner, aus dem Programme automatisch zu der Programmkategorie hinzugefügt werden, nur dann, wenn der Ordner geändert wurde, ihm Dateien hinzugefügt oder Dateien daraus gelöscht wurden.

- Das Feld **Untersuchungsintervall (1–168 Stunden)**. In diesem Feld können Sie angeben, nach welchem Zeitraum (in Stunden) Kaspersky Security Center den Ordner, der zur automatischen Ergänzung der Programmkategorie dient, durchsuchen soll.

  Das Feld ist verfügbar, wenn das Kontrollkästchen **Untersuchung des Ordners auf Änderungen erzwingen** aktiviert ist.

Schritt 7. Benutzerkategorie erstellen

Schließen Sie den Assistenten ab.

Um über die Programmoberfläche eine neue Auslösebedingung für eine Regel der „Programmkontrolle“ hinzuzufügen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Programmkontrolle** aus.
3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.
4. Wählen Sie die Regel aus, für die Sie eine Auslösebedingung konfigurieren möchten.

   Die Eigenschaften für die Regel der Programmkontrolle werden geöffnet.
5. Wählen Sie die Registerkarte **Bedingungen: N** oder **Ausnahmen: N** aus und klicken Sie auf **Hinzufügen**.
6. Wählen Sie die Auslösebedingungen für die Regel der Programmkontrolle:

   - **Bedingungen aus den Eigenschaften der gestarteten Programme**. In der Liste der laufenden Programme können Sie die Programme auswählen, auf die die Regel der Programmkontrolle angewendet wird. Kaspersky Endpoint Security listet auch Programme auf, die zuvor auf dem Computer ausgeführt wurden. Sie müssen das Kriterium auswählen, das Sie zum Erstellen einer oder mehrerer Regel-Auslösebedingungen verwenden möchten: **Datei-Hash**, **Zertifikat**, **KL-Kategorie**, **Metadaten** oder **Datei- oder Ordnerpfad**.
   - **Bedingungen „KL-Kategorie”**. Eine *KL-Kategorie* ist eine Liste von Programmen, die gemeinsame Themenattribute haben. Die Liste wird von Kaspersky-Experten geführt. Zur KL-Kategorie „Office-Programme“ gehören beispielsweise Programme aus den Paketen Microsoft Office, Adobe® Acrobat® und anderen.
   - **Benutzerdefinierte Bedingung**. Sie können die Programmdatei und eine der Regel-Auslösebedingungen auswählen: **Datei-Hash**, **Zertifikat**, **Metadaten** oder **Datei- oder Ordnerpfad**.
   - **Bedingung nach Dateilaufwerk (Wechseldatenträger)**. Die Regel der Programmkontrolle wird nur auf Dateien angewendet, die auf einem Wechseldatenträger ausgeführt werden.
   - **Bedingungen aus den Dateieigenschaften des angegebenen Ordners**. Die Regel der „Programmkontrolle“ wird nur auf Dateien in dem angegebenen Ordner angewendet. Sie können auch Dateien aus Unterordnern einschließen oder ausschließen. Sie müssen das Kriterium auswählen, das Sie zum Erstellen einer oder mehrerer Regel-Auslösebedingungen verwenden möchten: **Datei-Hash**, **Zertifikat**, **KL-Kategorie**, **Metadaten** oder **Datei- oder Ordnerpfad**.
7. Speichern Sie die vorgenommenen Änderungen.

Bitte beachten Sie beim Hinzufügen von Bedingungen die folgenden besonderen Überlegungen zur Programmkontrolle:

- Kaspersky Endpoint Security unterstützt `*` und `?` Zeichen für die Eingabe einer Maske in den Metadaten: **Dateiname**, **Anwendungsname**, **Anbieter**.
- Kaspersky Endpoint Security unterstützt den MD5-Dateihash nicht und kontrolliert den Start von Programmen nicht auf Basis des MD5-Hashs. Als Auslösebedingung für eine Regel wird der SHA256-Hash verwendet.
- Es wird davor gewarnt, als Auslösebedingungen für Regeln nur die Kriterien **Aussteller** und **Subjekt des Zertifikats** zu verwenden. Die Verwendung dieser Kriterien ist unzuverlässig.
- Wenn Sie im Feld **Datei- oder Ordnerpfad** einen symbolischen Link verwenden, wird empfohlen, den symbolischen Link aufzulösen, damit die Regel der Programmkontrolle korrekt funktioniert. Klicken Sie dazu auf **Symbolischen Link auflösen**.

Ausführbare Dateien aus dem Ordner „Ausführbare Dateien“ zu einer Programmkategorie hinzufügen

Der Ordner **Ausführbare Dateien** enthält eine Liste der ausführbaren Dateien, die auf Computern gefunden wurden. Kaspersky Endpoint Security erstellt die Liste der ausführbaren Dateien nach der Ausführung der Inventarisierungsaufgabe.

So fügen Sie ausführbare Dateien aus dem Ordner Ausführbare Dateien zu der Programmkategorie hinzu:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur **Erweitert** → **Programmverwaltung** → **Ausführbare Dateien**. aus.
3. Wählen Sie im Arbeitsbereich die ausführbaren Dateien aus, die Sie zu der Programmkategorie hinzufügen möchten.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für die ausgewählten ausführbaren Dateien und wählen Sie den Punkt **Zur Kategorie hinzufügen** aus.
5. Gehen Sie im angezeigten Fenster wie folgt vor:
   - Wählen Sie im oberen Fensterbereich eine der folgenden Varianten aus:
     - **Zu neuer Programmkategorie hinzufügen**. Wählen Sie diese Variante aus, wenn Sie eine neue Programmkategorie erstellen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.
     - **Zu bestehender Programmkategorie hinzufügen**. Wählen Sie diese Variante aus, wenn Sie eine vorhandene Programmkategorie auswählen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.

- Wählen Sie im Block **Regeltyp** eine der folgenden Optionen aus:
  - **Regeln zum Hinzufügen zu den Einschlüssen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien zu einer Programmkategorie hinzugefügt werden.
  - **Regeln zum Hinzufügen zu den Ausschlüssen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien aus einer Programmkategorie ausgeschlossen werden.
- Wählen Sie im Block **Als Bedingung verwendete Parameter** eine der folgenden Optionen aus:
  - **Zertifikatinformationen (oder SHA256-Hashes für Dateien ohne Zertifikat)**.
  - **Zertifikatdetails (Dateien ohne Zertifikat werden übersprungen)**.
  - **Nur SHA256 (Dateien ohne Hash werden übersprungen)**.
  - **Nur MD5 (Modus eingestellt. Nur für Version Kaspersky Endpoint Security 10 Service Pack 1)**.

6. Speichern Sie die vorgenommenen Änderungen.

Ausführbare Dateien, die mit Ereignissen zusammenhängen, zu einer Programmkategorie hinzufügen

Um ausführbare Dateien, die mit Ereignissen der „Programmkontrolle" zusammenhängen, zu einer Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse** aus.
3. Wählen Sie in der Dropdown-Liste **Ereignisauswahlen** eine Auswahl von Ereignissen über die Verwendung der Komponente „Programmkontrolle" aus (Ereignisse aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle" anzeigen, Ereignisse aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle" anzeigen).
4. Klicken Sie auf **Auswahl starten**.
5. Wählen Sie die Ereignisse aus, für welche ausführbare Dateien zu der Programmkategorie hinzugefügt werden sollen.
6. Öffnen Sie durch Rechtsklick das Kontextmenü für die ausgewählten Ereignisse und wählen Sie den Punkt **Zur Kategorie hinzufügen** aus.

7. Konfigurieren Sie im angezeigten Fenster die Einstellungen der Programmkategorie:

   - Wählen Sie im oberen Fensterbereich eine der folgenden Varianten aus:

     - **Zu neuer Programmkategorie hinzufügen**. Wählen Sie diese Variante aus, wenn Sie eine neue Programmkategorie erstellen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.

     - **Zu bestehender Programmkategorie hinzufügen**. Wählen Sie diese Variante aus, wenn Sie eine vorhandene Programmkategorie auswählen und ausführbare Dateien zu dieser Kategorie hinzufügen möchten.

   - Wählen Sie im Block **Regeltyp** eine der folgenden Optionen aus:

     - **Regeln zum Hinzufügen zu den Einschlüssen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien zu einer Programmkategorie hinzugefügt werden.

     - **Regeln zum Hinzufügen zu den Ausschlüssen**. Wählen Sie diese Variante aus, wenn Sie Bedingungen festlegen möchten, nach denen ausführbare Dateien aus einer Programmkategorie ausgeschlossen werden.

   - Wählen Sie im Block **Als Bedingung verwendete Parameter** eine der folgenden Optionen aus:

     - **Zertifikatdetails (oder SHA-256-Hashs für Dateien ohne ein Zertifikat)**.

     - **Zertifikatdetails (Dateien ohne ein Zertifikat werden übersprungen)**

     - **Nur SHA-256 (Dateien ohne Hash werden übersprungen)**

     - **Nur MD5 (Modus eingestellt; Nur für Version Kaspersky Endpoint Security 10 Service Pack 1)**.

8. Speichern Sie die vorgenommenen Änderungen.

Regel der Programmkontrolle hinzufügen

Um über Kaspersky Security Center eine Regel für die „Programmkontrolle" hinzuzufügen:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Programmkontrolle" angezeigt.

4. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Regel der Programmkontrolle** wird geöffnet.

5. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine neue Kategorie erstellen möchten, gehen Sie wie folgt vor:

     a. Klicken Sie auf **Kategorie erstellen**.

        Der Assistent zum Erstellen einer benutzerdefinierten Kategorie wird gestartet.

b. Folgen Sie den Anweisungen des Assistenten zum Erstellen einer neuen Kategorie.

c. Wählen Sie aus der Dropdown-Liste **Kategorie** die erstellte Programmkategorie aus.

- Wenn Sie eine vorhandene Kategorie ändern möchten, gehen Sie wie folgt vor:

  a. Wählen Sie in der Dropdown-Liste **Kategorie** die erstellte Programmkategorie aus, die Sie ändern möchten.

  b. Klicken Sie auf **Eigenschaften**.

  c. Ändern Sie die Einstellungen der ausgewählten Programmkategorie.

  d. Speichern Sie die vorgenommenen Änderungen.

  e. Wählen Sie in der Dropdown-Liste **Kategorie** die erstellte Programmkategorie aus, auf deren Basis Sie eine Regel erstellen möchten.

6. Klicken Sie in der Tabelle **Benutzer und deren Rechte** auf die Schaltfläche **Hinzufügen**.

   Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

7. Gehen Sie in der Tabelle **Benutzer und deren Rechte** wie folgt vor:

   - Um Benutzern und/oder Benutzergruppen den Start von Programmen, die zur ausgewählten Kategorie gehören, zu erlauben, aktivieren Sie das Kontrollkästchen **Erlauben** in den entsprechenden Zeilen.
   - Um Benutzern und/oder Benutzergruppen den Start von Programmen, die zur ausgewählten Kategorie gehören, zu verbieten, aktivieren Sie das Kontrollkästchen **Blockieren** in den entsprechenden Zeilen.

8. Aktivieren Sie das Kontrollkästchen **Für andere Benutzer verbieten**, damit das Programm den Start von Programmen aus der gewählten Kategorie für alle Benutzer verbietet, die nicht in der Spalte **Benutzer oder Gruppe** angegeben sind und die nicht zu den in der Spalte **Benutzer oder Gruppe** angegebenen Benutzergruppen gehören.

9. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Programme, welche zu der ausgewählten Programmkategorie gehören, von Kaspersky Endpoint Security als vertrauenswürdige Programme mit Update-Funktionen betrachtet werden, die berechtigt sind, andere ausführbare Dateien, deren Start künftig zugelassen wird, zu erstellen.

   Bei der Migration von Einstellungen migriert Kaspersky Endpoint Security auch eine Liste mit ausführbaren Dateien, die von vertrauenswürdigen Programmen mit Update-Funktionen erstellt worden sind.

10. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine Regel der Programmkontrolle hinzu:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Programmkontrolle** aus.

3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.

4. Klicken Sie auf **Hinzufügen**.

   Dadurch wird das Fenster „Regeln der Programmkontrolle“ geöffnet.

5. Definieren Sie auf der Registerkarte **Allgemeine Einstellungen** die Haupteinstellungen der Regel:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Regel ein.

   c. Klicken Sie in der Tabelle **Benutzer und deren Rechte** auf die Schaltfläche **Hinzufügen**.

      Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.

      Die Regel gilt standardmäßig für alle Benutzer.

      > Ist in der Tabelle kein Benutzer angegeben, so kann die Regel nicht gespeichert werden.

   d. Definieren Sie in der Tabelle **Benutzer und deren Rechte** mit dem Schalter die Berechtigung der Benutzer, Programme zu starten.

   e. Aktivieren Sie das Kontrollkästchen **Für andere Benutzer verbieten**, damit die Anwendung verhindert, dass Anwendungen, die die Auslösebedingungen der Regel erfüllen, für alle Benutzer ausgeführt werden, die nicht in der Tabelle **Benutzer und deren Rechte** aufgeführt sind und die nicht zu einer Benutzergruppe gehören, die in der Tabelle **Benutzer und deren Rechte** aufgeführt sind.

      > Ist das Kontrollkästchen **Für andere Benutzer verbieten** deaktiviert, so kontrolliert Kaspersky Endpoint Security den Start von Programmen für jene Benutzer nicht, die nicht in der Tabelle **Benutzer und deren Rechte** angegeben sind und die nicht zu den in der Tabelle **Benutzer und deren Rechte** angegebenen Benutzergruppen gehören.

   f. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Kaspersky Endpoint Security Anwendungen, die den Auslösebedingungen der Regel entsprechen, als vertrauenswürdige Programme mit Update-Funktionen betrachtet. *Vertrauenswürdige Programme mit Update-Funktionen* sind Anwendungen, die berechtigt sind, andere ausführbare Dateien zu erstellen, die anschließend ausgeführt werden können.

      Löst eine App mehrere Regeln aus, so setzt Kaspersky Endpoint Security unter den folgenden Voraussetzungen das Kennzeichen *Vertrauenswürdige Programme mit Update-Funktionen*:

      - Alle Regeln erlauben die Ausführung der Anwendung.
      - Das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen** ist mindestens für eine Regel aktiviert.

6. Erstellen oder bearbeiten Sie auf der Registerkarte **Bedingungen: N** die Liste der einschließenden Auslösebedingungen für die Regel.

7. Erstellen oder bearbeiten Sie auf der Registerkarte **Ausnahmen: N** die Liste der Ausschlussbedingungen für das Auslösen der Regel.

   Bei der Migration von Einstellungen migriert Kaspersky Endpoint Security auch eine Liste mit ausführbaren Dateien, die von vertrauenswürdigen Programmen mit Update-Funktionen erstellt worden sind.

8. Speichern Sie die vorgenommenen Änderungen.

Ändern des Status einer Regel der Programmkontrolle mithilfe von Kaspersky Security Center

Um den Status einer Regel der „Programmkontrolle“ in der Verwaltungskonsole zu ändern:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Programmkontrolle“ angezeigt.
4. Öffnen Sie in der Spalte **Status** durch Linksklick das Kontextmenü und wählen Sie einen der folgenden Punkte aus:

   - **Ein**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.
   - **Aus**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.
   - **Test**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, auf welche die Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.
5. Speichern Sie die vorgenommenen Änderungen.

So ändern Sie den Status einer Regel der „Programmkontrolle“ über die Benutzeroberfläche:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Programmkontrolle** aus.
3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

   Dies öffnet die Liste der Regeln für die Programmkontrolle.
4. Öffnen Sie in der Spalte **Status** das Kontextmenü und wählen Sie einen der folgenden Punkte aus:

   - **Aktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ verwendet wird.
   - **Deaktiviert**. Dieser Status bedeutet, dass die Regel von der Komponente „Programmkontrolle“ ignoriert wird.
   - **Testmodus**. Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche diese Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.
5. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Regeln der Programmkontrolle

Sie können die Liste der Regeln der Programmkontrolle in eine XML-Datei exportieren. Mit der Export-/Importfunktion können Sie ein Backup für die Liste mit den Regeln der Programmkontrolle anlegen oder die Liste auf einen anderen Server migrieren.

Wenn Sie Regeln der „Programmkontrolle“ exportieren und importieren, beachten Sie bitte die folgenden Sonderbedingungen:

- Kaspersky Endpoint Security exportiert die Regelliste nur für den momentan aktiven „Programmkontrolle“-Modus. Das bedeutet, wenn die „Programmkontrolle“ im Deny-Liste-Modus läuft, exportiert Kaspersky Endpoint Security nur die Regeln für diesen Modus. Um die Regelliste für den Allow-Liste-Modus zu exportieren, müssen Sie den Modus ändern und den Exportvorgang erneut ausführen.

- Kaspersky Endpoint Security verwendet Programmkategorien für die „Programmkontrolle“. Wenn Sie die Liste der „Programmkontrolle“-Regeln auf einen anderen Server migrieren, müssen Sie auch die Liste der Programmkategorien migrieren. Nähere Informationen über den Export und Import von Programmkategorien finden Sie in der Hilfe zu Kaspersky Security Center.

Exportieren und Importieren einer Liste von Regeln der Programmkontrolle in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

4. So ändern Sie den Status einer Regel der Programmkontrolle:

   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

   Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.

   b. Klicken Sie auf den Link **Exportieren**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.

5. Um eine Liste der Regeln für die „Programmkontrolle“ zu importieren:

   a. Klicken Sie auf den Link **Importieren**.

   Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren einer Liste von Regeln der Programmkontrolle in der Web Console und der Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **App-Kontrolle**.
5. Wählen Sie unter **Funktionsmodus** eine Liste mit Regeln aus: Deny-Liste oder Allow-Liste für Programme.
6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie die Regeln, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

   Kaspersky Endpoint Security exportiert die Liste der Regeln in eine json-Datei im standardmäßigen Download-Ordner.
7. So importieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Klicken Sie auf die Schaltfläche → **Import**.

   Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

Ereignisse aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle“ anzeigen

Um die Ereignisse anzuzeigen, die aus den Ausführungsergebnissen der Komponente „Programmkontrolle“ stammen und in Kaspersky Security Center eintreffen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf **Auswahl erstellen**.
4. Gehen Sie im folgenden Fenster zum Abschnitt **Ereignisse**.
5. Klicken Sie auf **Alle zurücksetzen**.
6. Aktivieren Sie in der Tabelle **Ereignisse** das Kontrollkästchen **Programmstart verboten**.

7. Speichern Sie die vorgenommenen Änderungen.

8. Wählen Sie in der Liste **Ereignisauswahlen** die erstellte Auswahl aus.

9. Klicken Sie auf **Auswahl starten**.

Bericht über verbotene Programme anzeigen

Um einen Bericht über verbotene Programme anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte** aus.

3. Klicken Sie auf **Neue Berichtsvorlage**.

   Der „Assistent für das Erstellen einer Berichtsvorlage“ wird gestartet.

4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** die Variante **Andere → Bericht über verbotene Anwendungen** aus.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Öffnen Sie den Bericht durch Doppelklick.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Regeln der Programmkontrolle testen

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, für neu erstellte Regeln den Test für Regeln der Programmkontrolle zu aktivieren und ihre Funktion zu analysieren. Wenn der Testlauf für die Regel der Programmkontrolle aktiviert ist, werden Programme, für welche der Start durch die Programmkontrolle verboten ist, von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Für die Funktionsanalyse von Regeln der Programmkontrolle müssen die Ereignisse aus den Ausführungsergebnissen der Komponente „Programmkontrolle“ überprüft werden, die bei Kaspersky Security Center eintreffen. Wenn im Testmodus für alle Programme, die der Benutzer zum Arbeiten benötigt, keine Ereignisse über ein Startverbot vorliegen, sind die Regeln korrekt. Andernfalls wird empfohlen, die Einstellungen der von Ihnen erstellten Regeln zu präzisieren, zusätzliche Regeln zu erstellen oder vorhandene Regeln zu löschen.

Kaspersky Endpoint Security erlaubt standardmäßig den Start aller Programme, unter Ausnahme von Programmen, die durch Regeln verboten sind.

Prüfung von Regeln der „Programmkontrolle“ aktivieren und deaktivieren

Um in Kaspersky Security Center den Test für die Regeln der „Programmkontrolle“ zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.

   Im rechten Fensterbereich werden die Einstellungen für die Komponente „Programmkontrolle“ angezeigt.
4. Wählen Sie in der Dropdown-Liste **Kontrollmodus** eines der folgenden Elemente aus:

   - **Deny-Liste**. Bei Auswahl dieser Variante erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Anwendungen. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Verbotsregeln der Programmkontrolle erfüllt sind.
   - **Allow-Liste**. Bei Auswahl dieser Variante verbietet die Programmkontrolle allen Benutzern den Start beliebiger Anwendungen. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Erlaubnisregeln der Programmkontrolle erfüllt sind.
5. Führen Sie eine der folgenden Aktionen aus:

   - Um den Test für die Regeln der „Programmkontrolle“ zu aktivieren, wählen Sie in der Dropdown-Liste **Aktion** das Element **Regeln testen** aus.
   - Wenn Sie die „Programmkontrolle“ aktivieren möchten, um den Start von Anwendungen auf Benutzercomputern zu verwalten, wählen Sie in der Dropdown-Liste den Punkt **Regeln anwenden**.
6. Speichern Sie die vorgenommenen Änderungen.

Um den Test für die Regeln der Programmkontrolle zu aktivieren oder um eine Sperraktion der Programmkontrolle auszuwählen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Programmkontrolle** aus.
3. Klicken Sie auf die Schaltfläche **Blockierte Programme** oder **Erlaubte Programme**.

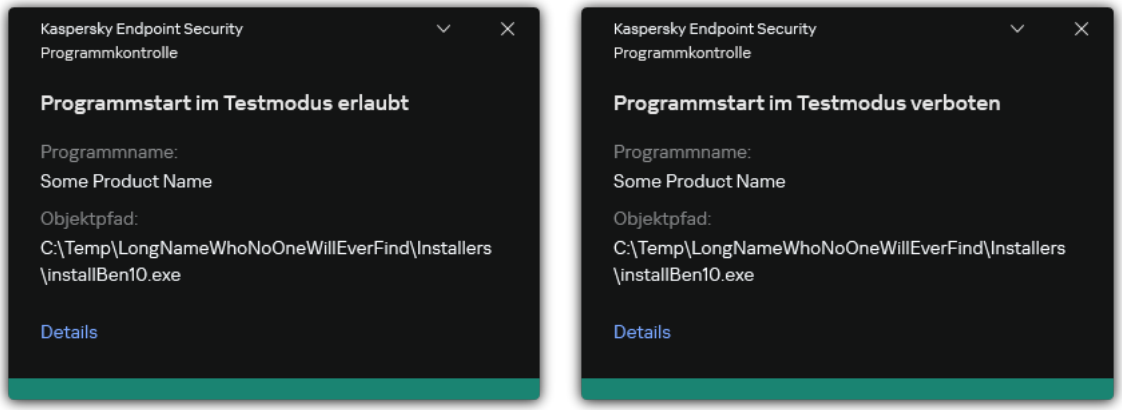
   Dies öffnet die Liste der Regeln für die Programmkontrolle.

4. Wählen Sie in der Spalte **Status** die Option **Testmodus**.

   Dieser Status bedeutet, dass Kaspersky Endpoint Security den Start der Programme, für welche diese Regel gilt, immer erlaubt. Gleichzeitig werden aber Informationen über den Start dieser Programme protokolliert.

5. Speichern Sie die vorgenommenen Änderungen.

Programme, für welche die Komponente „Programmkontrolle“ den Start verbietet, werden von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet. Sie können auch die Anzeige von Benachrichtigungen über das Testen von Regeln auf dem Benutzercomputer konfigurieren (siehe folgende Abbildung).



Benachrichtigungen der „Programmkontrolle“ im Testmodus

Bericht über im Testmodus verbotene Programme anzeigen

Um einen Bericht über im Testmodus verbotene Programme anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte** aus.

3. Klicken Sie auf **Neue Berichtsvorlage**.

   Der „Assistent für das Erstellen einer Berichtsvorlage“ wird gestartet.

4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** die Option **Andere → Bericht über verbotene Anwendungen im Testmodus** aus.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Öffnen Sie den Bericht durch Doppelklick.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Ereignisse aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle“ anzeigen

Um die Ereignisse anzuzeigen, die als Ergebnisse des Testlaufs der Komponente „Programmkontrolle“ in Kaspersky Security Center eintreffen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse** aus.
3. Klicken Sie auf **Auswahl erstellen**.
4. Gehen Sie im folgenden Fenster zum Abschnitt **Ereignisse**.
5. Klicken Sie auf **Alle zurücksetzen**.
6. Aktivieren Sie in der Tabelle **Ereignisse** die Kontrollkästchen **Programmstart im Testmodus verboten** und **Programmstart im Testmodus erlaubt**.
7. Speichern Sie die vorgenommenen Änderungen.
8. Wählen Sie in der Liste **Ereignisauswahlen** die erstellte Auswahl aus.
9. Klicken Sie auf **Auswahl starten**.

Aktivitätsmonitor für Programme

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Der *Aktivitätsmonitor für Programme* dient dazu, in Echtzeit Informationen über die Aktivität von Programmen auf einem Benutzercomputer anzuzeigen.

Die Verwendung des „Aktivitätsmonitors für Programme“ erfordert die Installation der Komponenten „Programmkontrolle“ und „Programm-Überwachung“. Wenn diese Komponenten nicht installiert sind, ist der Abschnitt „Aktivitätsmonitor für Programme“ im Programmhauptfenster ausgeblendet.

Um den „Aktivitätsmonitor für Programme“ zu starten:

Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Aktivitätsmonitor für Programme**.

Dieses Fenster enthält auf drei Registerkarten mit Informationen über die Aktivität von Programmen auf dem Benutzercomputer:

- Die Registerkarte **Alle Programme** enthält Informationen über alle Programme, die auf dem Computer installiert sind.
- Die Registerkarte **Wird ausgeführt** enthält Echtzeitinformationen über den Verbrauch der Computerressourcen durch die einzelnen Programme. Von dieser Registerkarte aus können Sie die Berechtigungen für ein bestimmtes Programm anpassen.
- Die Registerkarte **Beim Hochfahren starten** enthält eine Liste der Programme, die beim Betriebssystemstart gestartet werden.

Wenn Sie Informationen zur Programmaktivität auf einem Benutzercomputer ausblenden möchten, können Sie den Benutzerzugriff auf das Tool „Aktivitätsmonitor für Programme“ einschränken.

So blenden Sie den „Aktivitätsmonitor für Programme“ auf der Programmoberfläche mithilfe der Verwaltungskonsole (MMC) aus

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Benutzeroberfläche** aus.
4. Verwenden Sie das Kontrollkästchen **Abschnitt „Aktivitätsmonitor für Programme“ ausblenden**, um den Zugriff auf das Tool zu erlauben oder zu verbieten.
5. Speichern Sie die vorgenommenen Änderungen.

So blenden Sie den „Aktivitätsmonitor für Programme“ auf der Programmoberfläche mithilfe der „Web Console“ und „Cloud Console“ aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Interaktion mit dem Benutzer**.
5. Verwenden Sie das Kontrollkästchen **Abschnitt „Aktivitätsmonitor für Programme“ ausblenden**, um den Zugriff auf das Tool zu erlauben oder zu verbieten.
6. Speichern Sie die vorgenommenen Änderungen.

Regeln für das Erstellen von Masken für Datei- oder Ordnernamen

Eine *Maske für den Datei- oder Ordnernamen* ist ein Platzhalter für einen Datei- oder Ordnernamen und für eine Dateierweiterung.

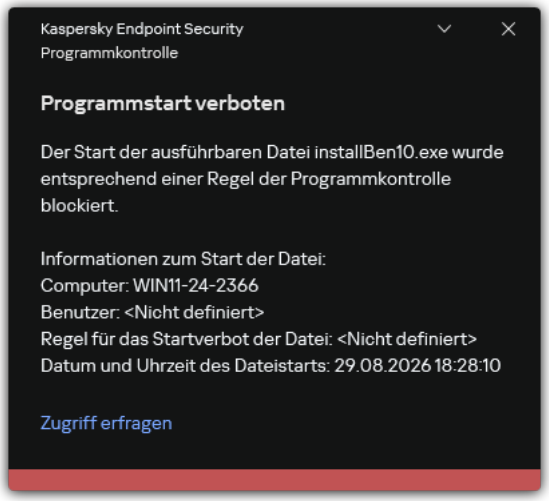
Für die Maske eines Datei- oder Ordnernamens sind folgende Platzhalter zulässig:

- Das Symbol `*` (Sternchen), das eine beliebige Zeichenkombination ersetzt (einschließlich einer leeren Zeichenfolge). Beispiel: Die Maske `C:\*.txt` umfasst alle Pfade von Dateien mit der Erweiterung `txt`, die sich in Ordnern und Unterordnern auf Laufwerk (C:) befinden.

- 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.

Meldungsvorlagen für die Programmkontrolle ändern

Versucht ein Benutzer, ein Programm zu starten, das durch eine Regel der Programmkontrolle verboten ist, so meldet Kaspersky Endpoint Security, dass der Programmstart blockiert wurde. Die Kaspersky-Experten haben eine Nachrichtenvorlage vorbereitet. In dieser Nachricht wird dem Benutzer erklärt, warum das Programm gesperrt wurde (siehe folgende Abb.). Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden. Wenn eine Nachricht generiert wird, ruft Kaspersky Endpoint Security den Wert der Variablen aus den Betriebssystemeinstellungen ab und fügt ihn passend zum Computer, Benutzer und Ereignis in die Nachricht ein.



Benachrichtigung der „Programmkontrolle"

Wenn der Benutzer der Meinung ist, der Programmstart sei irrtümlich blockiert worden, kann der Benutzer aus der Sperrmeldung eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks senden. Dazu muss der Benutzer auf **Zugriff erfragen** klicken und eine Nachricht an den Administrator senden, um die Situation zu beschreiben. Sie können auch eine Vorlage für die Nachricht an den Administrator erstellen. Dieser Nachricht können Sie Daten hinzufügen, die Ihre Entscheidung, den Zugriff auf das Programm zuzulassen oder zu sperren, begründen. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Verbot des Programmstarts**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

So bearbeiten Sie die Nachrichtenvorlage der Programmkontrolle über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Programmkontrolle** aus.
4. Klicken Sie im Block **Einstellungen für Nachrichtenvorlagen** auf **Vorlagen**.
5. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die Vorlagen der Programmkontrolle:

   - **Nachricht beim Blockieren**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert.

     Im Testmodus können Sie keine Nachrichtenvorlagen für die „Programmkontrolle“ konfigurieren. Im Testmodus zeigt die „Programmkontrolle“ voreingestellte Benachrichtigungen an.

   - **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.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable** und wählen Sie die gewünschte Variable in der Liste aus.

   Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Standard** wiederherstellen.
6. Speichern Sie die vorgenommenen Änderungen.

So bearbeiten Sie die Nachrichtenvorlage der Programmkontrolle über die Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle → App-Kontrolle**.
5. Klicken Sie im Block **Vorlagen für Nachrichten** auf den Link **Meldungen über das Verbot des Programmstarts** und konfigurieren Sie die Vorlagen für Nachrichten der Programmkontrolle:

   - **Nachricht an den Benutzer**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert.

     Im Testmodus können Sie keine Nachrichtenvorlagen für die „Programmkontrolle“ konfigurieren. Im Testmodus zeigt die „Programmkontrolle“ voreingestellte Benachrichtigungen an.

   - **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.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Auf Standard zurücksetzen** wiederherstellen.

6. Speichern Sie die vorgenommenen Änderungen.

So bearbeiten Sie die Nachrichtenvorlage der Programmkontrolle über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Programmkontrolle** aus.
3. Konfigurieren Sie im Block **Vorlagen für Nachrichten über Programmblockierung** die Nachrichtenvorlagen für die „Programmkontrolle“:

   - **Nachricht beim Blockieren**. Vorlage der Nachricht, die beim Auslösen einer Regel der Programmkontrolle erscheint, wenn diese Regel den Programmstart blockiert.

     Im Testmodus können Sie keine Nachrichtenvorlagen für die „Programmkontrolle“ konfigurieren. Im Testmodus zeigt die „Programmkontrolle“ voreingestellte Benachrichtigungen an.

   - **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.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable hinzufügen** und wählen Sie die gewünschte Variable in der Liste aus.

   Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Zurücksetzen** wiederherstellen.

4. Speichern Sie die vorgenommenen Änderungen.

Variablen in Nachrichtenvorlagen der Programmkontrolle

In Vorlagen für Nachrichten an Benutzer oder an den Administrator können Sie die folgenden Variablen verwenden:

- **Name der ausgelösten Regel** – `%RULE%`.

  Name der Regel, durch die die Ausführung einer Datei blockiert wurde.

- **Aktuelles Datum** – `%DATE%`.

  Datum, an dem die Ausführung der Datei blockiert wurde (im Format TT.MM.JJJJ).

- **Aktuelle Uhrzeit** – `%TIME%`.

  Uhrzeit, zu der die Ausführung der Datei blockiert wurde (im Format hh:mm).

- **Benutzername** – `%USER_NAME%`.

  Name des aktuellen Benutzerkontos auf dem Computer, auf dem die Ausführung der Datei blockiert wurde, im Format `<device name>\<user alias>` (z. B. `DESKTOP-123\John.Smith`).

- **Computername** – `%COMPUTER_NAME%`.

  Name des Computers, auf dem die Ausführung der Datei blockiert wurde.

- **Name der ausführbaren Datei** – `%FILE_NAME%`.

  Name der ausführbaren Datei des blockierten Programms.

- **KL-Kategorie der ausführbaren Datei** – `%KL_CAT%`.

  KL-Kategorie, zu der das blockierte Programm gehört (z. B. *Browser* oder andere Kategorie).

- **Pfad der ausführbaren Datei** – `%FILE_PATH%`.

  Vollständiger Pfad der ausführbaren Datei des blockierten Programms.

- **Version der ausführbaren Datei** – `%FILE_VERSION%`.

  Version der ausführbaren Datei des blockierten Programms.

- **Ursprünglicher Name der ausführbaren Datei** – `%ORIGINAL_FILE_NAME%`.

  Ursprünglicher Name der ausführbaren Datei des blockierten Programms. Der Dateiname ist in den Eigenschaften der ausführbaren Datei des Programms angegeben.

- **Hersteller** – `%FILE_PUBLISHER%`.

  Hersteller des blockierten Programms.

- **Programmname** – `%FILE_PRODUCT_NAME%`.

  Name des blockierten Programms.

- **Programmversion** – `%PRODUCT_VERSION%`.

  Version des blockierten Programms.

- **Hash der ausführbaren Datei** – `%FILE_HASH%`.

  Hash der ausführbaren Datei des blockierten Programms.

- **Aussteller des Zertifikats** – `%CERT_ISSUER%`.

  Aussteller des Zertifikats, mit dem die ausführbare Datei signiert ist.

- **Subjekt des Zertifikats** – `%CERT_SUBJECT%`.

  Inhaber des Zertifikats, mit dem die ausführbare Datei signiert ist.

- **Fingerabdruck des Zertifikats** – `%CERT_THUMBPRINT%`.

  Fingerabdruck des Zertifikats, mit dem die ausführbare Datei signiert ist.

Bewährte Methoden für die Inventarisierung ausführbarer Dateien

Die Aufgabe *Inventar* erfasst Informationen über ausführbare Dateien (z. B. EXE-, BAT- und CMD-Dateien), DLL-Module und Skripte (PowerShell, JS und andere). Diese Informationen werden benötigt, um Kategorien der Programmkontrolle und Programmberechtigungen für die Komponente „Programm-Überwachung“ zu konfigurieren. Die Aufgabe *Inventar* sollte regelmäßig ausgeführt werden, damit die Informationen auf dem neuesten Stand bleiben. Die Aufgabe *Inventar* ist ebenso wie die Aufgabe *Schadsoftware-Untersuchung* ressourcenintensiv. Daher wird empfohlen, die Aufgabe so zu konfigurieren, dass sie nachts oder am Wochenende ausgeführt wird.

Schritte zur Inventarisierung ausführbarer Dateien

1. Wählen Sie die Gruppe der Referenzcomputer aus, auf denen die für Ihr Unternehmen typische Software installiert ist. Es wird empfohlen, die Anzahl der Computer für die Inventarisierung ausführbarer Dateien auf ein Minimum zu beschränken. Je weniger Aufgaben *Inventar* vorhanden sind, desto geringer ist die Belastung des Kaspersky Security Center Administrationsservers.

2. Verschieben Sie die Referenzcomputer in der Konsole von Kaspersky Security Center in eine separate Administrationsgruppe. Sie können die Gruppe beispielsweise *Referenzcomputer* nennen.

3. Erstellen Sie für die Administrationsgruppe *Referenzcomputer* eine Aufgabe *Inventar*. Es wird empfohlen, die Standardeinstellungen der Aufgabe beizubehalten.

Beispiel für die Inventarisierung ausführbarer Dateien in einem Unternehmen

Angenommen, in Ihrem Unternehmen gibt es 100 Computer mit Windows 11 25H2. Auf allen Computern sind dieselbe Version und Sprachversion des Betriebssystems installiert. Auch die auf den Computern installierten Updates sind identisch.

In einem solchen Unternehmen müssen Sie die Aufgabe *Inventar* nicht auf allen Computern ausführen. Die meisten ausführbaren Dateien auf diesen Computern sind identisch. Es reicht aus, eine Aufgabe für einen Referenzcomputer zu erstellen. Sie können für Computer, deren Konfiguration von der Referenz abweicht, zusätzliche Aufgaben *Inventar* erstellen.

Bewährte Praktiken für die Implementierung einer Liste zulässiger Programme

Bei der Planung der Implementierung einer Liste von erlaubten Programmen wird empfohlen, die folgenden Aktionen durchzuführen:

1. Folgende Typen von Gruppierungen erstellen:

   - Benutzergruppen Gruppen mit Benutzern, für welche die Verwendung unterschiedlicher Sätze von Programmen erlaubt werden soll.

   - Administrationsgruppen Eine oder mehrere Gruppen von Computern, auf die das Kaspersky Security Center die Liste der erlaubten Programme anwendet. Es ist erforderlich, mehrere Gruppen von Computern zu erstellen, wenn für diese Gruppen unterschiedliche Allowlist-Einstellungen verwendet werden.

2. Liste mit Programmen, deren Start erlaubt werden soll, erstellen

   Bevor die Liste erstellt wird, sollten die folgenden Aktionen ausgeführt werden:

   a. Aufgabe zur Inventarisierung starten

      Informationen über die Erstellung, die Einstellungsänderungen und den Start der Inventarisierungsaufgabe sind im Abschnitt „Aufgabenverwaltung“ verfügbar.

   b. Liste der ausführbarer Dateien überprüfen

Konfigurieren des Allowlist-Modus für Programme

Um den Allowlist-Modus zu testen, wird folgendes Vorgehen empfohlen:

1. Erstellung von Programmkategorien, die jene Programme enthalten, deren Start erlaubt werden soll

   Sie können eine der folgenden Erstellungsmethoden für die Programmkategorien auswählen:

   - **Manuell zu erweiternde Kategorie**. Sie können diese Kategorie unter Verwendung der folgenden Bedingungen manuell ergänzen:
     - Metadaten einer Datei. Kaspersky Security Center fügt alle ausführbaren Dateien, welche die angegebenen Metadaten aufweisen, zu der Programmkategorie hinzu.
     - Datei-Hash. Kaspersky Security Center fügt alle ausführbaren Dateien, die den angegebenen Hash haben, zu der Programmkategorie hinzu.

       Wenn diese Bedingung verwendet wird, ist die automatische Installation von Updates nicht möglich, da die Dateien der einzelnen Versionen einen unterschiedlichen Hash besitzen.

     - Zertifikat einer Datei. Kaspersky Security Center fügt alle ausführbaren Dateien, die mit dem angegebenen Zertifikat signiert sind, zu der Programmkategorie hinzu.
     - KL-Kategorie. Kaspersky Security Center nimmt alle ausführbaren Dateien, die zur angegebenen KL-Kategorie gehören, in die Programmkategorie auf.
     - Programmordner. Kaspersky Security Center fügt alle ausführbaren Dateien aus diesem Ordner zu der Programmkategorie hinzu.

       Die Verwendung der Bedingung **Anwendungsordner** ist möglicherweise riskant, da dann der Start aller Programme aus dem angegebenen Ordner erlaubt wird. Regeln, die Programmkategorien mit der Bedingung **Anwendungsordner** verwenden, sollten nur für jene Benutzer verwendet werden, für welche die automatische Update-Installation erlaubt werden muss.

   - **Kategorie für ausführbare Dateien aus dem angegebenen Ordner**. Sie können einen Ordner angeben, der ausführbare Dateien enthält, die automatisch in die erstellte Programmkategorie aufgenommen werden sollen.
   - **Kategorie für ausführbare Dateien der gewählten Geräte**. Sie können einen Computer angeben, dessen ausführbare Dateien automatisch in die erstellte Programmkategorie aufgenommen werden sollen.

     Wenn Programmkategorien auf diese Weise erstellt werden, erhält Kaspersky Security Center die Informationen über Programme auf dem Computer aus dem Ordner **Ausführbare Dateien**.

2. Wählen Sie den Allowlist-Modus für die Komponente „Programmkontrolle“.

3. Regeln der Programmkontrolle unter Verwendung der erstellten Programmkategorien erstellen

   Die Regeln **Goldene Kategorie** und **Vertrauenswürdige Programme mit Update-Funktionen** werden anfänglich für den Zulässigkeitslistenmodus definiert. Diese Regeln der Programmkontrolle entsprechen den KL-Kategorien. Zur KL-Kategorie *Goldene Kategorie* gehören jene Programme, welche die normale Funktion des Betriebssystems gewährleisten. Zur KL-Kategorie *Vertrauenswürdige Programme mit Update-Funktionen* gehören Programme mit Update-Funktionen der gängigen Softwarehersteller. Diese Regeln können nicht gelöscht werden. Die Einstellungen dieser Regeln können nicht geändert werden. Standardmäßig ist die Regel **Goldene Kategorie** aktiviert, und die Regel **Vertrauenswürdige Programme mit Update-Funktionen** ist deaktiviert. Der Start von Programmen, welche den Auslösebedingungen dieser Regeln entsprechen, ist für alle Benutzer erlaubt.

4. Programme festlegen, für welche die automatische Update-Installation erlaubt werden muss

   Sie können die automatische Installation von Updates auf folgende Weise erlauben:

   - Erstellen einer erweiterten Liste mit erlaubten Programmen, nachdem der Start für alle Programme aus beliebigen KL-Kategorien erlaubt wurde
   - Erstellen einer erweiterten Liste mit erlaubten Programmen, nachdem der Start für alle Programme erlaubt wurde, die mit einem Zertifikat signiert sind

     Um den Start alle Programme die mit einem Zertifikat signiert sind, zu erlauben, können Sie eine Kategorie mit einer Bedingung erstellen, die auf einem Zertifikat basiert und in welcher nur der Parameter **Antragsteller** mit dem Wert `*` verwendet wird.
   - Für die Regel der Programmkontrolle den Parameter **Vertrauenswürdige Programme mit Update-Funktionen** festlegen. 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 den Start von Programmen, die durch in der Regel enthaltene Programme installiert oder aktualisiert wurden, vorausgesetzt, dass auf diese Programme keine Sperrregeln angewendet werden.

     Bei der Migration von Einstellungen migriert Kaspersky Endpoint Security auch eine Liste mit ausführbaren Dateien, die von vertrauenswürdigen Programmen mit Update-Funktionen erstellt worden sind.
   - Einen Ordner erstellen und die ausführbaren Dateien jener Programme, für welche Sie die automatische Update-Installation erlauben möchten, in diesen Ordner verschieben. Anschließend eine Programmkategorie mit der Bedingung **Anwendungsordner** erstellen und den Pfad dieses Ordners angeben. Danach eine Erlaubnisregel erstellen und diese Kategorie auswählen.

     Die Verwendung der Bedingung **Anwendungsordner** ist möglicherweise riskant, da dann der Start aller Programme aus dem angegebenen Ordner erlaubt wird. Regeln, die Programmkategorien mit der Bedingung **Anwendungsordner** verwenden, sollten nur für jene Benutzer verwendet werden, für welche die automatische Update-Installation erlaubt werden muss.

Testen des Allowlist-Modus

Um sicherzustellen, dass Programme, die Sie zum Arbeiten benötigen, nicht durch Regeln der Programmkontrolle blockiert werden, wird empfohlen, für neu erstellte Regeln den Test für Regeln der Programmkontrolle zu aktivieren und ihre Funktion zu analysieren. Wenn der Testlauf aktiviert ist, werden Programme, für welche der Start durch Regeln der Programmkontrolle verboten ist, von Kaspersky Endpoint Security nicht blockiert. Es werden aber Benachrichtigungen über ihren Start an den Administrationsserver gesendet.

Um den Allowlist-Modus zu testen, wird folgendes Vorgehen empfohlen:

1. Testzeitraum festlegen (von mehreren Tagen bis zu zwei Monaten)
2. Test für die Regeln der Programmkontrolle aktivieren
3. Analyse der Testergebnisse unter Verwendung von Ereignissen aus den Ergebnissen des Testlaufs der Komponente „Programmkontrolle" und der Berichte über im Testmodus verbotene Programme
4. Ändern Sie Einstellungen für den Allowlist-Modus unter Berücksichtigung der Analyseergebnisse.

   Aufgrund der Testergebnisse können Sie ausführbare Dateien, die mit Ereignissen zusammenhängen, zu der Programmkategorie hinzufügen.

Unterstützung für den Allowlist-Modus

Nachdem eine Sperraktion der Programmkontrolle ausgewählt wurde, sollte die Unterstützung des Allowlist-Modus fortgesetzt werden. Dazu dient folgendes Vorgehen:

- Funktionsanalyse der Regeln der Programmkontrolle unter Verwendung von Ereignissen aus den Ergebnissen der Verwendung der Komponente „Programmkontrolle" und der Berichte über verbotene Starts
- Analyse von Benutzeranfragen für den Zugriff auf Programme.
- Analysieren Sie unbekannte ausführbare Dateien, indem Sie ihren Ruf im Kaspersky Security Network überprüfen.
- Vor der Installation von Updates für das Betriebssystem oder für Programme, sollten diese Updates in der Testgruppe für Computer installiert werden, um zu überprüfen, wie sie von den Regeln der Programmkontrolle verarbeitet werden.
- Hinzufügen der erforderlichen Programme zu den Kategorien, die in den Regeln der Programmkontrolle verwendet werden

Kontrolle von Netzwerkports

Wenn Kaspersky Endpoint Security ausgeführt wird, überwachen die Komponenten Web-Kontrolle, Schutz vor E-Mail-Bedrohungen, Schutz vor Web-Bedrohungen, Verhaltensanalyse und Exploit-Prävention die Datenströme, die über bestimmte Protokolle und bestimmte offene TCP- und UDP-Ports des Benutzercomputers übertragen werden. Die Komponente „Schutz vor E-Mail-Bedrohungen" analysiert beispielsweise die Informationen, die per SMTP-Protokoll übertragen werden, während die Komponente „Schutz vor Web-Bedrohungen" die per HTTP- und FTP-Protokolle übertragenen Informationen analysiert.

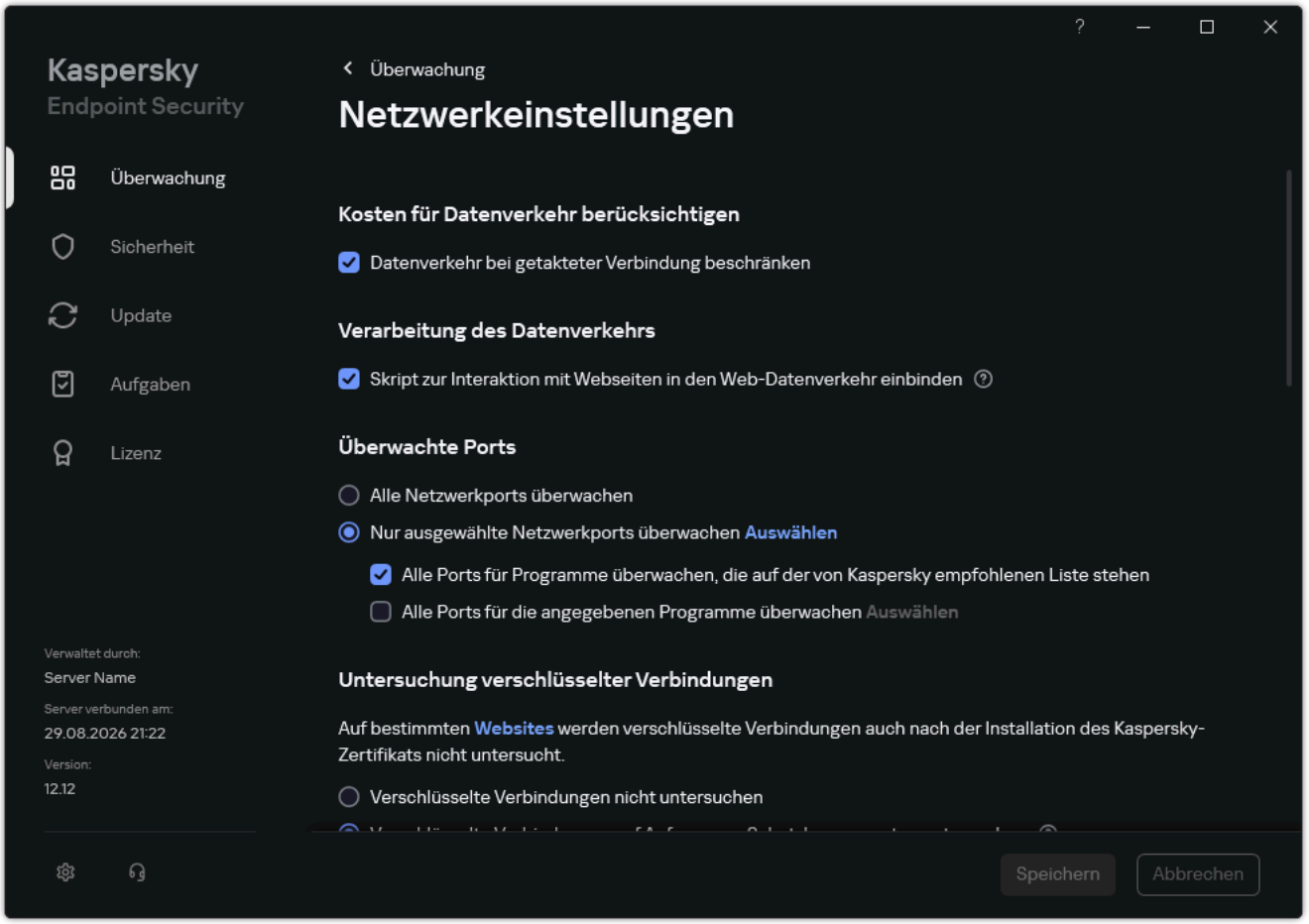
Kaspersky Endpoint Security teilt die TCP- und UDP-Ports des Benutzercomputers je nach Angriffswahrscheinlichkeit in mehrere Gruppen ein. Einige Netzwerkports sind für gefährdete Dienste reserviert. Es wird empfohlen, die Netzwerkports, die für anfällige Dienste reserviert sind, genauer zu überwachen, da für sie ein erhöhtes Risiko besteht, Ziel eines Netzwerkangriffs zu werden. Wenn Sie außergewöhnliche Dienste verwenden, denen außergewöhnliche Netzwerkports zugewiesen sind, so können diese Netzwerkports angreifenden Computern ebenfalls als Ziel dienen. Sie können eine Liste von Netzwerkanschlüssen und eine Liste von Programmen angeben, die Netzwerkzugriff anfordern. Diese Ports und Programme erhalten dann bei der Überwachung des Netzwerkverkehrs besondere Aufmerksamkeit von den Komponenten Schutz vor E-Mail-Bedrohungen und Schutz vor Web-Bedrohungen.

Um die Sicherheit des Computers zu gewährleisten, überwachen die Komponenten Verhaltenserkennung und Exploit-Prävention auch Datenströme, die über Netzwerkports fließen. Die Komponenten überwachen den Netzwerkverkehr kontinuierlich auf einzelne, möglicherweise bedrohliche Prozesse.

Kontrolle aller Netzwerkports aktivieren

Gehen Sie folgendermaßen vor, um die Kontrolle aller Netzwerkports zu aktivieren:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Netzwerkeinstellungen** aus.



Einstellungen der Überwachung von Netzwerkports

3. Wählen Sie im Block **Überwachte Ports** die Variante **Alle Netzwerkports überwachen** aus.
4. Speichern Sie die vorgenommenen Änderungen.

Liste der zu kontrollierenden Netzwerkports erstellen

Gehen Sie folgendermaßen vor, um eine Liste der zu kontrollierenden Netzwerkports zu erstellen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Netzwerkeinstellungen** aus.
3. Wählen Sie im Block **Überwachte Ports** die Variante **Nur ausgewählte Netzwerkports überwachen** aus.

4. Klicken Sie auf **Auswählen**.

   Dies öffnet eine Liste von Netzwerkports, die normalerweise für die Übertragung von E-Mail und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.

5. Verwenden Sie den Schalter in der Spalte **Status**, um die Kontrolle von Netzwerkports zu aktivieren oder zu deaktivieren.

6. Gehen Sie folgendermaßen vor, um einen Netzwerkport zur Liste der Netzwerkports hinzuzufügen:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie in dem sich öffnenden Fenster die Netzwerkportnummer und eine kurze Beschreibung ein.

   c. Setzen Sie den Status **Aktiv** oder **Inaktiv** für die Kontrolle von Netzwerkports.

7. Speichern Sie die vorgenommenen Änderungen.

Wenn der passive FTP-Modus verwendet wird, kann die Verbindung über einen beliebigen Netzwerkport hergestellt werden, der nicht auf der Liste der kontrollierten Ports steht. Um solche Verbindungen zu schützen, aktivieren Sie die Kontrolle aller Netzwerkports oder konfigurieren Sie die Kontrolle der Netzwerkports für Programme, die FTP-Verbindungen herstellen.

Liste der Programme erstellen, für die alle Netzwerkports überwacht werden

Sie können eine Liste mit Programmen erstellen, für die Kaspersky Endpoint Security alle Netzwerkports kontrollieren soll.

Es wird empfohlen, in die Liste der Programme, für die Kaspersky Endpoint Security alle Netzwerkports kontrollieren soll, jene Programme aufzunehmen, die Daten über das FTP-Protokoll empfangen oder senden.

Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Netzwerkports kontrolliert werden sollen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.

3. Wählen Sie im Block **Überwachte Ports** die Variante **Nur ausgewählte Netzwerkports überwachen** aus.

4. Aktivieren Sie das Kontrollkästchen **Alle Ports für Programme überwachen, die auf der von Kaspersky empfohlenen Liste stehen**.

   Wenn dieses Kontrollkästchen aktiviert ist, kontrolliert Kaspersky Endpoint Security alle Ports für die folgenden Programme:

   - Adobe Acrobat Reader
   - Apple Application Support

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Internet Explorer
- Java
- mIRC
- Opera
- Pidgin
- Safari
- Mail.ru-Agent
- Yandex.Browser

5. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme überwachen**.
6. Klicken Sie auf **Auswählen**.

   Dies öffnet eine Liste von Programmen, deren Netzwerkports von Kaspersky Endpoint Security überwacht werden.
7. Verwenden Sie den Schalter in der Spalte **Status**, um die Kontrolle von Netzwerkports zu aktivieren oder zu deaktivieren.
8. Wenn ein Programm nicht auf der Programmliste steht, können Sie es wie folgt hinzufügen:
   a. Klicken Sie auf **Hinzufügen**.
   b. Geben Sie in dem sich öffnenden Fenster den Pfad zu der ausführbaren Datei des Programms und eine kurze Beschreibung ein.
   c. Setzen Sie den Status **Aktiv** oder **Inaktiv** für die Kontrolle von Netzwerkports.
9. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren von Listen überwachter Ports

Kaspersky Endpoint Security verwendet die folgenden Listen zur Überwachung von Netzwerkports: Liste der Netzwerkports und Liste der Programme, deren Ports von Kaspersky Endpoint Security überwacht werden. Sie können Listen überwachter Ports in eine XML-Datei exportieren. Anschließend können Sie die Datei ändern, um beispielsweise eine große Anzahl von Ports mit derselben Beschreibung hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup für die Listen der überwachten Ports anzulegen oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren von Listen überwachter Ports in der Verwaltungskonsole (MMC)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Netzwerkeinstellungen**.
5. So exportieren Sie die Liste der Netzwerkports:

   a. Wählen Sie im Block **Überwachte Ports** die Variante **Nur ausgewählte Netzwerkports überwachen** aus.

   b. Klicken Sie auf den Link **n Ports ausgewählt**.

   Das Fenster **Netzwerkports** wird geöffnet. Im Fenster **Netzwerkports** befindet sich eine Liste der Netzwerkports, die normalerweise für die Übertragung von E-Mails und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.

   c. Wählen Sie in der Liste der Netzwerkports die Ports aus, die Sie exportieren möchten.

   d. Klicken Sie auf **Export**.

   e. Geben Sie im angezeigten Fenster den Namen der XLM-Datei ein, in welche Sie die Liste der Netzwerkports exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   f. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Netzwerkports in die XLM-Datei.
6. So exportieren Sie die Liste der Programme, deren Ports von Kaspersky Endpoint Security überwacht werden:

   a. Aktivieren Sie im Block **Überwachte Ports** das Kontrollkästchen **Alle Ports für die angegebenen Programme überwachen**.

   b. Klicken Sie auf den Link **n Programme ausgewählt**.

   c. Wählen Sie in der Liste der Programme die Programme aus, die Sie exportieren möchten.

   d. Klicken Sie auf **Export**.

   e. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Programme exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   f. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Programme in die XLM-Datei.
7. So importieren Sie die Liste der Netzwerkports:

   a. Klicken Sie in der Liste der Netzwerkports auf die Schaltfläche **Import**.

   Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Netzwerkports importieren möchten.

b. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Netzwerkports gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

8. So importieren Sie eine Liste von Programmen, deren Ports von Kaspersky Endpoint Security überwacht werden:

a. Klicken Sie in der Liste der Programme auf **Import**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Anwendungen importieren möchten.

b. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Programmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

9. Speichern Sie die vorgenommenen Änderungen.

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Netzwerkeinstellungen** aus.

4. Wählen Sie im Block **Überwachte Ports** die Variante **Nur ausgewählte Netzwerkports überwachen** aus.

5. Klicken Sie auf **Einstellungen**.

Das Fenster **Netzwerkports** wird geöffnet. Im Fenster **Netzwerkports** befindet sich eine Liste der Netzwerkports, die normalerweise für die Übertragung von E-Mails und Netzwerkverkehr verwendet werden. Diese Liste mit Netzwerkports gehört zum Lieferumfang von Kaspersky Endpoint Security.

6. So exportieren Sie die Liste der Netzwerkports:

a. Wählen Sie in der Liste der Netzwerkports die Ports aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

Wenn Sie keinen Port ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ports.

b. Klicken Sie auf **Exportieren**.

c. Geben Sie im angezeigten Fenster den Namen der XLM-Datei ein, in welche Sie die Liste der Netzwerkports exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

d. Speichern Sie die Datei.

Kaspersky Endpoint Security exportiert die gesamte Liste der Netzwerkports in die XLM-Datei.

7. So exportieren Sie die Liste der Programme, deren Ports von Kaspersky Endpoint Security überwacht werden:

a. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme überwachen**.

b. Wählen Sie in der Liste der Programme die Programme aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

Wenn Sie kein Programm ausgewählt haben, exportiert Kaspersky Endpoint Security alle Programme.

c. Klicken Sie auf **Exportieren**.

d. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Programme exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

e. Speichern Sie die Datei.

Kaspersky Endpoint Security exportiert die gesamte Liste der Programme in die XLM-Datei.

8. So importieren Sie die Liste der Netzwerkports:

a. Klicken Sie in der Liste der Netzwerkports auf die Schaltfläche **Importieren**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Netzwerkports importieren möchten.

b. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Netzwerkports gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

9. So importieren Sie eine Liste von Programmen, deren Ports von Kaspersky Endpoint Security überwacht werden:

a. Klicken Sie in der Liste der Programme auf **Importieren**.

Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Anwendungen importieren möchten.

b. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Programmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

10. Speichern Sie die vorgenommenen Änderungen.

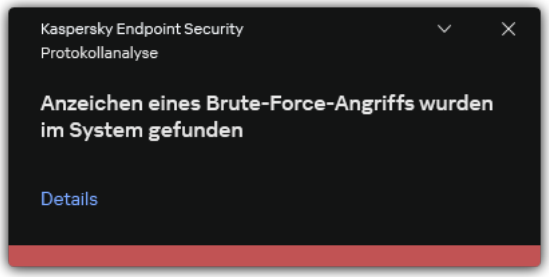
Protokollanalyse

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 „Protokollanalyse“ überwacht die Integrität der geschützten Umgebung basierend auf der Windows-Ereignisprotokollanalyse. Wenn das Programm ungewöhnliche Verhaltensmerkmale im System erkennt, wird der Administrator informiert, da solches Verhalten auf einen versuchten Cyberangriff hinweisen kann.

Kaspersky Endpoint Security analysiert Windows-Ereignisprotokolle und erkennt Verstöße gemäß den Regeln. Die Komponente enthält vordefinierte Regeln. Vordefinierte Regeln basieren auf einer heuristischen Analyse. Sie können auch Ihre eigenen Regeln hinzufügen (benutzerdefinierte Regeln). Wenn eine Regel ausgelöst wird, erstellt das Programm ein Ereignis mit dem Status *Kritisch* (siehe Abbildung unten).

Wenn Sie die Protokollanalyse verwenden möchten, stellen Sie sicher, dass die Sicherheitseinstellungen der Audit-Richtlinie konfiguriert sind und das System die relevanten Ereignisse protokolliert (Einzelheiten finden Sie auf der Website des technischen Supports von Microsoft).



Protokollanalysebenachrichtigung

Vordefinierte Regeln konfigurieren

Vordefinierte Regeln enthalten Vorlagen für anormale Aktivitäten auf dem geschützten Computer. Abnormale Aktivität kann auf einen versuchten Angriff hindeuten. Vordefinierte Regeln basieren auf einer heuristischen Analyse. Für die Protokollanalyse stehen sieben vordefinierte Regeln zur Verfügung. Sie können diese Regeln aktivieren oder deaktivieren. Vordefinierte Regeln können nicht gelöscht werden.

Sie können die Auslösekriterien für Regeln konfigurieren, die Ereignisse für die folgenden Vorgänge überwachen:

- Passwort-Brute-Force-Erkennung
- Netzwerk-Login-Erkennung

So konfigurieren Sie vordefinierte Regeln in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Protokollanalyse** aus.
4. Stellen Sie sicher, dass das Kontrollkästchen **Protokollanalyse** aktiviert ist.
5. Klicken Sie im Block **Vordefinierte Regeln** auf **Einstellungen**.
6. Aktivieren oder deaktivieren Sie Kontrollkästchen, um vordefinierte Regeln zu konfigurieren:
   - **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**.
   - **Während einer Netzwerkanmeldesitzung wurde eine ungewöhnliche Aktivität erkannt**.
   - **Anzeichen für eine Gefährdung der Windows-Ereignisprotokolle wurden gefunden**.

- **Ungewöhnliche Aktionen im Auftrag eines neu installierten Dienstes wurden erkannt**.
- **Eine ungewöhnliche Anmeldung mit expliziten Anmeldedaten wurde erkannt**.
- **Anzeichen eines Angriffs mit gefälschtem Kerberos-PAC (MS14-068) wurden im System gefunden**.
- **Verdächtige Änderungen in der privilegierten integrierten Administratorgruppe wurden erkannt**.

7. Konfigurieren Sie ggf. die Regel **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**:
   a. Klicken Sie auf die Schaltfläche **Einstellungen** unter der Regel.
   b. Geben Sie in dem sich öffnenden Fenster die Anzahl der Versuche und einen Zeitraum an, innerhalb dessen Versuche zur Eingabe eines Passworts unternommen werden müssen, damit die Regel ausgelöst wird.
   c. Klicken Sie auf **OK**.
8. Wenn Sie die Regel **Während einer Netzwerkanmeldesitzung wurde eine ungewöhnliche Aktivität erkannt** ausgewählt haben, müssen Sie die entsprechenden Einstellungen konfigurieren:
   a. Klicken Sie auf die Schaltfläche **Einstellungen** unter der Regel.
   b. Geben Sie im Block **Erkennung von Netzwerkanmeldungen** Start und Ende des Intervalls ein.

      Kaspersky Endpoint Security betrachtet Anmeldeversuche, die während des angegebenen Intervalls durchgeführt werden, als anormale Aktivität.

      Das Intervall ist standardmäßig nicht angegeben und Anmeldeversuche werden von der App nicht überwacht. Damit Anmeldeversuche permanent vom Programm überwacht werden, geben Sie das Intervall 0:00 bis 23:59 an. Der Beginn und das Ende des Intervalls dürfen nicht übereinstimmen. Wenn sie den gleichen Wert haben, werden Anmeldeversuche nicht durch die App überwacht.
   c. Erstellen Sie die Liste der vertrauenswürdigen Benutzer und vertrauenswürdigen IP-Adressen (IPv4 und IPv6).

      Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können. Kaspersky Endpoint Security überwacht die Anmeldeversuche dieser Benutzer und Computer nicht.
   d. Klicken Sie auf **OK**.
9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie vordefinierte Regeln über die „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Protokollanalyse**.
5. Stellen Sie sicher, dass der Schalter **Protokollanalyse AKTIVIERT** aktiviert ist.

6. Aktivieren oder deaktivieren Sie im Block **Vordefinierte Regeln** die vordefinierten Regeln mithilfe der Schalter.

   - **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**.
   - **Während einer Netzwerkanmeldesitzung wurde eine ungewöhnliche Aktivität erkannt**.
   - **Anzeichen für eine Gefährdung der Windows-Ereignisprotokolle wurden gefunden**.
   - **Ungewöhnliche Aktionen im Auftrag eines neu installierten Dienstes wurden erkannt**.
   - **Eine ungewöhnliche Anmeldung mit expliziten Anmeldedaten wurde erkannt**.
   - **Anzeichen eines Angriffs mit gefälschtem Kerberos-PAC (MS14-068) wurden im System gefunden**.

   a. **Verdächtige Änderungen in der privilegierten integrierten Administratorgruppe wurden erkannt**.

7. Konfigurieren Sie ggf. die Regel **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**:

   a. Klicken Sie auf **Einstellungen** unter der Regel.

   b. Geben Sie in dem sich öffnenden Fenster die Anzahl der Versuche und einen Zeitraum an, innerhalb dessen Versuche zur Eingabe eines Passworts unternommen werden müssen, damit die Regel ausgelöst wird.

   c. Klicken Sie auf **OK**.

8. Wenn Sie die Regel **Während einer Netzwerkanmeldesitzung wurde eine ungewöhnliche Aktivität erkannt** ausgewählt haben, müssen Sie die entsprechenden Einstellungen konfigurieren:

   a. Klicken Sie auf **Einstellungen** unter der Regel.

   b. Geben Sie im Block **Erkennung von Netzwerkanmeldungen** Start und Ende des Intervalls ein.

   Kaspersky Endpoint Security betrachtet Anmeldeversuche, die während des angegebenen Intervalls durchgeführt werden, als anormale Aktivität.

   Das Intervall ist standardmäßig nicht angegeben und Anmeldeversuche werden von der App nicht überwacht. Damit Anmeldeversuche permanent vom Programm überwacht werden, geben Sie das Intervall 0:00 bis 23:59 an. Der Beginn und das Ende des Intervalls dürfen nicht übereinstimmen. Wenn sie den gleichen Wert haben, werden Anmeldeversuche nicht durch die App überwacht.

   c. Fügen Sie im Block **Ausnahmen** vertrauenswürdige Benutzer und vertrauenswürdige IP-Adressen (IPv4 und IPv6) hinzu.

   Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können. Kaspersky Endpoint Security überwacht die Anmeldeversuche dieser Benutzer und Computer nicht.

   d. Klicken Sie auf **OK**.

9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie vordefinierte Regeln (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Protokollanalyse** aus.

3. Stellen Sie sicher, dass der Schalter **Protokollanalyse** aktiviert ist.

4. Klicken Sie im Block **Vordefinierte Regeln** auf **Konfigurieren**.

5. Aktivieren oder deaktivieren Sie Kontrollkästchen, um vordefinierte Regeln zu konfigurieren:

   - **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**.
   - **Es wurde eine ungewöhnliche Aktivität während einer Netzwerkanmeldesitzung erkannt**.
   - **Anzeichen für eine Gefährdung der Windows-Ereignisprotokolle wurden gefunden**.
   - **Ungewöhnliche Aktionen im Auftrag eines neu installierten Dienstes wurden erkannt**.
   - **Eine ungewöhnliche Anmeldung mit expliziten Anmeldedaten wurde erkannt**.
   - **Anzeichen eines Angriffs mit gefälschtem Kerberos-PAC (MS14-068) wurden im System gefunden**.

   a. **Verdächtige Änderungen in der privilegierten integrierten Administratorgruppe wurden erkannt**.

6. Konfigurieren Sie ggf. die Regel **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**:

   a. Klicken Sie auf **Einstellungen** unter der Regel.

   b. Geben Sie in dem sich öffnenden Fenster die Anzahl der Versuche und einen Zeitraum an, innerhalb dessen Versuche zur Eingabe eines Passworts unternommen werden müssen, damit die Regel ausgelöst wird.

7. Wenn Sie die Regel **Es wurde eine ungewöhnliche Aktivität während einer Netzwerkanmeldesitzung erkannt** ausgewählt haben, müssen Sie die entsprechenden Einstellungen konfigurieren:

   a. Klicken Sie auf **Einstellungen** unter der Regel.

   b. Geben Sie im Block **Erkennung von Netzwerkanmeldungen** Start und Ende des Intervalls ein.

   Kaspersky Endpoint Security betrachtet Anmeldeversuche, die während des angegebenen Intervalls durchgeführt werden, als anormale Aktivität.

   Das Intervall ist standardmäßig nicht angegeben und Anmeldeversuche werden von der App nicht überwacht. Damit Anmeldeversuche permanent vom Programm überwacht werden, geben Sie das Intervall 0:00 bis 23:59 an. Der Beginn und das Ende des Intervalls dürfen nicht übereinstimmen. Wenn sie den gleichen Wert haben, werden Anmeldeversuche nicht durch die App überwacht.

   c. Fügen Sie im Block **Ausnahmen** vertrauenswürdige Benutzer und vertrauenswürdige IP-Adressen (IPv4 und IPv6) hinzu.

   Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können. Kaspersky Endpoint Security überwacht die Anmeldeversuche dieser Benutzer und Computer nicht.

8. Speichern Sie die vorgenommenen Änderungen.

Wenn die Regel ausgelöst wird, erstellt Kaspersky Endpoint Security ein *Kritisches Ereignis*.

Benutzerdefinierte Regeln hinzufügen

Sie können Ihre eigenen Auslösekriterien für die Protokollanalyseregel festlegen. Dazu müssen Sie eine Ereignis-ID eingeben und eine Ereignisquelle auswählen. Sie können die Ereignis-ID auf der Website des Technischen Supports von Microsoft nachschlagen. Sie können eine Ereignisquelle aus den Standardprotokollen auswählen: *Application*, *Security* oder *System*. Sie können auch das Protokoll eines Drittanbieterprogramms angeben. Sie können den Namen des Programmprotokolls des Drittanbieters mit dem Tool Event Viewer herausfinden. Programmprotokolle von Drittanbietern werden im Ordner „Programm- und Dienstprotokolle" gespeichert (z. B. das *Windows PowerShell*-Protokoll).

Das Programm überprüft nicht, ob das angegebene Protokoll tatsächlich im Windows-Ereignisprotokoll vorhanden ist. Wenn der Name des Protokolls einen Fehler enthält, überwacht das Programm keine Ereignisse aus diesem Protokoll.

Die Liste der benutzerdefinierten Regeln enthält bereits drei Regeln, die von Kaspersky-Experten erstellt wurden.

So fügen Sie in der Verwaltungskonsole (MMC) eine benutzerdefinierte Regel hinzu

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle** → **Protokollanalyse** aus.
4. Stellen Sie sicher, dass das Kontrollkästchen **Protokollanalyse** aktiviert ist.
5. Klicken Sie im Block **Benutzerdefinierte Regeln** auf **Einstellungen**.
6. Es öffnet sich ein Fenster. Wählen Sie im angezeigten Fenster die benutzerdefinierten Regeln, die Sie aktivieren möchten.
7. Klicken Sie ggf. auf **Hinzufügen**, um Ihre eigenen benutzerdefinierten Regeln zu erstellen.
8. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die benutzerdefinierte Regel:
   - **Regelname**.
   - **Name des Protokolls**. Windows-Ereignisprotokolle. Die folgenden Protokolle sind verfügbar: *Application*, *Security*, *System*.
   - **Quelle**. Programmprotokolle von Drittanbietern. Sie können den Namen des Programmprotokolls des Drittanbieters mit dem Tool Event Viewer herausfinden. Programmprotokolle von Drittanbietern werden im Ordner „Programm- und Dienstprotokolle" gespeichert (z. B. das *Windows PowerShell*-Protokoll).
   - **Ereignis-IDs**. Ereignis-IDs im Windows-Ereignisprotokoll. Sie können die Ereignis-ID in der technischen Dokumentation von Microsoft nachschlagen.
9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine benutzerdefinierte Regel in der Web Console und der Cloud Console hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle** → **Protokollanalyse**.
5. Stellen Sie sicher, dass der Schalter **Protokollanalyse AKTIVIERT** aktiviert ist.
6. Wählen Sie im Block **Benutzerdefinierte Regeln** die benutzerdefinierten Regeln aus, die Sie aktivieren möchten.
7. Klicken Sie ggf. auf **Hinzufügen**, um Ihre eigenen benutzerdefinierten Regeln zu erstellen.
8. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die benutzerdefinierte Regel:
   - **Regelname**.
   - **Benutzerdefinierter Protokollname**. Windows-Ereignisprotokolle. Die folgenden Protokolle sind verfügbar: *Application*, *Security*, *System*.
   - **Herkunft**. Programmprotokolle von Drittanbietern. Sie können den Namen des Programmprotokolls des Drittanbieters mit dem Tool Event Viewer herausfinden. Programmprotokolle von Drittanbietern werden im Ordner „Programm- und Dienstprotokolle" gespeichert (z. B. das *Windows PowerShell*-Protokoll).
   - **Ereignis-IDs**. Ereignis-IDs im Windows-Ereignisprotokoll. Sie können die Ereignis-ID in der technischen Dokumentation von Microsoft nachschlagen.
9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie in der Programmoberfläche eine benutzerdefinierte Regel hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle** → **Protokollanalyse** aus.
3. Stellen Sie sicher, dass der Schalter **Protokollanalyse** aktiviert ist.
4. Klicken Sie im Block **Benutzerdefinierte Regeln** auf **Konfigurieren**.
5. Es öffnet sich ein Fenster. Wählen Sie im angezeigten Fenster die benutzerdefinierten Regeln, die Sie aktivieren möchten.
6. Klicken Sie ggf. auf **Hinzufügen**, um Ihre eigenen benutzerdefinierten Regeln zu erstellen.
7. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die benutzerdefinierte Regel:
   - **Regelname**.
   - **Name des Protokolls**. Windows-Ereignisprotokolle. Die folgenden Protokolle sind verfügbar: *Application*, *Security*, *System*.

- **Quelle**. Programmprotokolle von Drittanbietern. Sie können den Namen des Programmprotokolls des Drittanbieters mit dem Tool Event Viewer herausfinden. Programmprotokolle von Drittanbietern werden im Ordner „Programm- und Dienstprotokolle“ gespeichert (z. B. das *Windows PowerShell*-Protokoll).

- **Ereignis-ID**. Ereignis-IDs im Windows-Ereignisprotokoll. Sie können die Ereignis-ID in der technischen Dokumentation von Microsoft nachschlagen.

8. Speichern Sie die vorgenommenen Änderungen.

Wenn die Regel ausgelöst wird, erstellt Kaspersky Endpoint Security ein *kritisches* Ereignis.

Überwachung der Systemintegrität

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.

Ab Version 12.6 wird in Kaspersky Endpoint Security für Windows die Komponente „Überwachung der Datei-Integrität“ durch die Komponente „Überwachung der Systemintegrität“ ersetzt. Die Überwachung der Systemintegrität enthält alle Funktionen der Überwachung der Dateiintegrität und ermöglicht zusätzlich die Überwachung von Registrierungsänderungen und angeschlossenen Geräten.

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.

Echtzeitüberwachung der Systemintegrität

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.

Prüfung der Systemintegrität auf Befehl

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.

Migration der Einstellungen für die Überwachung der Datei-Integrität

Wenn Sie Kaspersky Endpoint Security auf Version 12.6 aktualisieren, werden die Einstellungen für die Überwachung der Datei-Integrität automatisch migriert. Im Rahmen der Migration werden die Überwachungsregeln in die Überwachung der Systemintegrität verschoben. Die Regeln der Überwachung der Datei-Integrität werden auch in die Überwachung der Systemintegrität migriert, wenn KSWS nach KES migriert wird.

Um für die Überwachung der Systemintegrität eine ordnungsgemäße Ausführung der zu gewährleisten, sollten sowohl die App von Kaspersky Endpoint Security als auch das Verwaltungs-Plug-in auf Version 12.6 aktualisiert werden. Wenn Sie eine frühere Version des Verwaltungs-Plug-ins installiert haben, können Sie die Überwachung der Systemintegrität nicht konfigurieren, da in dem Verwaltungs-Plug-in der Abschnitt **Überwachung der Systemintegrität** nicht vorhanden ist.

Über Regeln für die Überwachung der Systemintegrität

Damit die Überwachung der Systemintegrität funktioniert, müssen Sie mindestens eine Regel hinzufügen. Eine *Regel für die Überwachung der Systemintegrität* ist eine Reihe von Kriterien, die den Zugriff von Benutzern auf Dateien und auf die Registrierung definieren. Die Überwachung der Systemintegrität erkennt Änderungen an Dateien und an der Registrierung innerhalb des angegebenen *Überwachungsbereichs*. Der Überwachungsbereich ist eines der Kriterien für eine Regel zur Überwachung der Systemintegrität.

Die Überwachung der Systemintegrität kann die folgenden Objekte überwachen:

- Dateien
- Registrierung
- Externe Geräte

Besonderheiten bei der Dateiüberwachung

Die Überwachung der Systemintegrität überwacht Änderungen an Dateien und Ordnern sowie an Dateien, die dem Überwachungsbereich hinzugefügt oder daraus entfernt werden. Diese Änderungen können auf eine Verletzung der Computersicherheit hinweisen. Wir empfehlen, selten geänderte Objekte oder Objekte hinzuzufügen, auf die nur der Administrator Zugriff hat. Dies hilft, die Anzahl der Ereignisse bei der Überwachung der Systemintegrität zu reduzieren.

Änderungen an Dateien in freigegebenen Ordnern des Servers werden nicht von der Überwachung der Systemintegrität kontrolliert. Die Überwachung der Systemintegrität kann nur lokal verwendet werden.

Kaspersky Endpoint Security überwacht die Änderungen an Dateien und Ordnern nur auf den Datenträgern, die beim Start der Echtzeitüberwachung der Systemintegrität verbunden waren. Wenn ein Datenträger beim Start der Echtzeitüberwachung der Systemintegrität nicht verbunden war, überwacht die App die Änderungen an Dateien und Ordnern auf diesem Datenträger nicht, selbst wenn die Dateien und Ordner zum Überwachungsbereich hinzugefügt wurden.

Besonderheiten bei der Überwachung der Registrierung

Die Überwachung der Systemintegrität überwacht die Registrierung. Diese Änderungen können auf eine Verletzung der Computersicherheit hinweisen.

Die Überwachung der Systemintegrität überwacht die folgenden Stammschlüssel der Registrierung:

- `HKCR`
- `HKLM`
- `HKU`
- `HKCC`
- `HKEY_CLASSES_ROOT`
- `HKEY_LOCAL_MACHINE`
- `HKEY_USERS`
- `HKEY_CURRENT_CONFIG` (nur in Echtzeit-Überwachung der Systemintegrität verfügbar)
- `HKEY_CURRENT_USER` (nur in Echtzeit-Überwachung der Systemintegrität verfügbar)

> Die Aufgabe *Prüfung der Systemintegrität* unterstützt den Schlüssel `HKEY_CURRENT_USER` nicht. Sie können einen Schlüssel unter `HKEY_USERS` als `HKEY_USERS\<user profile ID>\<key>` angeben.

Besonderheiten bei der Überwachung externer Geräte

Die Überwachung der Systemintegrität überwacht das Verbinden und Trennen externer Geräte. Dies ist erforderlich, um den Computer vor Sicherheitsbedrohungen zu schützen, die beim Dateiaustausch mit solchen Geräten bestehen können. Die Überwachung der Systemintegrität überwacht den Zugriff auf externe Geräte nicht und blockiert den Dateiaustausch nicht. Den Zugriff auf Geräte können Sie mithilfe der App-Komponente Gerätekontrolle konfigurieren.

> Wenn die Aufgabe *Baseline-Überwachung der Systemintegrität* ausgeführt wird, wird das erneute Verbinden externer Geräte ignoriert, falls die Geräte denselben Laufwerkbuchstaben im Betriebssystem haben. Damit Ereignisse protokolliert werden, müssen die erneut angeschlossenen Geräte unterschiedliche Laufwerkbuchstaben haben.

Die Überwachung der Systemintegrität überwacht die Verbindung die folgenden Typen von externen Geräten:

- Wechseldatenträger (einschließlich USB-Sticks)
- Festplatte

- Externer Netzwerkadapter
- CD/DVD-ROM/Blu-ray-Laufwerk
- Scanner/Kamera

Echtzeitüberwachung der Systemintegrität

Mit der Überwachung der Systemintegrität können Änderungen am Betriebssystem in Echtzeit verfolgt werden. Sie können Änderungen nachverfolgen, die auf Sicherheitslücken auf dem Computer hinweisen können. Die Komponente kann solche Änderungen blockieren oder nur entsprechende Ereignisse protokollieren.

Damit die Überwachung der Systemintegrität funktioniert, müssen Sie mindestens eine Regel hinzufügen. Eine *Regel für die Überwachung der Systemintegrität* ist eine Reihe von Kriterien, die den Zugriff von Benutzern auf Dateien und auf die Registrierung definieren. Die Überwachung der Systemintegrität erkennt Änderungen an Dateien und an der Registrierung innerhalb des angegebenen *Überwachungsbereichs*. Der Überwachungsbereich ist eines der Kriterien für eine Regel zur Überwachung der Systemintegrität.

Modi für die Echtzeitüberwachung der Systemintegrität

Sie müssen sicherstellen, dass die Regeln für die Überwachung der Systemintegrität keine Aktionen mit Ressourcen blockiert werden, die für das Betriebssystem oder andere Dienste wichtig sind. Darum wird empfohlen, den Testmodus zu aktivieren und die Auswirkungen der Komponente auf das System zu analysieren. Im Testmodus blockiert Kaspersky Endpoint Security keine Benutzeraktivitäten, die gemäß den Regeln verboten sind, sondern generiert Ereignisse des Typs *Warnung* ⚠.

Die Komponente „Echtzeitüberwachung der Systemintegrität“ verfügt über zwei Modi:

- Verbieten

  In diesem Modus verfolgt die Überwachung der Systemintegrität Änderungen im System und führt eine Aktion gemäß den Regeln aus: **Erlauben** oder **Blockieren**. Außerdem generiert die Überwachung der Systemintegrität ein entsprechendes Ereignis und ändert den Status des Geräts in der Kaspersky Security Center-Konsole.

- Informieren

  In diesem Modus erlaubt die Überwachung der Systemintegrität Aktionen mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich. Wenn die Aktion mit Dateien oder der Registrierung verboten ist, generiert das Programm ein Ereignis: *Der verbotene Vorgang wurde im Testmodus erlaubt*. Um zu analysieren, wie sich Regeln auf das System auswirken, können Sie sich die Berichte ansehen.

Echtzeitüberwachung der Systemintegrität aktivieren

So aktivieren Sie die Echtzeitüberwachung der Systemintegrität über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Überwachung der Systemintegrität** aus.

4. Aktivieren Sie das Kontrollkästchen **Überwachung der Systemintegrität**.

5. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Echtzeitüberwachung der Systemintegrität aus:

   - **Verbieten**. In diesem Modus blockiert die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis.

   - **Informieren**. In diesem Modus erlaubt die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis.

6. Aktivieren Sie im Block **Echtzeitüberwachung der Systemintegrität** das Kontrollkästchen **Echtzeitüberwachung der Systemintegrität**.

7. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.

   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ* ⓘ, *Warnung* ⚠, *Kritisch* ⓘ.

   Die Überwachung der Systemintegrität zeichnet aktuelle Verbindungen mit externen Geräten auf. Die App beginnt mit der Überwachung der Verbindung und Trennung externer Geräte, nachdem die Komponente in den App-Einstellungen aktiviert wurde. Wenn künftig ein externes Gerät angeschlossen oder getrennt wird, generiert die App ein entsprechendes Ereignis.

8. Konfigurieren Sie die Datei- und Registrierungsüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien und Registrierung überwachen**.

   b. Klicken Sie auf **Einstellungen**.

   Dadurch wird die Liste mit den Regeln für die Überwachung der Systemintegrität geöffnet.

   c. Klicken Sie auf **Hinzufügen**.

   Sie können auch Regeln aus einer anderen Quelle importieren.

   d. Konfigurieren Sie die Regel für die Überwachung der Systemintegrität (siehe folgende Tabelle).

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Echtzeitüberwachung der Systemintegrität über die Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle → Überwachung der Systemintegrität**.

5. Aktivieren Sie den Schalter **Überwachung der Systemintegrität AKTIVIERT**.

6. Wählen Sie die Registerkarte **Windows** aus.

7. Wählen Sie unter **Echtzeitüberwachung der Systemintegrität** einen Modus für die Echtzeitüberwachung der Systemintegrität aus:

   - **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.

8. Konfigurieren Sie die Datei- und Registrierungsüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien und Registrierung überwachen**.

   b. Klicken Sie auf **Regeln**.

      Dadurch wird die Liste mit den Regeln für die Überwachung der Systemintegrität geöffnet.

   c. Klicken Sie auf **Hinzufügen**.

      Sie können auch Regeln aus einer anderen Quelle importieren.

   d. Konfigurieren Sie die Regel für die Überwachung der Systemintegrität (siehe folgende Tabelle).

9. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.

   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Kritisch*.

   Die Überwachung der Systemintegrität zeichnet aktuelle Verbindungen mit externen Geräten auf. Die App beginnt mit der Überwachung der Verbindung und Trennung externer Geräte, nachdem die Komponente in den App-Einstellungen aktiviert wurde. Wenn künftig ein externes Gerät angeschlossen oder getrennt wird, generiert die App ein entsprechendes Ereignis.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie die Echtzeitüberwachung der Systemintegrität über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Überwachung der Systemintegrität** aus.

3. Aktivieren Sie den Schalter **Überwachung der Systemintegrität**.

4. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Echtzeitüberwachung der Systemintegrität aus:

   - **Verbieten**. In diesem Modus blockiert die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis.

   - **Informieren**. In diesem Modus erlaubt die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis.

5. Aktivieren Sie im Block **Echtzeitüberwachung der Systemintegrität** das Kontrollkästchen **Echtzeitüberwachung der Systemintegrität**.

6. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.

   b. Wählen Sie in der Dropdown-Liste **Signifikanz von Ereignissen** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ* ⓘ, *Warnung* ⚠, *Kritisch* ⓘ.

   Die Überwachung der Systemintegrität zeichnet aktuelle Verbindungen mit externen Geräten auf. Die App beginnt mit der Überwachung der Verbindung und Trennung externer Geräte, nachdem die Komponente in den App-Einstellungen aktiviert wurde. Wenn künftig ein externes Gerät angeschlossen oder getrennt wird, generiert die App ein entsprechendes Ereignis.

7. Konfigurieren Sie die Datei- und Registrierungsüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien und Registrierung überwachen**.

   b. Klicken Sie auf **Einrichten**.

   Dadurch wird die Liste mit den Regeln für die Überwachung der Systemintegrität geöffnet.

   c. Klicken Sie auf **Hinzufügen**.

   Sie können auch Regeln aus einer anderen Quelle importieren.

8. Konfigurieren Sie die Regel für die Überwachung der Systemintegrität (siehe folgende Tabelle).

9. Speichern Sie die vorgenommenen Änderungen.

Einstellungen einer Regel für die Echtzeitüberwachung der Systemintegrität

Einstellung	Beschreibung
Regelname	Name der Regel für die Echtzeitüberwachung der Systemintegrität
Vorgänge mit Dateien und Registrierung	• **Erlauben**. Die Überwachung der Systemintegrität erlaubt Aktionen mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich. • **Blockieren**. Der ausgewählte Modus bestimmt, wie sich die Überwachung der Systemintegrität verhält. Wenn Sie den *Systemschutzmodus* ausgewählt haben, blockiert die Überwachung der Systemintegrität Aktionen mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich, generiert ein entsprechendes Ereignis und ändert den Status des Geräts in der Kaspersky Security Center-Konsole. Wenn Sie den *Testmodus* ausgewählt haben, erlaubt die Überwachung der Systemintegrität Aktionen mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich.

Einstellung	Beschreibung
Signifikanz von Ereignissen	Kaspersky Endpoint Security protokolliert Dateiänderungsereignisse, wenn eine Datei oder ein Registrierungsschlüssel im Überwachungsbereich geändert wird. Es gibt folgende Prioritätsstufen für Ereignisse: *Informativ*, *Warnung*, *Kritisch*.

Überwachungsbereich	• **Datei**. Liste der Dateien und Ordner, die von der Komponente überwacht werden. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
	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` funktioniert nicht.
	  • 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.
	• **Registrierung**. Liste der Registrierungsschlüssel und -werte, die von der Komponente überwacht werden. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Ausnahmen	• **Datei**. Liste der Ausnahmen vom Überwachungsbereich. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. Beispiel: `C:\Folder\Application\*.log`. Ausnahmeneinträge haben eine höhere Priorität als Einträge im Überwachungsbereich.
	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` funktioniert nicht.
	  • 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.
	• **Registrierung**. Liste der Ausnahmen vom Überwachungsbereich. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. Ausnahmeneinträge haben eine höhere Priorität als Einträge im Überwachungsbereich.

Vertrauenswürdige Benutzer und/oder Benutzergruppen	Ein *vertrauenswürdiger Benutzer* ist ein Benutzer, der Aktionen mit Dateien und Registrierungsschlüsseln im Überwachungsbereich ausführen darf. Wenn Kaspersky Endpoint Security eine Aktion erkennt, die von einem vertrauenswürdigen Benutzer ausgeführt wurde, generiert die Überwachung der Systemintegrität ein Ereignis des Typs *Informativ*. Sie können Benutzer in Active Directory, in der Liste für Benutzerkonten in Kaspersky Security Center oder durch manuelle Eingabe eines lokalen Benutzernamens auswählen. Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können.
Markierungen für Dateivorgänge / Überwachte Vorgänge	Markierungen, die die Aktion mit Dateien oder Registrierungsschlüsseln charakterisieren, die von der App überwacht werden.
Hashing	Berechnung des Datei-Hashs bei einer Änderung. Kaspersky Endpoint Security fügt Informationen über den Hash der Datei hinzu, wenn ein Ereignis generiert wird.

Prüfung der Systemintegrität auf Befehl

Die Aufgabe zur Prüfung der Systemintegrität auf Befehl können Sie manuell oder nach einem Zeitplan ausführen. Wenn die Aufgabe *Prüfung der Systemintegrität* ausgeführt wird, vergleicht die App den aktuellen Status der Objekte, die zum Überwachungsbereich gehören, mit ihrem *Baseline*-Status. Im Gegensatz zur Echtzeitüberwachung der Systemintegrität können Sie mit der Aufgabe *Prüfung der Systemintegrität* die Anzahl der Ereignisse begrenzen und einen Gesamtbericht über die Änderungen im Betriebssystem erstellen.

Damit die Überwachung der Systemintegrität funktioniert, müssen Sie mindestens eine Regel hinzufügen. Eine *Regel für die Überwachung der Systemintegrität* ist eine Reihe von Kriterien, die den Zugriff von Benutzern auf Dateien und auf die Registrierung definieren. Die Überwachung der Systemintegrität erkennt Änderungen an Dateien und an der Registrierung innerhalb des angegebenen *Überwachungsbereichs*. Der Überwachungsbereich ist eines der Kriterien für eine Regel zur Überwachung der Systemintegrität. Sie können Regeln konfigurieren, die sowohl von der Echtzeitüberwachung der Systemintegrität als auch von der Aufgabe *Prüfung der Systemintegrität* verwendet werden, oder Sie können separate Regeln für die Aufgabe erstellen. Um eine Baseline zu erstellen, wendet Kaspersky Endpoint Security den Überwachungsbereich der Aufgabe *Prüfung der Systemintegrität* auf die Aufgabe *Baseline-Update* an.

Baseline erstellen und aktualisieren

Die Aufgabe *Prüfung der Systemintegrität* erfordert eine Baseline, damit sie funktioniert. Eine *Baseline* ist ein aufgezeichneter Zustand von Objekten im System, den die App beim Vergleich mit dem aktuellen Zustand als Referenz verwendet. Unterscheidet sich der aktuelle Systemstatus von dem in der Baseline aufgezeichneten Systemstatus, generiert Kaspersky Endpoint Security ein entsprechendes Ereignis. Sie können eine Baseline mithilfe der Aufgabe *Baseline-Update* erstellen oder aktualisieren.

Sie können die Baseline in den folgenden Modi aktualisieren:

- Vollständiges Update.

  Die App aktualisiert alle Objekte im Überwachungsbereich.

- Inkrementelles Update.

  Die App erkennt und aktualisiert nur geänderte oder neue Objekte.

So erstellen oder aktualisieren Sie eine Baseline über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Baseline-Update** aus.

Schritt 2. Baseline-Update-Modus auswählen

Wählen Sie einen Baseline-Update-Modus aus:

- **Vollständiges Update**. Die App aktualisiert alle Objekte im Überwachungsbereich.
- **Inkrementelles Update**. Die App erkennt und aktualisiert nur geänderte oder neue Objekte.

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Aufgabennamen festlegen

Geben Sie den Namen der Aufgabe ein, z. B. *Baseline 2024*.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So erstellen oder aktualisieren Sie eine Baseline über die Web Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Baseline-Update**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Baseline 2024*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Wählen Sie einen Baseline-Update-Modus aus:

   - **Vollständiges Update**. Die App aktualisiert alle Objekte im Überwachungsbereich.
   - **Inkrementelles Update**. Die App erkennt und aktualisiert nur geänderte oder neue Objekte.

10. Speichern Sie die vorgenommenen Änderungen.

11. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

12. Klicken Sie auf **Starten**.

Überwachungsbereich für die Aufgabe Prüfung der Systemintegrität konfigurieren

Standardmäßig ist der Überwachungsbereich der Aufgabe *Prüfung der Systemintegrität* identisch mit dem Überwachungsbereich der Echtzeitüberwachung der Systemintegrität. Sie können einen anderen Überwachungsbereich für die Aufgabe konfigurieren.

Der Import der Schlüssel `HKEY_CURRENT_USER` und `HKEY_CURRENT_CONFIG` für die Aufgabe *Prüfung der Systemintegrität* wird durch die Überwachung der Systemintegrität nicht unterstützt. Wenn diese Schlüssel zum Überwachungsbereich der Aufgabe gehören, generiert das Programm das Ereignis *Der Überwachungsbereich enthält ungültige Objekte*.

So konfigurieren Sie über die Verwaltungskonsole (MMC) einen anderen Überwachungsbereich für die Aufgabe Prüfung der Systemintegrität

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Überwachung der Systemintegrität** aus.
4. Aktivieren Sie das Kontrollkästchen **Überwachung der Systemintegrität**.
5. Wählen Sie unter **Prüfung der Systemintegrität** den Konfigurationsmodus der Aufgabe aus: **Benutzerdefinierte Einstellungen**.
6. Konfigurieren Sie die Überwachung externer Geräte:
   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.
   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Kritisch*.

   Die Überwachung der Systemintegrität zeichnet Informationen darüber auf, welche externen Geräte zum Zeitpunkt der Baseline-Erstellung verbunden waren. Wenn ein externes Gerät später verbunden wird, generiert die App ein entsprechendes Ereignis. Wenn die Aufgabe *Prüfung der Systemintegrität* ausgeführt wird, wird das Trennen externer Geräte nicht überwacht.
7. Konfigurieren Sie die Datei- und Registrierungsüberwachung:
   a. Aktivieren Sie das Kontrollkästchen **Dateien und Registrierung überwachen**.
   b. Klicken Sie auf **Einstellungen**.

      Dadurch wird die Liste mit den Regeln für die Überwachung der Systemintegrität geöffnet.
   c. Klicken Sie auf **Hinzufügen**.

      Sie können auch Regeln aus einer anderen Quelle importieren.
   d. Konfigurieren Sie die Regel für die Überwachung der Systemintegrität (siehe folgende Tabelle).
8. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die Web Console einen anderen Überwachungsbereich für die Aufgabe Prüfung der Systemintegrität

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Sicherheitskontrolle → Überwachung der Systemintegrität**.
5. Wählen Sie die Registerkarte **Windows** aus.

6. Aktivieren Sie den Schalter **Überwachung der Systemintegrität AKTIVIERT**.

7. Wählen Sie unter **Prüfung der Systemintegrität** den Konfigurationsmodus der Aufgabe aus: **Benutzerdefinierte Einstellungen**.

8. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.

   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ* ⓘ, *Warnung* ⚠, *Kritisch* ⓘ.

   Die Überwachung der Systemintegrität zeichnet Informationen darüber auf, welche externen Geräte zum Zeitpunkt der Baseline-Erstellung verbunden waren. Wenn ein externes Gerät später verbunden wird, generiert die App ein entsprechendes Ereignis. Wenn die Aufgabe *Prüfung der Systemintegrität* ausgeführt wird, wird das Trennen externer Geräte nicht überwacht.

9. Konfigurieren Sie die Datei- und Registrierungsüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien und Registrierung überwachen**.

   b. Klicken Sie auf **Regeln**.

   Dadurch wird die Liste mit den Regeln für die Überwachung der Systemintegrität geöffnet.

   c. Klicken Sie auf **Hinzufügen**.

   Sie können auch Regeln aus einer anderen Quelle importieren.

   d. Konfigurieren Sie die Regel für die Überwachung der Systemintegrität (siehe folgende Tabelle).

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die App-Benutzeroberfläche einen anderen Überwachungsbereich für die Aufgabe Prüfung der Systemintegrität

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Sicherheitskontrolle → Überwachung der Systemintegrität** aus.

3. Aktivieren Sie den Schalter **Überwachung der Systemintegrität**.

4. Wählen Sie unter **Prüfung der Systemintegrität** den Konfigurationsmodus der Aufgabe aus: **Benutzerdefinierte Einstellungen**.

5. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.

   b. Wählen Sie in der Dropdown-Liste **Signifikanz von Ereignissen** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ* ⓘ, *Warnung* ⚠, *Kritisch* ⓘ.

   Die Überwachung der Systemintegrität zeichnet Informationen darüber auf, welche externen Geräte zum Zeitpunkt der Baseline-Erstellung verbunden waren. Wenn ein externes Gerät später verbunden wird, generiert die App ein entsprechendes Ereignis. Wenn die Aufgabe *Prüfung der Systemintegrität* ausgeführt wird, wird das Trennen externer Geräte nicht überwacht.

6. Konfigurieren Sie die Datei- und Registrierungsüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien und Registrierung überwachen**.

   b. Klicken Sie auf **Einrichten**.

      Dadurch wird die Liste mit den Regeln für die Überwachung der Systemintegrität geöffnet.

   c. Klicken Sie auf **Hinzufügen**.

      Sie können auch Regeln aus einer anderen Quelle importieren.

   d. Konfigurieren Sie die Regel für die Überwachung der Systemintegrität (siehe folgende Tabelle).

7. Speichern Sie die vorgenommenen Änderungen.

Einstellungen einer Regel für die Aufgabe Prüfung der Systemintegrität

Einstellung	Beschreibung
Regelname	Name der Regel für die Aufgabe *Prüfung der Systemintegrität*.
Signifikanz von Ereignissen	Kaspersky Endpoint Security protokolliert Dateiänderungsereignisse, wenn eine Datei oder ein Registrierungsschlüssel im Überwachungsbereich geändert wird. Es gibt folgende Prioritätsstufen für Ereignisse: *Informativ*, *Warnung*, *Kritisch*.

Überwachungsbereich	• **Datei**. Liste der Dateien und Ordner, die von der Komponente überwacht werden. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
	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` funktioniert nicht.
	  • 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.
	• **Registrierung**. Liste der Registrierungsschlüssel und -werte, die von der Komponente überwacht werden. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske.

Ausnahmen	• **Datei**. Liste der Ausnahmen vom Überwachungsbereich. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. Beispiel: `C:\Folder\Application\*.log`. Ausnahmeneinträge haben eine höhere Priorität als Einträge im Überwachungsbereich.
	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` funktioniert nicht.
	  • 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.
	• **Registrierung**. Liste der Ausnahmen vom Überwachungsbereich. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. Ausnahmeneinträge haben eine höhere Priorität als Einträge im Überwachungsbereich.

Aufgabe Prüfung der Systemintegrität starten

Die Aufgabe *Prüfung der Systemintegrität* ermöglicht es, Dateien oder Registrierungsschlüssel auf Änderungen zu überprüfen und das Verbinden externer Geräte zu überprüfen. Um Dateien auf Änderungen zu überprüfen, können Sie die Aufgabe *Prüfung der Systemintegrität* in den folgenden Modi ausführen:

- Schnelle Untersuchung.

  Wenn Dateien auf Änderungen überprüft werden, untersucht die App nur Dateiattribute. Inhalte von Dateien werden von der App nicht untersucht.

- Vollständige Untersuchung.

  Wenn Dateien auf Änderungen überprüft werden, untersucht die App alle Dateiattribute und die Inhalte von Dateien.

Der Ausführungsmodus der Aufgabe hat keinen Einfluss auf die Überprüfung der Registrierung oder externer Geräte.

So führen Sie die Aufgabe Prüfung der Systemintegrität über die Verwaltungskonsole (MMC) aus

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
3. Klicken Sie auf **Neue Aufgabe**.

   Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.
4. Wählen Sie **Kaspersky Endpoint Security → Baseline-Überwachung der Systemintegrität** aus. Wählen Sie einen Modus für die Überwachung der Systemintegrität aus:

   - **Vollständige Untersuchung**. In diesem Modus überprüft das Programm alle Attribute und Hashes von Dateien.
   - **Schnelle Untersuchung**. In diesem Modus überprüft das Programm nur die Attribute von Dateien.
5. Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

   - Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – nicht zugeordnete Geräte. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
   - Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.
   - Geben Sie die Geräte an, für die Sie die Aufgabe ausführen möchten.
   - Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
6. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.
7. Konfigurieren Sie einen Zeitplan für den Aufgabenstart, z. B. manuell oder an einem bestimmten Wochentag.
8. Geben Sie einen Namen für die Aufgabe ein.
9. Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So führen Sie die Aufgabe Prüfung der Systemintegrität über die Web Console aus

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Prüfung der Systemintegrität**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Wöchentliche Prüfung der Systemintegrität*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Wählen Sie einen Modus für die Prüfung der Systemintegrität aus:

   - **Schnelle Untersuchung**. Die App überprüft nur Dateiattribute. Inhalte von Dateien werden von der App nicht untersucht.

   - **Vollständige Untersuchung**. Die App überprüft alle Dateiattribute sowie die Inhalte von Dateien.

10. Speichern Sie die vorgenommenen Änderungen.

11. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

12. Klicken Sie auf **Starten**.

Damit die Aufgabe *Prüfung der Systemintegrität* erfolgreich abgeschlossen werden kann, muss der Überwachungsbereich der Aufgabe *Prüfung der Systemintegrität* vollständig mit der Baseline übereinstimmen. Wenn sich der Überwachungsbereich unterscheidet, wird die Aufgabe mit einem Fehler beendet. Um die Überwachungsbereiche zu synchronisieren, führen Sie die Aufgabe *Baseline-Update* mit einem neuen Überwachungsbereich aus.

Regeln für die Überwachung der Systemintegrität exportieren und importieren

Sie können die Liste der Regeln für die Überwachung der Systemintegrität in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Einträgen desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie ein Backup für die Liste mit den Regeln der Überwachung der Systemintegrität anlegen oder die Liste auf einen anderen Server migrieren.

Der Import der Schlüssel `HKEY_CURRENT_USER` und `HKEY_CURRENT_CONFIG` für die Aufgabe *Prüfung der Systemintegrität* wird durch die Überwachung der Systemintegrität nicht unterstützt. Wenn diese Schlüssel zum Überwachungsbereich der Aufgabe gehören, generiert das Programm das Ereignis *Der Überwachungsbereich enthält ungültige Objekte*.

Exportieren und importieren einer Liste mit Regeln für die Überwachung der Systemintegrität über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Sicherheitskontrolle → Überwachung der Systemintegrität** aus.
4. So exportieren oder importieren Sie Regeln für die *Echtzeitüberwachung der Systemintegrität*:
   a. Klicken Sie im Block **Echtzeitüberwachung der Systemintegrität** auf **Einstellungen**.
   b. So exportieren Sie eine Liste mit Regeln für die Echtzeitüberwachung der Systemintegrität:
      1. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.
         Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.
      2. Klicken Sie auf den Link **Exportieren**.
      3. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
      4. Speichern Sie die Datei.
         Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.
   c. So importieren Sie Regeln für die Echtzeitüberwachung der Systemintegrität:
      1. Klicken Sie auf den Link **Importieren**.
         Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

2. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

5. So exportieren oder importieren Sie Regeln für die *Prüfung der Systemintegrität*:

   a. Wählen Sie im Block **Prüfung der Systemintegrität** die Variante **Benutzerdefinierte Einstellungen** aus.

   b. Klicken Sie auf **Einstellungen**.

   c. So exportieren Sie die Liste mit Regeln für die Prüfung der Systemintegrität:

      1. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

         Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.

      2. Klicken Sie auf den Link **Exportieren**.

      3. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

      4. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.

   d. So importieren Sie eine Liste mit Regeln für die Prüfung der Systemintegrität:

      1. Klicken Sie auf den Link **Importieren**.

         Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

      2. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

6. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste mit Regeln für die Überwachung der Systemintegrität (in der Web Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Sicherheitskontrolle → Überwachung der Systemintegrität**.

5. Wählen Sie die Registerkarte **Windows** aus.

6. So exportieren oder importieren Sie Regeln für die *Echtzeitüberwachung der Systemintegrität*:

   a. Klicken Sie im Block **Echtzeitüberwachung der Systemintegrität** auf den Link **Regeln**.

   b. So exportieren Sie eine Liste mit Regeln für die Echtzeitüberwachung der Systemintegrität:

      1. Wählen Sie die Regeln, die Sie exportieren möchten.

      2. Klicken Sie auf die Schaltfläche → **Exportieren**.

         Kaspersky Endpoint Security exportiert die Liste der Regeln in eine json-Datei im standardmäßigen Download-Ordner.

   c. So importieren Sie Regeln für die Echtzeitüberwachung der Systemintegrität:

      1. Klicken Sie auf die Schaltfläche → **Import**.

         Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der vertrauenswürdigen Adressen importieren möchten.

      2. Öffnen Sie die Datei.

         Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.

7. So exportieren oder importieren Sie Regeln für die *Prüfung der Systemintegrität*:

   a. Wählen Sie im Block **Prüfung der Systemintegrität auf Befehl** die Variante **Benutzerdefinierte Einstellungen** aus.

   b. Klicken Sie auf den Link **Regeln**.

   c. So exportieren Sie die Liste mit Regeln für die Prüfung der Systemintegrität:

      1. Wählen Sie die Regeln, die Sie exportieren möchten.

      2. Klicken Sie auf die Schaltfläche → **Exportieren**.

         Kaspersky Endpoint Security exportiert die Liste der Regeln in eine json-Datei im standardmäßigen Download-Ordner.

   d. So importieren Sie eine Liste mit Regeln für die Prüfung der Systemintegrität:

      1. Klicken Sie auf die Schaltfläche → **Import**.

         Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der vertrauenswürdigen Adressen importieren möchten.

      2. Öffnen Sie die Datei.

         Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

Berichte zur Überwachung der Systemintegrität anzeigen

Um die Leistung der Regeln für die Überwachung der Systemintegrität zu analysieren, können Sie die von der App erstellten Berichte und Ereignisse zurate ziehen. Kaspersky Endpoint Security erstellt die folgenden Berichte über die Komponente:

- In der App-Benutzeroberfläche:
  - Bericht zur Überwachung der Systemintegrität
  - Bericht zur Prüfung der Systemintegrität
  - Bericht zum Baseline-Update

  Diese Berichte enthalten Ereignisse der Überwachung der Systemintegrität.
- Berichte in der Kaspersky Security Center-Konsole:
  - Bericht über Computer, auf denen Überwachungsregeln am häufigsten ausgelöst wurden
  - Bericht über die Überwachungsregeln, die am häufigsten ausgelöst wurden

  Standardmäßig umfasst ein Bericht die letzten 30 Tage, einschließlich des Datums der Berichterstellung.

  So zeigen Sie in der Verwaltungskonsole (MMC) Berichte zur Überwachung der Systemintegrität an

  1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
  2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte** aus.
  3. Klicken Sie auf **Neue Berichtsvorlage**.

     Der „Assistent für das Erstellen einer Berichtsvorlage“ wird gestartet.
  4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie beim Schritt **Typ der Berichtsvorlage auswählen** einen Bericht zur Überwachung der Systemintegrität aus (Abschnitt **Andere**):
     - **Die 10 Geräte, auf denen die Regeln zur Überwachung der Dateiintegrität bzw. zur Überwachung der Systemintegrität am häufigsten ausgelöst wurden**.
     - **Die 10 Regeln zur Überwachung der Dateiintegrität bzw. zur Überwachung der Systemintegrität, die auf den Geräten am häufigsten ausgelöst wurden**.

     Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.
  5. Öffnen Sie den Bericht durch Doppelklick.

  Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

So zeigen Sie in der Web Console Berichte zur Überwachung der Systemintegrität an

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Überwachung** → **Berichte** aus.
2. Klicken Sie auf **Hinzufügen**.

   Der „Assistent für das Erstellen einer Berichtsvorlage“ wird gestartet.
3. Wählen Sie unter **Vorlagentyp** im Abschnitt **Sonstige** einen Bericht zur Überwachung der Systemintegrität aus:

   - **Die 10 Geräte, auf denen die Regeln zur Überwachung der Dateiintegrität bzw. zur Überwachung der Systemintegrität am häufigsten ausgelöst wurden**.
   - **Die 10 Regeln zur Überwachung der Dateiintegrität bzw. zur Überwachung der Systemintegrität, die auf den Geräten am häufigsten ausgelöst wurden**.

   Nachdem der Assistent für das Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle.
4. Wählen Sie den Bericht aus und führen Sie ihn aus.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Um von der App generierte Ereignisse anzuzeigen, können Sie auch die Ereignisauswahlen in der Kaspersky Security Center-Konsole verwenden.

Status der Systemintegrität zurücksetzen

In der Kaspersky Security Center-Konsole können Computer einen der folgenden Statuswerte haben: *OK*, *Warnung* oder *Kritisch*. Wenn die Überwachung der Systemintegrität eine Änderung an Dateien oder Registrierungsschlüsseln im Überwachungsbereich erkennt, ändert sich der Status des Computers in *Warnung* oder *Kritisch*. Der von der Überwachung der Systemintegrität zugewiesene Status heißt *Status der Systemintegrität*. Sie können den Status der Systemintegrität beispielsweise zurücksetzen, wenn Sie aufgrund einer Analyse davon überzeugt sind, dass die gefundene Änderung an Objekten die Sicherheit des Computers nicht beeinträchtigt.

So setzen Sie den Status der Systemintegrität über die Verwaltungskonsole (MMC) zurück

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Status der Systemintegrität zurücksetzen** aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Zeitplan des Aufgabenstarts anpassen

Konfigurieren Sie den Aufgabenzeitplan, z. B. mit der Option „manuell“.

Schritt 4. Aufgabennamen festlegen

Geben Sie den Namen der Aufgabe ein, z. B. *Status zurücksetzen nach Änderung des Überwachungsbereichs*.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So setzen Sie den Status der Systemintegrität über die Web Console zurück

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Status der Systemintegrität zurücksetzen**.

c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, z. B. *Status zurücksetzen nach Änderung des Überwachungsbereichs*.

d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Endpoint Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

8. Klicken Sie auf **Starten**.

Wenn sich der Computerstatus aufgrund von Ereignissen bei der Überwachung der Systemintegrität in *Warnung* oder *Kritisch* geändert hat, wird der Status des Computers auf *OK* zurückgesetzt. Wenn sich der Computerstatus auch aufgrund anderer Ereignisse geändert hat, bleibt der Status des Computers unverändert.

Cloud Discovery

Cloud Discovery verwaltet den Benutzerzugriff auf Cloud-Dienste. Solche Cloud-Dienste sind beispielsweise Microsoft Teams, Salesforce und Microsoft Office 365. Cloud-Dienste sind nach Kategorien angeordnet, z. B. *Filehosting-Anbieter*, *Messenger*, *E-Mail*. Die Kaspersky-Experten aktualisieren die Cloud Discovery-Kategorien und die in den Kategorien enthaltenen Cloud-Dienste regelmäßig. Kaspersky Endpoint Security aktualisiert die Auswahl von Kategorien und Cloud-Diensten zusammen mit den App-Datenbanken. Das bedeutet: Cloud Discovery verwendet Kaspersky Security Network nicht zur Kategorisierung von Cloud-Diensten.

Cloud Discovery bietet die folgende Funktionalität:

- Überwachung der Nutzung von Cloud-Diensten
- Sperrung des Benutzerzugriffs auf Cloud-Dienste

Systemanforderungen

Cloud Discovery ist verfügbar, wenn die folgenden Bedingungen erfüllt sind:

- Die Anwendung ist auf einem Computer mit Windows für Workstations installiert.

  Sie Komponente ist nicht für Server verfügbar.

- Kaspersky Security Center Version 15.1 oder höher.

  Die Komponente ist in der Verwaltungskonsole (MMC) nicht verfügbar. Sie können Cloud Discovery in Kaspersky Security Center Web Console und Kaspersky Security Center Cloud Console konfigurieren.

- Lizenz für Kaspersky Next.

Aktivieren Sie die Programmfunktionalität, die für die Cloud Discovery-Komponente erforderlich ist:

1. **Verschlüsselte Verbindungen untersuchen**. Diese Funktionalität ist für die Überwachung des HTTPS-Datenverkehrs erforderlich. Diese Funktionalität können Sie im Abschnitt **Netzwerkeinstellungen** verwalten.

2. **Skript zur Interaktion mit Webseiten in den Web-Datenverkehr einbinden**. Das Skript ermöglicht die Registrierung von Cloud Discovery-Ereignissen. Das Skript gewährleistet die voll funktionsfähige Sperrung des Zugriffs auf Cloud-Dienste. Ohne das Skript sperrt die App den Zugriff nur nach den Domänen von Cloud-Diensten. Diese Funktionalität können Sie im Abschnitt **Netzwerkeinstellungen** verwalten.

Sie können auch die Funktionalität **Das Öffnen erlaubter Seiten protokollieren** aktivieren. Die Funktionalität bietet die Gruppierung von Ereignissen, wenn ein Benutzer Webseiten besucht, die zu derselben Domäne gehören. Wenn ein Benutzer einen Cloud-Dienst verwendet, protokolliert Cloud Discovery nur ein einziges Ereignis und nicht mehrere Ereignisse für jede einzelne Webseite. Diese Funktionalität können Sie im Abschnitt **Web-Kontrolle** verwalten.

Überwachung von Cloud-Diensten

Wenn ein Benutzer mit der Nutzung eines Cloud-Dienstes beginnt, registriert Kaspersky Endpoint Security dieses Ereignis und erstellt einen Eintrag im Bericht. Cloud Discovery kontrolliert die Cloud-Dienst-Nutzung sowohl im Browser als auch in entsprechenden Anwendungen. Cloud Discovery kontrolliert die Cloud-Dienst-Nutzung über HTTP und HTTPS.

So aktivieren Sie die Überwachung von Cloud-Diensten in Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kommunikations- und Web-Schutz → Cloud Discovery**.

5. Aktivieren Sie den Schalter **Cloud Discovery AKTIVIERT**.

6. Speichern Sie die vorgenommenen Änderungen.

Dadurch übermittelt die Anwendung Informationen über die genutzten Cloud-Dienste an Kaspersky Security Center. Sie können Informationen zur Cloud-Dienst-Nutzung in Berichten einsehen. Falls erforderlich, können Sie den Zugriff auf Cloud-Dienste sperren.

Sperrung des Zugriffs auf Cloud-Dienste

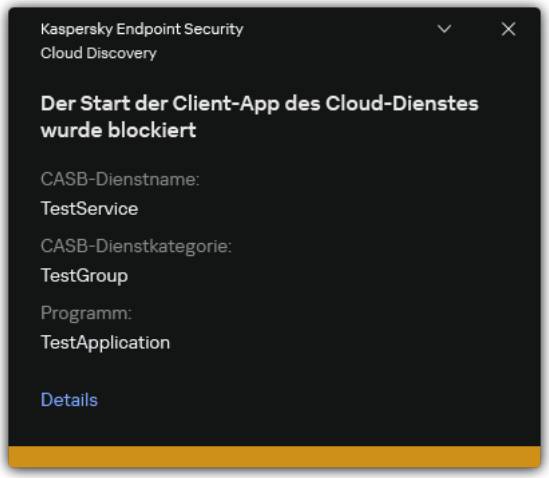
Die Sperrung des Zugriffs auf Cloud-Dienste ist nur im Rahmen der Kaspersky Next EDR Optimum- und XDR Expert-Lizenz verfügbar. Diese Funktion ist für die Lizenz „Kaspersky Next EDR Foundations“ nicht verfügbar. Einen Vergleich der Programmfunktionalität unter Berücksichtigung des Kaspersky Next-Lizenztyps finden Sie in der Hilfe zu Kaspersky Next.

Der Administrator kann den Benutzerzugriff auf Cloud Discovery-Kategorien oder auf individuelle Cloud-Dienste beschränken. Der Administrator kann beispielsweise nur sichere Cloud-Dienste zulassen und dadurch Datenlecks verhindern. In Cloud Discovery werden für jeden Cloud-Dienst *Informationen zur Risikostufe* angezeigt. Anhand der Risikostufe lassen sich Dienste identifizieren, welche die Sicherheitsanforderungen des Unternehmens nicht erfüllen.

Die Risikostufe ist ein geschätzter Wert und gibt keine Auskunft über die Qualität des Cloud-Dienstes oder dessen Hersteller. Die Risikostufe ist nur eine Empfehlung der Kaspersky-Experten.

Risikostufen von Cloud-Diensten werden im Abschnitt **Cloud Discovery** der Richtlinie in der Liste aller kontrollierten Cloud-Dienste angezeigt.

Andere Komponenten von Kaspersky Endpoint Security schützen vor Bedrohungen und verfolgen verdächtige Benutzeraktivitäten während der Nutzung von Cloud-Diensten.



Cloud Discovery-Benachrichtigung

Cloud-Anwendungen, die vor Kaspersky Endpoint Security gestartet wurden, werden von Cloud Discovery nicht gesperrt.

So sperren Sie den Zugriff auf Cloud-Dienste über die Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kommunikations- und Web-Schutz** → **Cloud Discovery**.
5. Aktivieren Sie den Schalter **Cloud Discovery AKTIVIERT**.

   Eine Liste der Cloud-Dienste wird angezeigt. Cloud-Dienste sind nach Kategorien angeordnet, z. B. *Filehosting-Anbieter*, *Messenger*, *E-Mail*. Die Kaspersky-Experten aktualisieren die Cloud Discovery-Kategorien und die in den Kategorien enthaltenen Cloud-Dienste regelmäßig. Kaspersky Endpoint Security aktualisiert die Auswahl von Kategorien und Cloud-Diensten zusammen mit den App-Datenbanken.

6. Verwenden Sie den Schalter in der Spalte **Zugriff**, um den Zugriff auf Cloud-Dienste zu konfigurieren.

7. Speichern Sie die vorgenommenen Änderungen.

Dadurch kontrolliert die Anwendung die Cloud-Dienst-Nutzung sowohl im Browser als auch in entsprechenden Anwendungen.

Vertrauenswürdige Zone

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Endpoint Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt.

Die vertrauenswürdige Zone wird manuell vom Systemadministrator angelegt. Berücksichtigt werden dabei die Besonderheiten von Objekten, die für die Arbeit erforderlich sind, sowie die Programme, die auf dem Computer installiert sind. Die Aufnahme von Objekten und Programmen in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Endpoint Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt oder Programm unschädlich ist. Ein Administrator kann einem Benutzer auch erlauben, seine eigene lokale vertrauenswürdige Zone für einen bestimmten Computer zu erstellen. Auf diese Weise können Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen.

Ab Kaspersky Endpoint Security 12.5 für Windows können Sie EDR-Telemetrie zur vertrauenswürdigen Zone hinzufügen. Dadurch können die Daten optimiert werden, die das Programm an den Telemetrie-Erfassungsserver für die Lösung Kaspersky Anti Targeted Attack Platform (EDR) sendet.

Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen.

Ab Kaspersky Endpoint Security 12.8 für Windows können Sie das Programm im Light Agent-Modus installieren, um virtuelle Umgebungen zu schützen. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren.

Erstellung von Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Endpoint Security ein Objekt nicht auf Viren und andere bedrohliche Programme. Die Untersuchungsausnahmen ermöglichen es, sicher mit legitimen Programmen zu arbeiten, mit denen Angreifer einen 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.

Derartige Programme können bei der Ausführung von Kaspersky Endpoint Security gesperrt werden. Sie können Untersuchungsausnahmen anpassen, um eine Sperrung von notwendigen Programmen zu verhindern. Dazu muss der vertrauenswürdigen Zone der Name oder eine Namensmaske hinzugefügt werden, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht. Es kann beispielsweise sein, dass Sie häufig mit dem Programm Radmin, zur Remote-Administration von Computern. Eine solche Programmaktivität wird von Kaspersky Endpoint Security als schädlich eingestuft und kann blockiert werden. Um zu verhindern, dass ein Programm gesperrt wird, muss eine Untersuchungsausnahme erstellt werden. In dieser Ausnahme wird ein Name oder eine Namensmaske angegeben, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht.

Ein auf Ihrem Computer installiertes Programm, das Informationen sammelt und zur Verarbeitung weiterleitet, kann von Kaspersky Endpoint Security als schädlich eingestuft werden. Um dies zu vermeiden, können Sie das Programm von der Untersuchung ausschließen. Dazu können Sie Kaspersky Endpoint Security entsprechend anpassen, wie in dieser Dokumentation beschrieben.

Untersuchungsausnahmen können von folgenden Komponenten und Programmaufgaben verwendet werden, die vom Systemadministrator erstellt wurden:

- Verhaltensanalyse.
- Exploit-Prävention.
- Programm-Überwachung.
- Schutz vor bedrohlichen Dateien.
- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.
- Aufgaben für die *Schadsoftware-Untersuchung*

Ein Objekt wird nicht von Kaspersky Endpoint Security untersucht, wenn beim Start einer Untersuchungsaufgabe das Laufwerk, auf dem sich das Objekt befindet, oder der Ordner, in dem sich das Objekt befindet, zum Untersuchungsbereich gehört. Wenn jedoch beim Start einer benutzerdefinierten Untersuchungsaufgabe dieses Objekt ausdrücklich ausgewählt wird, so bleibt die Untersuchungsausnahme unberücksichtigt.

So erstellen Sie eine Untersuchungsausnahme in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
5. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme → Untersuchungsausnahmen** auf **Einstellungen**.

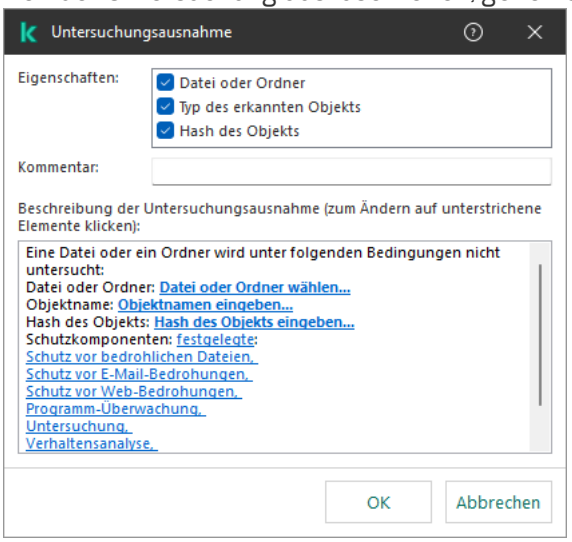
   Dies öffnet ein Fenster mit einer Liste der Ausnahmen.
6. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.
7. Markieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn dieses Kontrollkästchen deaktiviert ist, blendet Kaspersky Endpoint Security die konsolidierte Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus.

8. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

- **Kategorie**. Sie können Untersuchungsausnahmen in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens eine Untersuchungsausnahme hinzu.
- **Neue Ausnahme**. Kaspersky Endpoint Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.
- **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält das Programm *vordefinierte Untersuchungsausnahmen*. Außerdem wurden vordefinierte Untersuchungsausnahmen hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte Untersuchungsausnahmen auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.
- **Neue Ausnahme zur ausgewählten Kategorie**. Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.

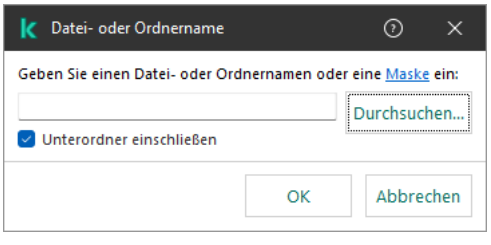
9. Um eine Datei oder einen Ordner von der Untersuchung auszuschließen, gehen Sie wie folgt vor:



Einstellungen für Ausnahmen

a. Aktivieren Sie im Block **Eigenschaften** das Kontrollkästchen **Datei oder Ordner**.

b. Klicken Sie auf den Link im Block unten, um das Fenster **Datei- oder Ordnername** zu öffnen.



Datei oder Ordner wählen

a. Geben Sie entweder den Datei- oder Ordnernamen oder die Maske eines Datei- oder Ordnernamens ein, oder klicken Sie auf **Durchsuchen** und wählen Sie in der Ordnerstruktur eine Datei oder einen Ordner aus.

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` funktioniert nicht.

- 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.

Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `?:\Users\*\Folder\` ein.

Kaspersky Endpoint Security unterstützt Umgebungsvariablen

Netzwerkordner können ausgeschlossen werden. Geben Sie dazu den Pfad des Netzwerkordners manuell ein (z. B. `\\Network Share\*`).

> Die Umgebungsvariable `%userprofile%` wird von Kaspersky Endpoint Security nicht unterstützt, wenn mit der Kaspersky Security Center-Konsole eine Liste mit Ausnahmen erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen `*` verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.

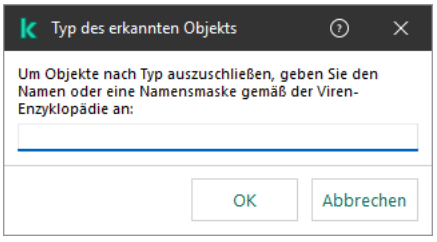
b. Deaktivieren Sie bei Bedarf die Funktion **Unterordner einschließen**. Wenn diese Funktion aktiviert ist, untersucht das Programm die Dateien nicht in allen Unterordnern. Wenn diese Funktion deaktiviert ist, schließt das Programm nur den ausgewählten Ordner aus dem Untersuchungsbereich aus. Diese Option ist standardmäßig aktiviert.

c. Speichern Sie die vorgenommenen Änderungen.

10. Um Objekte mit einem bestimmten Namen von der Untersuchung auszuschließen, gehen Sie wie folgt vor:

    a. Aktivieren Sie im Block **Eigenschaften** das Kontrollkästchen **Typ des erkannten Objekts**.

    b. Klicken Sie auf den Link im Block unten, um das Fenster **Typ des erkannten Objekts** zu öffnen.



Objekt wählen

    a. Um den Namen des Objekttyps einzugeben, verwenden Sie die Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

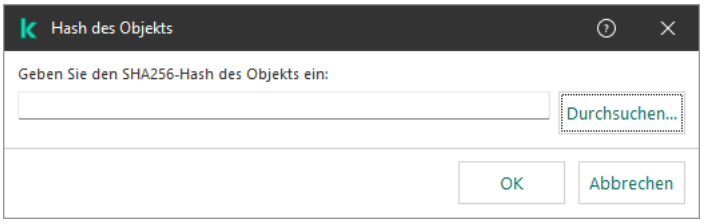
    Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

    b. Speichern Sie die vorgenommenen Änderungen.

11. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten:

    a. Aktivieren Sie im Block **Eigenschaften** das Kontrollkästchen **Hash des Objekts**.

    b. Klicken Sie auf den Link im Block unten, um das Fenster **Hash des Objekts** zu öffnen.



Datei wählen

    a. Geben Sie den Datei-Hash ein oder wählen Sie die Datei durch Klicken auf **Durchsuchen** aus.

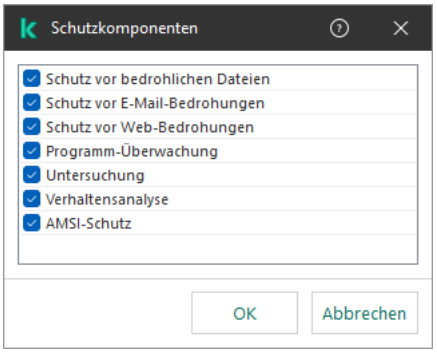
    Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

    b. Speichern Sie die vorgenommenen Änderungen.

12. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

13. Legen Sie die Komponenten von Kaspersky Endpoint Security fest, für die eine Untersuchungsausnahme verwendet werden soll.

    a. Klicken Sie auf den Link im Block unten, um das Fenster **Schutzkomponenten** zu öffnen.



Schutzkomponenten auswählen

    a. Aktivieren Sie die Kontrollkästchen für jene Komponenten, für welche die Untersuchungsausnahme gelten soll.

    Sind Komponenten in den Einstellungen einer Untersuchungsausnahme angegeben, so gilt die Ausnahme nur für diese Komponenten von Kaspersky Endpoint Security.

    Sind keine Komponenten in den Einstellungen einer Untersuchungsausnahme angegeben, so gilt die Ausnahme für alle Komponenten von Kaspersky Endpoint Security.

14. Klicken Sie auf **OK**.

    Die neue Ausnahme wird der Liste hinzugefügt. Sie können eine Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen neben dem Objekt.

15. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So erstellen Sie eine Untersuchungsausnahme in der Kaspersky Security Center Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.
5. Klicken Sie im folgenden Fenster auf den Link **Ausnahmen für die Schadsoftware-Untersuchung**.
6. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der Ausnahmen für alle Computer des Unternehmens erstellen möchten. Die Listen mit Ausnahmen in den übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die Ausnahmen der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Ausnahmen der übergeordneten Richtlinie können weder geändert noch gelöscht werden.

7. Markieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben**, wenn Sie es dem Benutzer ermöglichen möchten, eine lokale Liste von Ausnahmen zu erstellen. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Ausnahmenliste seine eigene lokale Ausnahmenliste erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Ausnahmen zugreifen. Wenn dieses Kontrollkästchen deaktiviert ist, blendet Kaspersky Endpoint Security die konsolidierte Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus.

8. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können Untersuchungsausnahmen in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens eine Untersuchungsausnahme hinzu.

   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält das Programm *vordefinierte Untersuchungsausnahmen*. Außerdem wurden vordefinierte Untersuchungsausnahmen hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte Untersuchungsausnahmen auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

   Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Kategorie und wählen Sie die Option **Neue Ausnahme** aus.

9. Wählen Sie aus, wie Sie die Ausnahme hinzufügen möchten: **Datei- oder Ordnerpfad**, **Objekttyp** oder **Objekt-Hash**.

10. Um eine Datei oder einen Ordner vom Scan auszuschließen, geben Sie den Pfad manuell ein. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

    - 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` funktioniert nicht.

    - 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.

      Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `?:\Users\*\Folder\` ein.

      Netzwerkordner können ausgeschlossen werden. Geben Sie dazu den Pfad des Netzwerkordners manuell ein (z. B. `\\Network Share\*`).

11. Wenn Sie einen bestimmten Objekttyp von Untersuchungen ausschließen möchten, geben Sie im Feld **Objekttyp** den Namen des Objekttyps gemäß der Klassifizierung der Kaspersky-Enzyklopädie ein (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

    Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

12. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten, geben Sie den Dateihash im Feld **Objekt-Hash** ein.

    Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

13. Wählen Sie im Block **Ausnahme anwenden auf** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

14. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

15. Klicken Sie auf **OK**.

    Die neue Ausnahme wird der Liste hinzugefügt. Über den Schalter können Sie eine Ausnahme jederzeit stoppen.

16. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

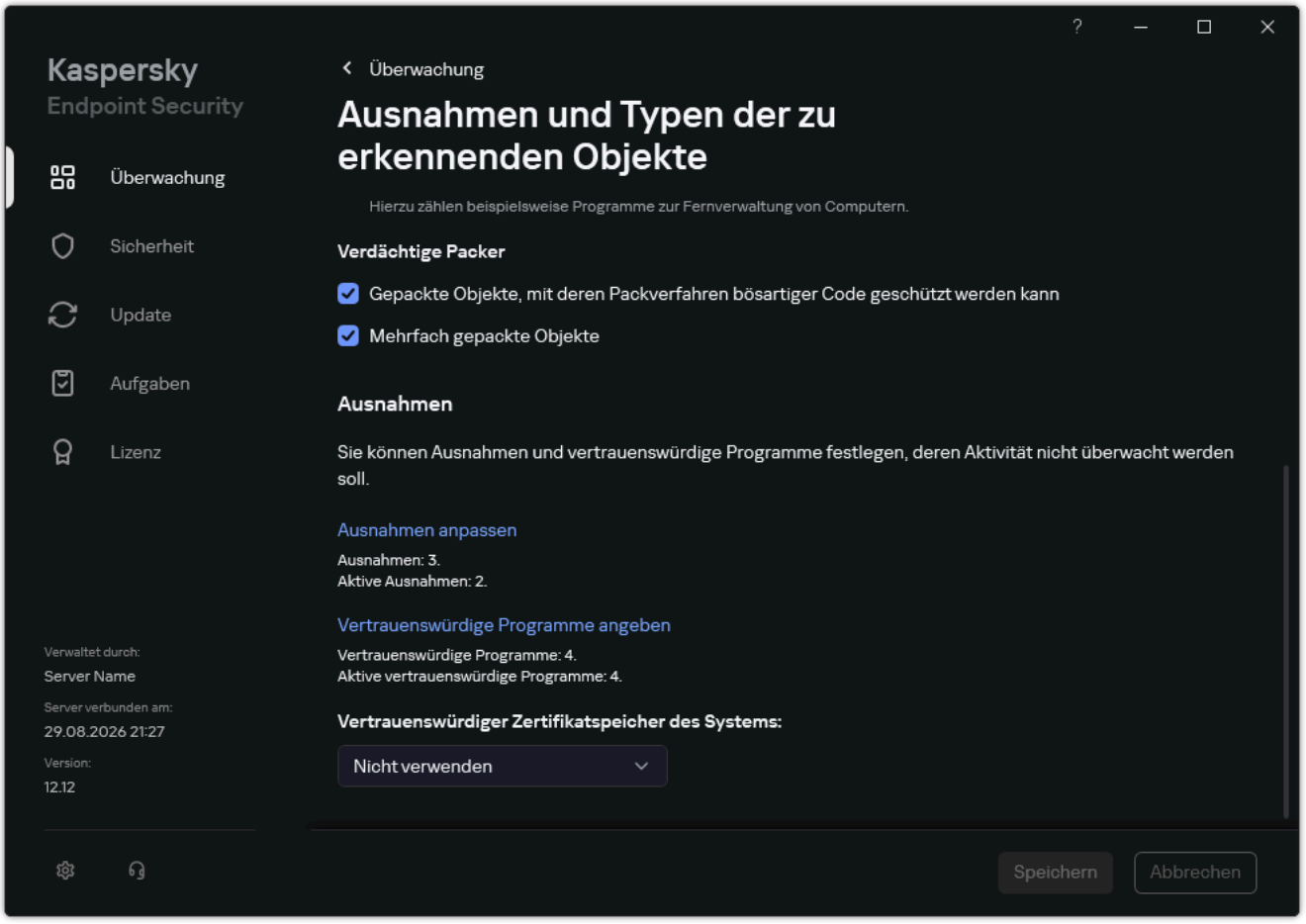
So erstellen Sie eine Untersuchungsausnahme in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.

3. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.

Kaspersky Endpoint Security blendet die Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration von Untersuchungsausnahmen in der Konsole blockiert (Symbol „geschlossenes Schloss“) und lokale Untersuchungsausnahmen verboten sind (das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben** ist deaktiviert).



Einstellungen für Ausnahmen

4. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können Untersuchungsausnahmen in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens eine Untersuchungsausnahme hinzu.

   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält das Programm *vordefinierte Untersuchungsausnahmen*. Außerdem wurden vordefinierte Untersuchungsausnahmen hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte Untersuchungsausnahmen auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

   Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Kategorie und wählen Sie die Option **Neue Ausnahme** aus.

5. Wenn Sie eine Datei oder einen Ordner von Untersuchungen ausschließen möchten, wählen Sie die Datei oder den Ordner aus, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

- 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` funktioniert nicht.

- 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.

  Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `?:\Users\*\Folder\` ein.

  Netzwerkordner können ausgeschlossen werden. Geben Sie dazu den Pfad des Netzwerkordners manuell ein (z. B. `\\Network Share\*`).

6. Wenn Sie einen bestimmten Objekttyp von Untersuchungen ausschließen möchten, geben Sie im Feld **Typ des erkannten Objekts** den Namen des Objekttyps gemäß der Klassifizierung der Kaspersky-Enzyklopädie ein (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

   Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

7. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten, geben Sie den Dateihash im Feld **Objekt-Hash** ein.

   Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

8. Wählen Sie im Block **Schutzkomponenten** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

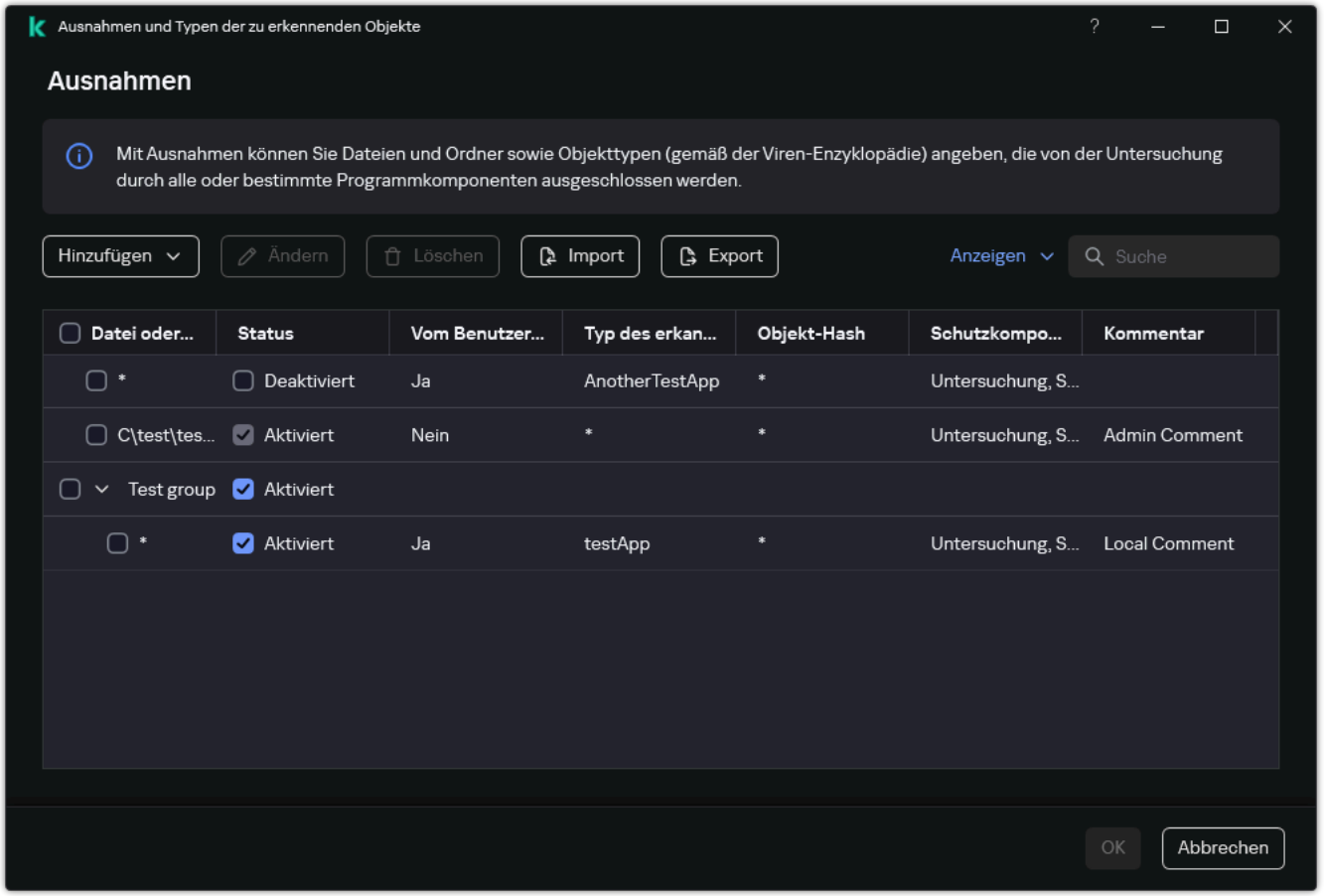
9. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

10. Wählen Sie den Status **Aktiv** für die Ausnahme.

11. Klicken Sie auf **Hinzufügen**.

    Die neue Ausnahme wird der Liste hinzugefügt. Sie können die Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen in der Spalte **Status**.

12. Speichern Sie die vorgenommenen Änderungen.



Liste der Ausnahmen

Beispiele für Pfadmasken:

Empfehlung: Geben Sie relative Pfade an, keine absoluten Pfade. Dadurch können Sie nicht nur Dateisystemobjekte ausschließen, sondern auch dateilose Objekte. Beispiel: `*\Program Files (x86)\Folder\Subfolder`.

Pfade für Dateien, die sich in einem beliebigen Ordner befinden können:

- Die Maske `*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe.
- Die Maske `example*` umfasst alle Pfade von Dateien mit dem Namen EXAMPLE.

Pfade für Dateien, die sich in einem bestimmten Ordner befinden können:

- Die Maske `C:\dir\*.*` umfasst alle Pfade von Dateien, die sich in `C:\dir\` befinden, allerdings nicht in den untergeordneten Ordnern von `C:\dir\`.
- Die Maske `C:\dir\*` umfasst alle Pfade von Dateien im Ordner `C:\dir\`, einschließlich untergeordneter Ordner.
- Die Maske `C:\dir\` umfasst alle Pfade von Dateien im Ordner `C:\dir\`, einschließlich untergeordneter Ordner.
- Die Maske `C:\dir\*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe im Ordner `C:\dir\`, allerdings nicht in den untergeordneten Ordnern von `C:\dir\`.
- Die Maske `C:\dir\test` umfasst alle Pfade von Dateien mit dem Namen test im Ordner `C:\dir\`, allerdings nicht in den untergeordneten Ordnern von `C:\dir\`.
- Die Maske `C:\dir\*\test` umfasst alle Pfade von Dateien mit dem Namen test im Ordner `C:\dir\` und in den untergeordneten Ordnern von `C:\dir\`.
- Die Maske `C:\dir1\*\dir3\` enthält alle Pfade zu Dateien in dir3-Unterordnern im Ordner `C:\dir1\` in einer Ebene.
- Die Maske `C:\dir1\**\dirN\` enthält alle Pfade zu Dateien in dirN-Unterordnern im Ordner `C:\dir1\` in jeder Ebene.

Pfade für Dateien, die sich in allen Ordnern mit dem angegebenen Namen befinden können:

- Die Maske `dir\*.*` umfasst alle Pfade von Dateien in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\*` umfasst alle Pfade von Dateien in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\` umfasst alle Pfade von Dateien in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieser Ordner.
- Die Maske `dir\test` umfasst alle Pfade von Dateien mit dem Namen test in Ordnern mit dem Namen dir, allerdings nicht in den Unterordnern dieses Ordners.

Eine Ausnahme nach dem Typ der gefundenen Objekte erstellen

Kaspersky Endpoint Security klassifiziert gefundene Objekte wie folgt:

- **Viren und Würmer**

  Unterkategorie: Viren und Würmer (Viruses_and_Worms)

  Gefahrenstufe: Hoch

  Klassische Viren und Würmer führen auf einem Computer Aktionen aus, die nicht vom Benutzer erlaubt wurden. Sie können sich selbst kopieren, wobei die Kopien ebenfalls zur Reproduktion fähig sind.

Klassischer Virus

Nachdem ein klassischer Virus in ein System eingedrungen ist, infiziert er eine Datei, aktiviert sich darin, führt seine schädlichen Aktionen aus und fügt anderen Dateien Kopien von sich hinzu.

Ein klassischer Virus vermehrt sich nur auf lokalen Computerressourcen und kann nicht selbständig in andere Rechner eindringen. Er kann nur auf andere Computer gelangen, wenn er seine Kopie einer Datei hinzufügt, die in einem gemeinsamen Ordner oder auf einer eingelegten CD gespeichert wird, oder wenn der Benutzer eine E-Mail-Nachricht verschickt, an welche die infizierte Datei angehängt ist.

Der Code eines klassischen Virus kann in unterschiedliche Computerbereiche, in das Betriebssystem oder in Programme eindringen. Abhängig vom Milieu werden *Dateiviren*, *Bootviren*, *Skriptviren* und *Makroviren* unterschieden.

Viren verwenden unterschiedliche Methoden, um Dateien zu infizieren. *Overwriting*-Viren schreiben ihren Code über den Code einer infizierten Datei und zerstören deren Inhalt. Die infizierte Datei funktioniert nicht mehr und kann nicht repariert werden. *Parasitic*-Viren verändern Dateien, wobei diese Dateien vollständig oder teilweise funktionsfähig bleiben. *Companion*-Viren verändern Dateien nicht, sondern legen Duplikate an. Beim Öffnen einer infizierten Datei wird ihr Zwilling gestartet, der ein Virus ist. Außerdem gibt es noch folgende Virentypen: *Link-Viren*, *OBJ-Viren*, *LIB-Viren*, *Quellcode*-Viren so wie viele andere.

Wurm

Genau wie ein klassischer Virus dringt auch ein Wurm in einen Computer ein, aktiviert seinen Code und führt schädliche Aktionen aus. Die Bezeichnung Wurm geht darauf zurück, dass er wie ein Wurm von Computer zu Computer „kriechen“ und seine Kopien ohne Erlaubnis des Benutzers über verschiedene Datenkanäle verbreiten kann.

Würmer werden grundsätzlich nach der Art ihrer Verbreitung unterschieden. Die folgende Tabelle klassifiziert die Wurmtypen nach der Verbreitungsmethode.

Verbreitungsmethoden von Würmern

Typ	Name	Beschreibung
Email-Worm	Email-Worm	Sie verbreiten sich über E-Mails. Eine infizierte E-Mail-Nachricht enthält eine angehängte Datei mit einer Wurmkopie oder einem Link zu einer solchen Datei, die sich auf einer gehackten oder speziell erstellten Website befindet. Wenn Sie die angehängte Datei öffnen, wird der Wurm aktiviert. Wenn Sie auf den Link klicken, die Datei herunterladen und dann öffnen, beginnt der Wurm auch mit seinen bösartigen Aktionen. Danach verbreitet er seine Kopien. Dazu sucht er andere E-Mail-Adressen und schickt infizierte Nachrichten an diese.
IM-Worm	IM-Client-Würmer	Sie verbreiten sich über IM-Clients. Ein IM-Wurm verschickt in der Regel Nachrichten mit einem Link, der zu einer Website mit seiner Kopie führt, an die Adressen der Kontaktliste. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
IRC-Worm	Würmer für Internet-Chats	Sie verbreiten sich über Internet Relay Chats. Dies sind Dienstsysteme, mit denen über das Internet in Echtzeit Gespräche mit anderen Teilnehmern möglich sind. Ein solcher Wurm veröffentlicht im Internet-Chat eine Datei mit seiner Kopie oder einem Link zu einer Datei. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
Net-Worm	Netzwürmer (Würmer für Computernetzwerke)	Sie verbreiten sich über Computernetzwerke. Im Unterschied zu anderen Wurmtypen verbreitet sich ein Netzwurm ohne Zutun des Benutzers. Er sucht im lokalen Netzwerk nach Computern, auf denen Programme laufen, die Schwachstellen aufweisen. Zu diesem Zweck schickt er ein spezielles Netzwerkpaket (Exploit), das den Wurmcode oder einen Teil davon enthält. Befindet sich ein „verwundbarer“ Computer im Netzwerk, nimmt er das Netzwerkpaket an. Nachdem der Wurm vollständig in den Computer eingedrungen ist, aktiviert er sich.

Typ	Name	Beschreibung
P2P-Worm	Würmer für Dateitausch-Netzwerke	Sie verbreiten sich über Peer-to-Peer-Netze. Um in ein P2P-Netz einzudringen, kopiert sich der Wurm in einen Ordner, der zum Dateiaustausch verwendet wird und sich gewöhnlich auf einem PC befindet. Das P2P-Netz zeigt Informationen über diese Datei an. Ein Benutzer kann die infizierte Datei wie andere angebotene Dateien im Netzwerk „finden", herunterladen und öffnen. Komplexere Würmer imitieren das Netzwerkprotokoll eines konkreten P2P-Netzes: Sie antworten positiv auf Suchanfragen und bieten ihre Kopien zum Download an.
Wurm	Sonstige Würmer	Zu den sonstigen Netzwürmern zählen: • Würmer, die ihre Kopien in Netzwerkressourcen verbreiten. Unter Verwendung von Betriebssystemfunktionen durchsuchen sie verfügbare Netzwerkordner, bauen Verbindungen zu Computern im globalen Netzwerk auf und versuchen, umfassenden Zugriff auf ihre Laufwerke zu erhalten. Im Unterschied zu den oben beschriebenen Wurmarten verbreiten sich die sonstigen Würmer nicht selbständig weiter, sondern nur, wenn der Benutzer eine Datei mit einer Wurmkopie öffnet. • Würmer, die keine in dieser Tabelle beschriebenen Verbreitungsmethoden verwenden (z. B. Würmer, die sich über Mobiltelefone weiterverbreiten).

- **Trojaner (einschließlich Ransomware)**

  Subkategorie: trojanische Programme (Trojan_programs)

  Gefahrenstufe: Hoch

  Im Gegensatz zu Würmern und Viren erstellen trojanische Programme keine Kopien von sich. Sie dringen z. B. über E-Mails oder über den Browser in den Computer ein, wenn der Benutzer eine infizierte Webseite besucht. Trojanische Programme werden unter Beteiligung des Benutzers gestartet. Unmittelbar nach ihrem Start beginnen sie mit ihren schädlichen Aktionen.

  Jeder Trojaner-Typ zeigt ein individuelles Verhalten auf dem infizierten Computer. Die Hauptfunktionen von trojanischen Programmen sind das Sperren, Verändern oder Vernichten von Informationen sowie das Hervorrufen von Funktionsstörungen in Computern oder Computernetzwerken. Außerdem können trojanische Programme Dateien empfangen oder senden, Dateien ausführen, auf dem Bildschirm Meldungen anzeigen, auf Webseiten zugreifen, Programme herunterladen und installieren, und einen Computer neu starten.

  Häufig verwenden Angreifer eine „Kombination" aus unterschiedlichen Trojanerprogrammen.

  Die folgende Tabelle unterscheidet die Typen der trojanischen Programme nach ihrem Verhalten.

  Typen der trojanischen Programme nach ihrem Verhalten auf einem infizierten Computer

Typ	Name	Beschreibung
Trojan-ArcBomb	Trojanische Programme – „Archivbomben"	Archive. Beim Extrahieren vergrößert sich der Inhalt so stark, dass es auf dem Computer zu Funktionsstörungen kommt. Wenn der Benutzer versucht, ein solches Archiv zu entpacken, kann es sein, dass die Leistung des Computers sinkt, der Computer hängen bleibt oder die Festplatte mit „leeren" Daten überfüllt wird. Eine besondere Gefahr bilden „Archivbomben" für Datei- und Mailserver. Wird auf dem Server ein System zur automatischen Verarbeitung eingehender Daten verwendet, kann eine „Archivbombe" den Server zum Absturz bringen.
Backdoor	Trojanische Programme zur Remote-Administration	Dieser Typ gilt unter den trojanischen Programmen als der gefährlichste. Sie gleichen funktionsmäßig Programmen, die zur Remote-Administration auf einem Computer installiert werden. Diese Programme installieren sich auf dem Computer, ohne dass der Benutzer etwas davon bemerkt, und ermöglichen dem Angreifer die Fernsteuerung des Computers.

Typ	Name	Beschreibung
Trojan	Trojanische Programme	Dieser Typ umfasst folgende schädlichen Programme: • **Klassische trojanische Programme**. Diese Programme führen nur die Grundfunktionen trojanischer Programme aus: Sperrung, Veränderung oder Zerstörung von Informationen, Störung der Arbeit von Computern oder Computernetzwerken. Sie besitzen keine Zusatzfunktionen, über die andere Trojaner-Typen verfügen, die in dieser Tabelle beschrieben sind. • **„Mehrzweck"-Trojaner**. Sie besitzen Zusatzfunktionen, die gleichzeitig für mehrere Typen trojanischer Programme charakteristisch sind.
Trojan-Ransom	Trojanische Erpressungsprogramme	Sie nehmen die Daten auf einem PC als „Geisel", indem sie diese verändern oder sperren, oder stören die Arbeit des Computers, damit der Benutzer nicht mehr auf seine Daten zugreifen kann. Der Angreifer fordert vom Benutzer ein Lösegeld und verspricht, dafür ein Programm zu liefern, das die Funktionsfähigkeit des Computers und der Daten wiederherstellt.
Trojan-Clicker	Trojanische Clicker-Programme	Diese Programme greifen von einem PC aus auf Webseiten zu: Sie senden entweder selbst Befehle an den Browser oder ersetzen Webadressen, die in Systemdateien gespeichert sind. Mithilfe dieser Programme organisieren Angreifer Netzwerkangriffe oder steigern die Besucherzahlen von Seiten, um die Anzeigehäufigkeit von Werbebannern zu erhöhen.
Trojan-Downloader	Trojanische Download-Programme	Sie greifen auf die Webseite des Eindringlings zu, laden von dort andere bösartige Programme herunter und installieren sie auf dem Computer des Benutzers. Sie können den Dateinamen des böswilligen Programms enthalten, die heruntergeladen oder von der Webseite, auf die zugegriffen wird, empfangen werden soll.
Trojan-Dropper	Trojanische Installationsprogramme	Nachdem sie auf der Computerfestplatte gespeichert wurden, installieren sie andere trojanische Programme, die sich in ihrem Körper befinden. Angreifer können trojanische Installationsprogramme zu folgenden Zwecken verwenden: • um ohne Wissen des Benutzers ein schädliches Programm zu installieren: Trojanische Installationsprogramme zeigen keinerlei Meldungen an oder blenden falsche Meldungen über einen Fehler im Archiv oder eine inkorrekte Version des Betriebssystems ein. • um andere bekannte Schadsoftware vor der Entdeckung zu schützen: Nicht alle Antiviren-Programme können Schadsoftware in trojanischen Installationsprogrammen erkennen.
Trojan-Notifier	Trojanische Benachrichtigungsprogramme	Sie informieren einen Angreifer darüber, dass der infizierte Computer „online" ist und übermitteln folgende Informationen über den Computer: IP-Adresse, Nummer des offenen Ports oder E-Mail-Adresse. Sie nehmen per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise Kontakt mit dem Angreifer auf. Trojanische Benachrichtigungsprogramme werden häufig in Kombination mit unterschiedlichen Trojanerprogrammen eingesetzt. Sie teilen dem Angreifer mit, dass andere trojanische Programme erfolgreich auf einem PC installiert wurden.
Trojan-Proxy	Trojanische Proxy-Programme	Sie ermöglichen es einem Angreifer, über einen PC anonym auf Webseiten zuzugreifen. Sie dienen häufig zum Spam-Versand.
Trojan-PSW	Trojanische Programme zum Kennwortdiebstahl	Trojanische Programme, die Kennwörter stehlen (Password Stealing Ware). Sie berauben Benutzerkonten und stehlen beispielsweise Registrierungsdaten für Softwareprodukte. Solche Trojaner durchsuchen Systemdateien und die Registrierung nach vertraulichen Daten und schicken diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den „Angreifer". Einige dieser trojanischen Programme werden speziellen Typen zugeordnet, die in dieser Tabelle beschrieben sind. Dazu zählen Trojaner, die Bankkonten berauben (Trojan-Banker), Daten von IM-Clients stehlen (Trojan-IM) und Daten aus Netzwerkspielen entwenden (Trojan-GameThief).
Trojan-Spy	Trojanische Spyware-Programme	Sie spionieren den Benutzer aus und sammeln Informationen über die Aktionen, die der Benutzer bei der Arbeit am Computer ausführt. Sie können die Daten abfangen, die der Benutzer über die Tastatur eingibt, Screenshots machen oder Listen aktiver Programme sammeln. Die gesammelten Informationen werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.

Typ	Name	Beschreibung
Trojan-DDoS	Trojanische Programme für Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung). Häufig werden mehrere Computer von solchen Programmen infiziert, um sie dann gleichzeitig für einen gezielten Angriff auf einen Server zu verwenden. DoS-Programme realisieren einen Angriff von einem Computer aus, wobei der Benutzer davon weiß. DDoS-Programme (Distributed DoS) verwenden eine größere Anzahl von Computern ohne Wissen der Benutzer für verteilte Angriffe.
Trojan-IM	Trojanische Programme zum Diebstahl der Daten von IM-Client-Benutzern	Sie stehlen Nummern und Kennwörter der Benutzer von IM-Clients. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Rootkit	Rootkits	Sie maskieren andere bösartige Programme und deren Aktivität und verlängern so die Persistenz der Programme im Betriebssystem. Sie können auch Dateien, Prozesse im Speicher eines infizierten Computers oder Registrierungsschlüssel, die bösartige Programme ausführen, verbergen. Die Rootkits können den Datenaustausch zwischen Programmen auf dem Computer des Benutzers und anderen Computern im Netzwerk maskieren.
Trojan-SMS	Trojanische Programme für SMS-Nachrichten	Sie infizieren Handys und versenden SMS-Nachrichten an kostenpflichtige Nummern.
Trojan-GameThief	Trojanische Programme zum Diebstahl von Benutzerdaten aus Netzwerkspielen	Sie stehlen Kontodaten von Benutzern, die an Netzwerkspielen für Computer teilnehmen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Banker	Trojanische Programme zum Diebstahl von Daten über Bankkonten	Sie stehlen Daten über Bankkonten oder über Konten bei elektronischen Zahlungssystemen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Mailfinder	Trojanische Programme, die E-Mail-Adressen sammeln	Sie sammeln auf einem Computer E-Mail-Adressen und übermitteln diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. An die gesammelten Adressen kann der Angreifer Spam verschicken.

- **Schädliche Tools**

  Subkategorie: schädliche Tools

  Gefahrenstufe: Mittel

  Im Gegensatz zu anderen Arten von Malware führen bösartige Tools ihre Aktionen nicht sofort nach dem Start aus. Sie können auf dem Computer des Benutzers sicher gespeichert und gestartet werden. Angreifer verwenden die Funktionen dieser Programme, um Viren, Würmer und Trojaner zu erstellen, Netzwerkangriffe gegen Remote-Server zu organisieren, Computer zu „hacken“ und andere schädliche Aktionen durchzuführen.

  Die folgende Tabelle kategorisiert die unterschiedlichen Funktionen von schädlichen Tools.

  Funktionen von schädlichen Tools

Typ	Name	Beschreibung
Constructor	Konstrukteure	Mit ihrer Hilfe können neue Viren, Würmer und Trojaner erstellt werden. Einige Konstrukteure verfügen über eine standardmäßige Fensteroberfläche, in der über ein Menü der Typ einer zu erstellenden Schadsoftware, die Methode zur Debugger-Abwehr und sonstige Eigenschaften gewählt werden.
Dos	Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung).

Typ	Name	Beschreibung
Exploit	Exploits	*Exploits* bestehen aus einer Datenkombination oder aus Programmcode, der die Schwachstellen eines Programms, in dem er verarbeitet wird, ausnutzt, um auf dem Computer eine schädliche Aktion auszuführen. Ein Exploit kann beispielsweise Dateien schreiben oder lesen oder auf „infizierte" Webseiten zugreifen. Es gibt verschiedene Arten von Exploits, die Schwachstellen unterschiedlicher Programme oder Netzwerkdienste ausnutzen. Exploits werden als Netzwerkpaket über ein Netzwerk an mehrere Computer übertragen, um Computer mit anfälligen Netzwerkdiensten zu finden. Ein Exploit in einer DOC-Datei nutzt die Schwachstellen eines Textverarbeitungsprogramms. Er kann damit beginnen, die vom Angreifer programmierten Funktionen auszuführen, sobald der Benutzer eine infizierte Datei öffnet. Ein Exploit, der in eine E-Mail-Nachricht eingebettet ist, sucht nach Schwachstellen in einem Mail-Client. Er kann mit der Ausführung einer schädlichen Aktion beginnen, sobald der Benutzer die infizierte E-Mail in diesem Mail-Client öffnet. Mithilfe von Exploits werden Netzwürmer (Net-Worm) verbreitet. Nuker sind Netzwerkpakete, die einen Computer zum Absturz bringen.
FileCryptor	Verschlüsselungsprogramme	Chiffreure verschlüsseln schädliche Programme, um sie vor Antiviren-Programmen zu verstecken.
Flooder	Programme zur „Verunreinigung" von Netzwerken	Sie versenden eine hohe Anzahl von Nachrichten über Netzwerkkanäle. Zu diesem Typ zählen beispielsweise Programme, die der Verunreinigung von Internet Relay Chats dienen. Programme, die der Verunreinigung von Kanälen für E-Mail, IM-Clients und Mobilfunksysteme dienen, zählen nicht zu diesem Typ. Diese Programme werden separaten Typen zugeordnet, die ebenfalls in dieser Tabelle beschrieben sind (Email-Flooder, IM-Flooder und SMS-Flooder).
HackTool	Hacker-Tools	Sie können die Kontrolle über den Computer, auf dem sie installiert sind, übernehmen oder einen anderen Computer angreifen (z. B. ohne Erlaubnis des Benutzers andere Systembenutzer hinzufügen und Systemberichte löschen, um ihre Spuren im System zu verwischen). Zu diesem Typ gehören bestimmte Sniffer, die über schädliche Funktionen wie z. B. das Abfangen von Kennwörtern verfügen. Sniffer (Sniffers) sind Programme, die den Netzwerkverkehr abhören können.
Hoax	Böse Scherze	Diese Programme erschrecken einen Benutzer mit virenähnlichen Meldungen: Sie zeigen fiktive Meldungen über Virenfunde in sauberen Dateien oder über das Formatieren der Festplatte an.
Spoofer	Imitator-Tools	Sie senden E-Mails und Netzwerkanfragen mit gefälschten Absenderadressen. Imitatoren werden beispielsweise von Angreifern verwendet, um einen falschen Absender vorzutäuschen.
VirTool	Tools zur Modifikation schädlicher Programme	Sie erlauben es, andere schädliche Programme so zu modifizieren, dass sie sich vor Antiviren-Programmen verstecken können.
Email-Flooder	Programme zur „Verunreinigung" von E-Mail-Postfächern	Sie versenden eine hohe Anzahl von Nachrichten an E-Mail-Adressen („verstopfen diese mit Müll"). Die große Menge von E-Mails hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
IM-Flooder	Programme zur „Verunreinigung" von IM-Clients	Sie versenden eine hohe Anzahl von Nachrichten an Benutzer von IM-Clients Das hohe Nachrichtenaufkommen hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
SMS-Flooder	Programme zur „Verunreinigung" von SMS-Systemen	Sie versenden eine große Anzahl von SMS-Nachrichten an Mobiltelefone.

- **Adware**

  Unterkategorie: Werbe-Software (Adware)

  Gefahrenstufe: Mittel

  Adware-Programme dienen dazu, dem Benutzer Werbung zu zeigen. Sie zeigen auf der Oberfläche anderer Programme Werbebanner an oder leiten Suchanfragen auf Webseiten mit Werbung um. Einige von ihnen sammeln auf Werbung bezogene Informationen über den Benutzer und leiten sie an ihren Urheber weiter, z.B. Informationen darüber, welche Webseiten der Benutzer besucht und welche Suchanfragen er vornimmt. Im Gegensatz zu trojanischer Spyware leiten Adware-Programme diese Informationen mit der Erlaubnis des Benutzers weiter.

- **Dialer**

  Unterkategorie: Dialer.

  Gefahrenstufe: Mittel

  Dialer können über ein Modem heimlich Telefonverbindungen herstellen.

- **legitimes Programm, mit dem Angreifer den Computer oder die Benutzerdaten beschädigen können**

  Unterkategorie: Legitime Programme, mit denen Angreifer Ihren Computer oder Ihre Daten beschädigen können.

  Gefahrenstufe: Mittel

  Die Mehrzahl dieser Programme sind nützliche Programme. Zu diesen Programmen zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für FTP, HTTP und Telnet.

  Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf einem PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

  Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern. Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.

Typ	Name	Beschreibung
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- **Gepackte Objekte, mit deren Packverfahren bösartiger Code geschützt werden kann**

  Unterkategorie: Gepackte Dateien, die Schaden verursachen können.

  Gefahrenstufe: Mittel.

  Die Datei wurde mit einem speziellen Packer gepackt, der zum Packen von Schadsoftware verwendet wird: Viren, Würmer, Trojaner. Kaspersky Endpoint Security untersucht das SFX-Modul von selbstentpackenden SFX-Archiven (self-extracting archive).

  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.

- **Mehrfach gepackte Objekte**

  Unterkategorie: Mehrfach gepackte Dateien.

  Gefahrenstufe: Mittel.

  Die Datei wurde dreimal oder öfter mit einem oder mehreren Packern gepackt.

  Damit Antiviren-Programme die Schadsoftware nicht erkennen, verpacken Hacker eine Datei mehrfach. Kaspersky Endpoint Security untersucht gepackte Dateien.

Standardmäßig erkennt Kaspersky Endpoint Security alle Typen von Objekten. Für einen optimalen Schutz des Computers wird empfohlen, die Erkennung aller Objekttypen aktiviert zu lassen. Wenn Sie in Ihrem Unternehmen Dienstprogramme verwenden, die vom Programm als schädlich eingestuft werden, fügen Sie diese Dienstprogramme zu einer Ausnahmeliste hinzu, deaktivieren Sie aber nicht die Erkennung für den gesamten Objekttyp.

So wählen Sie die Typen der zu erkennenden Objekte aus (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
5. Klicken Sie im Block **Typen der zu erkennenden Objekte** auf **Einstellungen**.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen für die Objekttypen, die Kaspersky Endpoint Security erkennen soll.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So wählen Sie die Typen der zu erkennenden Objekte aus (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Erkennungseinstellungen**.

5. Aktivieren Sie im Block **Erkennung anderer Objekttypen** die Kontrollkästchen für die Objekttypen, die Kaspersky Endpoint Security erkennen soll.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

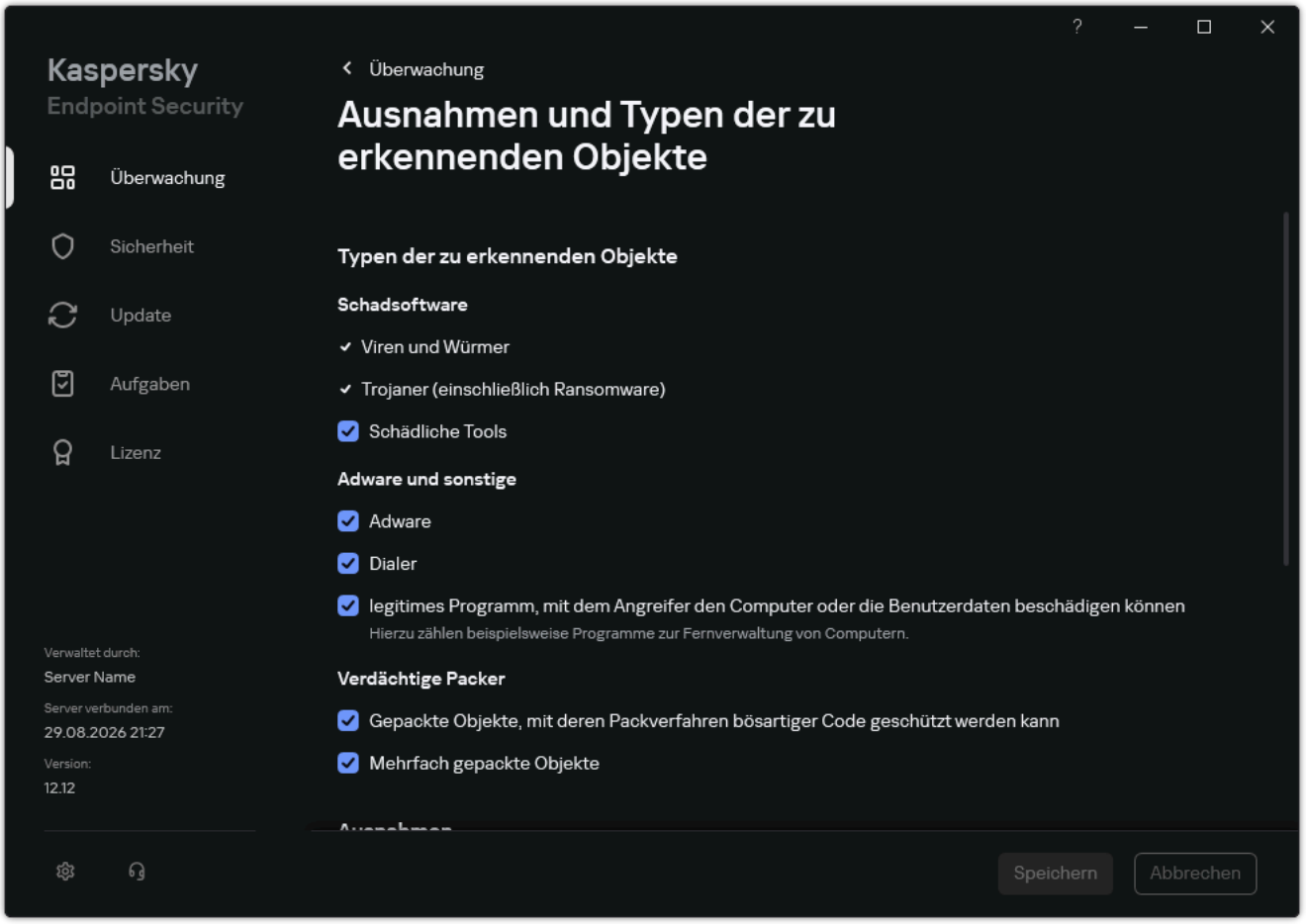
So wählen Sie die Typen der zu erkennenden Objekte aus (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Ausnahmen und Typen der zu erkennenden Objekte** aus.

3. Aktivieren Sie im Block **Typen der zu erkennenden Objekte** die Kontrollkästchen für die Objekttypen, die Kaspersky Endpoint Security erkennen soll.

4. Speichern Sie die vorgenommenen Änderungen.



Typen der zu erkennenden Objekte

Liste mit vertrauenswürdigen Programmen erstellen

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.

Untersuchungsausnahmen und vertrauenswürdige Programme unterscheiden sich wie folgt: Bei Ausnahmen untersucht Kaspersky Endpoint Security keine Dateien, während bei vertrauenswürdigen Programmen die initiierten Prozesse nicht kontrolliert werden. Wenn ein vertrauenswürdiges Programm eine schädliche Datei in einem Ordner erstellt, der nicht zu den Untersuchungsausnahmen gehört, erkennt Kaspersky Endpoint Security die Datei und beseitigt die Bedrohung. Wenn der Ordner zu den Ausnahmen gehört, überspringt Kaspersky Endpoint Security diese Datei.

Wenn Sie beispielsweise die Objekte, die von der Standard-App Microsoft-Editor verwendet werden, für ungefährlich halten, vertrauen Sie dieser App und Sie können Microsoft-Editor zur Liste der vertrauenswürdigen Programme hinzufügen, damit die von dieser App verwendeten Objekte nicht überwacht werden. Dadurch wird die Computerleistung erhöht, was bei Verwendung von Serveranwendungen besonders wichtig ist.

Außerdem können spezielle Aktionen, die von Kaspersky Endpoint Security als schädlich klassifiziert werden, im Rahmen bestimmter Programme ungefährlich sein. So ist das Abfangen eines Textes, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (z. B. Punto Switcher) ein normaler Vorgang. Es wird empfohlen, solche Programme in die Liste der vertrauenswürdigen Programme aufzunehmen, um ihre speziellen Funktionen zu berücksichtigen und sie von der Aktivitätskontrolle auszuschließen.

Vertrauenswürdige Programme helfen, Kompatibilitätsprobleme zwischen Kaspersky Endpoint Security und anderen Anwendungen zu vermeiden (z. B. das Problem einer doppelten Untersuchung des Netzwerkverkehrs eines fremden Computers durch Kaspersky Endpoint Security und durch eine andere Antiviren-Anwendung).

Die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms werden jedoch weiterhin auf Viren und andere Schadprogramme untersucht. Verwenden Sie Untersuchungsausnahmen, um ein Programm vollständig von der Untersuchung durch Kaspersky Endpoint Security auszuschließen.

So fügen Sie ein Programm zur vertrauenswürdigen Liste in der Verwaltungskonsole (MMC) hinzu

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
5. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme → Vertrauenswürdige Programme** auf **Einstellungen**.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.
6. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der vertrauenswürdigen Programme für alle Computer des Unternehmens erstellen möchten. Die Listen mit vertrauenswürdigen Programmen der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Programme der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Programme der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.
7. Aktivieren Sie das Kontrollkästchen **Verwendung lokaler vertrauenswürdiger Programme erlauben**, wenn Sie dem Benutzer die Erstellung einer lokalen Liste vertrauenswürdiger Programme ermöglichen möchten. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Liste vertrauenswürdiger Programme eine eigene lokale Liste vertrauenswürdiger Programme erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten vertrauenswürdigen Programme zugreifen. Wenn dieses Kontrollkästchen deaktiviert ist, blendet Kaspersky Endpoint Security die konsolidierte Liste der vertrauenswürdiges Programme in der App-Benutzeroberfläche aus.
8. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können vertrauenswürdige Programme in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens ein vertrauenswürdiges Programm hinzu.
   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.

- **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält die App *vordefinierte vertrauenswürdige Programme*. Außerdem wurden vordefinierte vertrauenswürdige Programme hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte vertrauenswürdige Programme auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

- **Neue Ausnahme zur ausgewählten Kategorie**. Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.

9. Wählen Sie die Vertrauenskriterien aus:

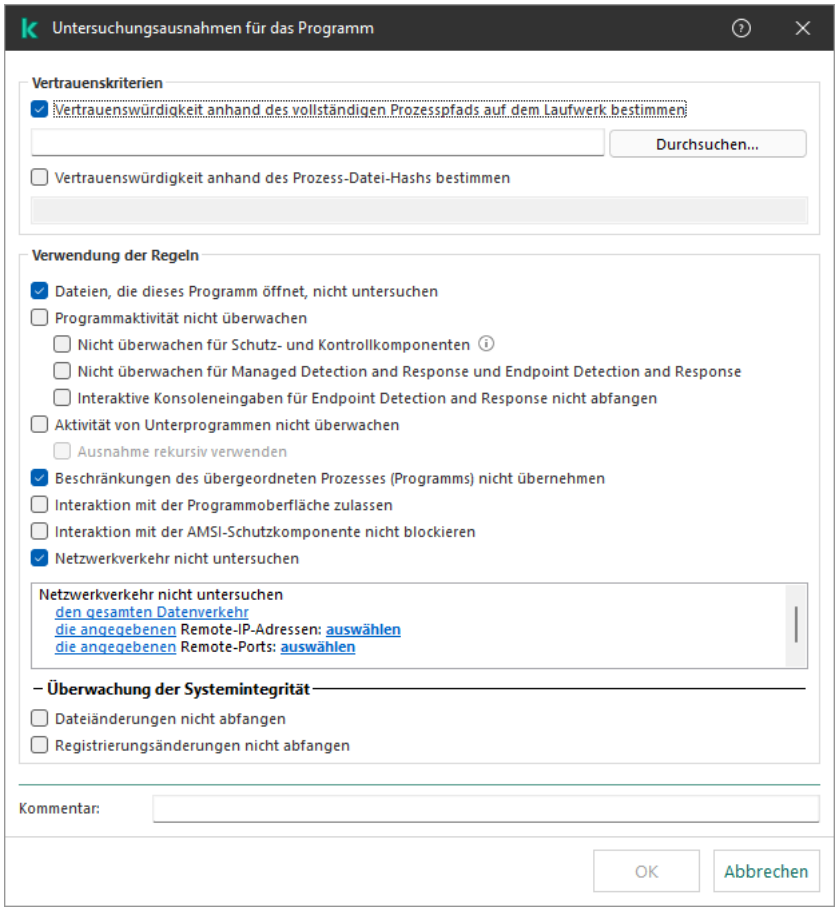
- **Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen**. Geben Sie den Pfad der ausführbaren Datei des vertrauenswürdigen Programms ein.

  Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

  Kaspersky Endpoint Security berücksichtigt beim Dateinamen eines vertrauenswürdigen Programms die Groß-/Kleinschreibung. Wenn Sie einen Dateinamen mit fehlerhafter Groß-/Kleinschreibung eingeben, erkennt Kaspersky Endpoint Security das vertrauenswürdige Programm nicht.

- **Vertrauenswürdigkeit anhand des Prozess-Datei-Hashs bestimmen**.

Die Umgebungsvariable `%userprofile%` wird von Kaspersky Endpoint Security nicht unterstützt, wenn eine Liste mit vertrauenswürdigen Programmen in der Kaspersky Security Center-Konsole erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen * verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.



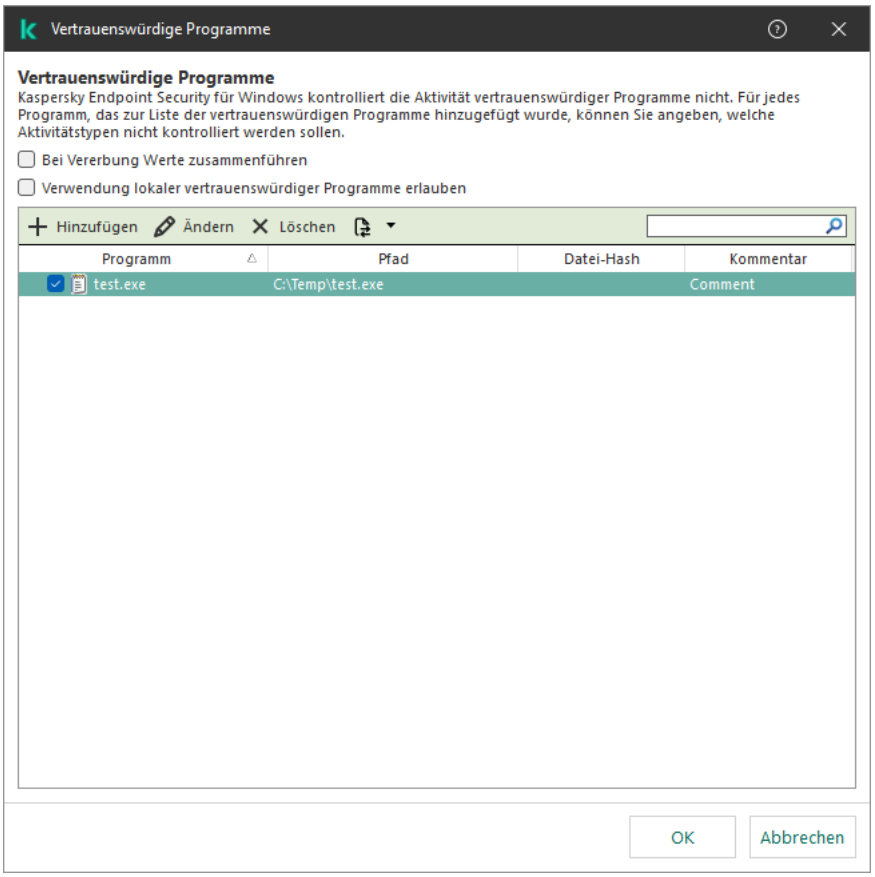
Einstellungen für vertrauenswürdige Programme

10. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

11. Klicken Sie auf **OK**.

    Das neue vertrauenswürdige Programm wird der Liste hinzugefügt. Sie können ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen. Dazu dient das Kontrollkästchen neben dem Objekt.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Liste der vertrauenswürdigen Programme

So fügen Sie ein Programm zur vertrauenswürdigen Liste in der Kaspersky Security Center Web Console hinzu

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.

5. Klicken Sie im folgenden Fenster auf den Link **Programme**.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.

6. Aktivieren Sie das Kontrollkästchen **Bei Vererbung Werte zusammenführen**, wenn Sie eine konsolidierte Liste der vertrauenswürdigen Programme für alle Computer des Unternehmens erstellen möchten. Die Listen mit vertrauenswürdigen Programmen der übergeordneten und untergeordneten Richtlinien werden zusammengefasst. Damit die Listen zusammengefasst werden können, muss die Vererbung von Einstellungen der übergeordneten Richtlinie aktiviert sein. Die vertrauenswürdigen Programme der übergeordneten Richtlinie sind in untergeordneten Richtlinien sichtbar, können dort aber nur angezeigt werden. Vertrauenswürdige Programme der übergeordneten Richtlinie können nicht geändert oder gelöscht werden.

7. Aktivieren Sie das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben**, wenn Sie dem Benutzer die Erstellung einer lokalen Liste vertrauenswürdiger Programme ermöglichen möchten. Auf diese Weise kann ein Benutzer zusätzlich zu der in der Richtlinie generierten allgemeinen Liste vertrauenswürdiger Programme eine eigene lokale Liste vertrauenswürdiger Programme erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen.

   Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten vertrauenswürdigen Programme zugreifen. Wenn dieses Kontrollkästchen deaktiviert ist, blendet Kaspersky Endpoint Security die konsolidierte Liste der vertrauenswürdiges Programme in der App-Benutzeroberfläche aus.

8. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können vertrauenswürdige Programme in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens ein vertrauenswürdiges Programm hinzu.

   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.

   - **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält die App *vordefinierte vertrauenswürdige Programme*. Außerdem wurden vordefinierte vertrauenswürdige Programme hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte vertrauenswürdige Programme auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

   Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Kategorie und wählen Sie die Option **Neue Ausnahme** aus.

9. Wählen Sie die Vertrauenskriterien aus:

   - **Datei- oder Ordnerpfad**. Geben Sie den Pfad der ausführbaren Datei des vertrauenswürdigen Programms ein.

     Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

     Kaspersky Endpoint Security berücksichtigt beim Dateinamen eines vertrauenswürdigen Programms die Groß-/Kleinschreibung. Wenn Sie einen Dateinamen mit fehlerhafter Groß-/Kleinschreibung eingeben, erkennt Kaspersky Endpoint Security das vertrauenswürdige Programm nicht.

   - **Programm-Hash**.

Die Umgebungsvariable %userprofile% wird von Kaspersky Endpoint Security nicht unterstützt, wenn in der Kaspersky Security Center-Konsole eine Liste mit vertrauenswürdigen Programmen erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen `*` verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.

10. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

11. Klicken Sie auf **OK**.

    Das neue vertrauenswürdige Programm wird der Liste hinzugefügt. Sie können ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen. Dazu dient das Kontrollkästchen in der Spalte **Status**.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

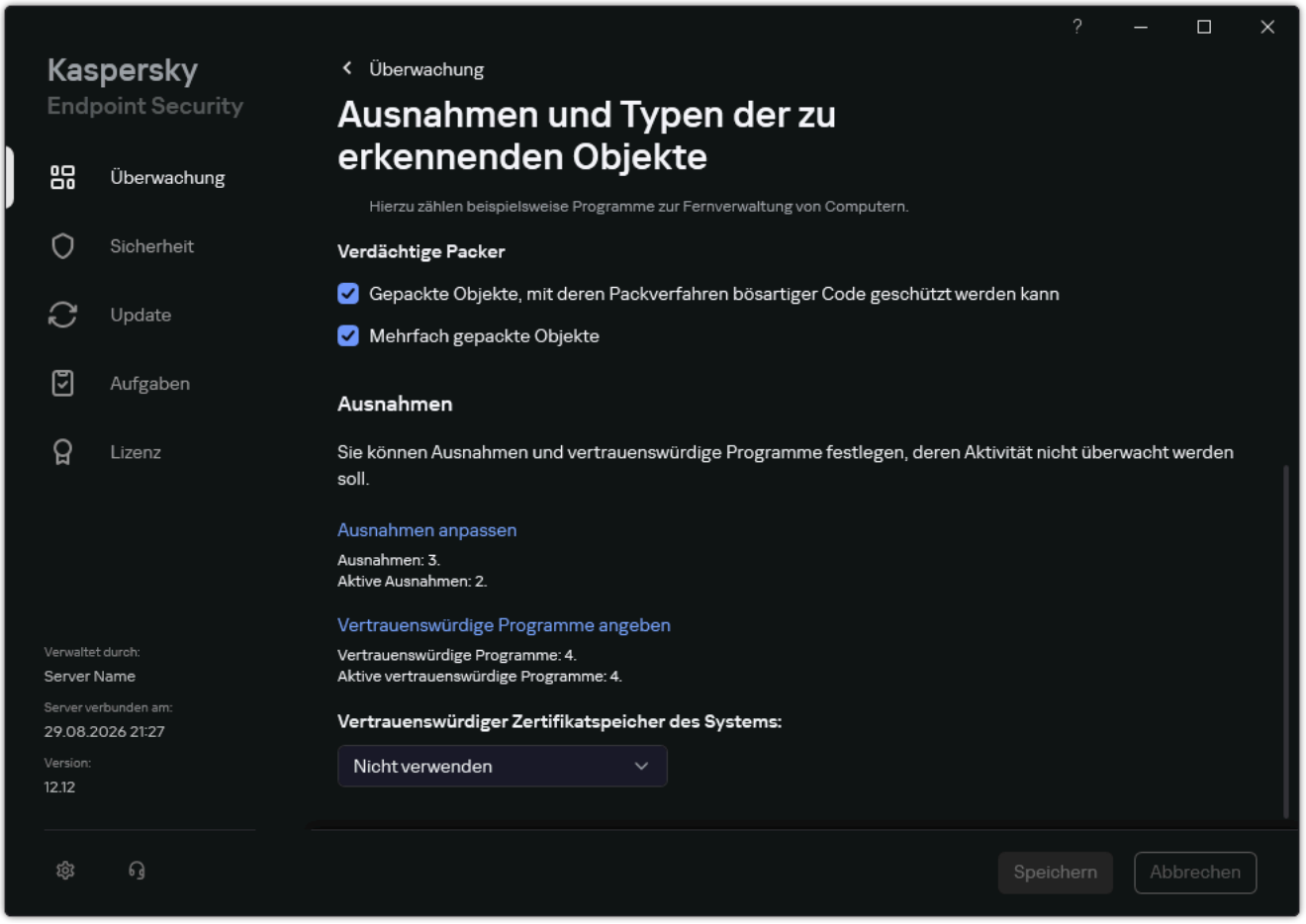
So fügen Sie ein Programm in der Programmschnittstelle zur vertrauenswürdigen Liste hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.

3. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.

Kaspersky Endpoint Security blendet die konsolidierte Liste für vertrauenswürdige Programme in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration vertrauenswürdiger Programme in der Konsole blockiert (Symbol „geschlossenes Schloss“) und lokale vertrauenswürdige Programme verboten sind (das Kontrollkästchen **Verwendung lokaler vertrauenswürdiger Programme erlauben** ist deaktiviert).



Einstellungen für Ausnahmen

4. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

- **Kategorie**. Sie können vertrauenswürdige Programme in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens ein vertrauenswürdiges Programm hinzu.
- **Neue Ausnahme**. Kaspersky Endpoint Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.
- **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält die App *vordefinierte vertrauenswürdige Programme*. Außerdem wurden vordefinierte vertrauenswürdige Programme hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte vertrauenswürdige Programme auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Kategorie und wählen Sie die Option **Neue Ausnahme** aus.

5. Wählen Sie die Vertrauenskriterien aus:

   - **Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen**. Geben Sie den Pfad der ausführbaren Datei des vertrauenswürdigen Programms ein.

     Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

     Kaspersky Endpoint Security berücksichtigt beim Dateinamen eines vertrauenswürdigen Programms die Groß-/Kleinschreibung. Wenn Sie einen Dateinamen mit fehlerhafter Groß-/Kleinschreibung eingeben, erkennt Kaspersky Endpoint Security das vertrauenswürdige Programm nicht.

   - **Vertrauenswürdigkeit anhand des Prozess-Datei-Hashs bestimmen**.

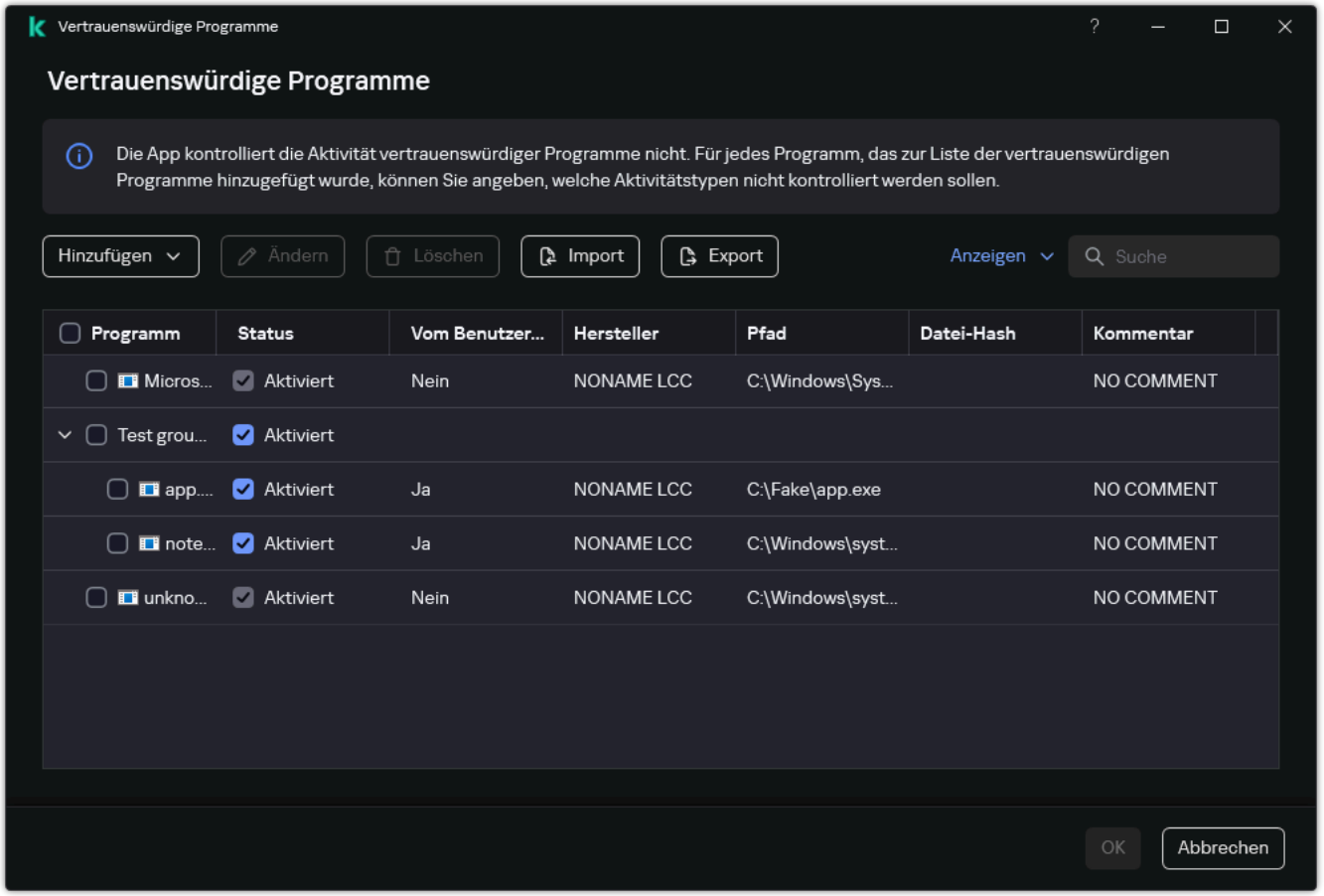
   Kaspersky Endpoint Security unterstützt Umgebungsvariablen und konvertiert den Pfad in der lokalen Programmoberfläche. Mit anderen Worten: Wenn Sie den Dateipfad `%userprofile%\Documents\File.exe` eingeben, wird der Eintrag `C:\Users\Fred123\Documents\File.exe` auf der lokalen Benutzeroberfläche des Programms für den Benutzer Fred123 hinzugefügt. Dementsprechend ignoriert Kaspersky Endpoint Security das vertrauenswürdige Programm `File.exe` für andere Benutzer. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen `*` verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.

6. Konfigurieren Sie im Fenster mit den Eigenschaften der vertrauenswürdigen Anwendung die erweiterten Einstellungen.

7. Klicken Sie auf **OK**.

   Das neue vertrauenswürdige Programm wird der Liste hinzugefügt. Sie können ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen. Dazu dient das Kontrollkästchen in der Spalte **Status**.

8. Speichern Sie die vorgenommenen Änderungen.



Liste der vertrauenswürdigen Programme

Einstellungen für vertrauenswürdige Programme

Einstellung	Beschreibung
Dateien, die dieses Programm öffnet, nicht untersuchen	Alle Dateien, die vom Programm geöffnet werden, sind von der Überprüfung durch Kaspersky Endpoint Security ausgeschlossen. Wenn Sie z. B. Programme zum Backup von Dateien verwenden, trägt diese Funktion dazu bei, den Ressourcenverbrauch von Kaspersky Endpoint Security zu reduzieren.
Programmaktivität nicht überwachen	Kaspersky Endpoint Security überwacht die Datei- und Netzwerkaktivität des Programms im Betriebssystem nicht. Sie können die Überwachung der Programmaktivität für verschiedene Komponenten von Kaspersky Endpoint Security konfigurieren: • **Nicht überwachen für Schutz- und Kontrollkomponenten**. Die Programmaktivität wird durch die folgenden Komponenten überwacht: Verhaltensanalyse, Exploit-Prävention, Programm-Überwachung, Rollback von schädlichen Aktionen und Firewall. • **Nicht überwachen für Managed Detection and Response und Endpoint Detection and Response**. Die Programmaktivität wird überwacht vom integrierten MDR-Agent und vom integrierten EDR (KATA) Agent. • **Interaktive Konsoleneingaben für Endpoint Detection and Response nicht abfangen**. Telemetriedaten über die Verwaltung der App in der Konsole werden durch Kaspersky Endpoint Security nicht gesendet. Telemetriedaten werden von Kaspersky Anti Targeted Attack Platform (EDR) verwendet.
Aktivität von Unterprogrammen nicht überwachen	Kaspersky Endpoint Security überwacht nicht die Datei- und Netzwerkaktivität der Programme, die von diesem Programm gestartet werden. Sie können die Ausnahme rekursiv anwenden. Dadurch wird erreicht, dass die App nicht die Aktivität der gesamten Kette von untergeordneten Programmen überwacht.
Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen	Die für den übergeordneten Prozess konfigurierten Einschränkungen werden von Kaspersky Endpoint Security nicht auf einen untergeordneten Prozess angewendet. Der übergeordnete Prozess wird von einem Programm gestartet, für das Programmrechte (Host Intrusion Prevention) und Netzwerkregeln für das Programm (Firewall) konfiguriert sind.
Aktivität von Unterprogrammen nicht überwachen	Kaspersky Endpoint Security überwacht nicht die Datei- und Netzwerkaktivität der Programme, die von diesem Programm gestartet werden. Sie können die Ausnahme rekursiv anwenden. Dadurch wird erreicht, dass die App nicht die Aktivität der gesamten Kette von untergeordneten Programmen überwacht.

Einstellung	Beschreibung
Interaktion mit der Programmoberfläche zulassen	Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security blockiert alle Versuche, Programme von einem Remote-Computer aus zu verwalten. Ist dieses Kontrollkästchen aktiviert, wird einem Remote-Administrationsprogramm erlaubt, Einstellungen für Kaspersky Endpoint Security über die Benutzeroberfläche von Kaspersky Endpoint Security zu verwalten.
Interaktion mit der AMSI-Schutzkomponente nicht blockieren	Kaspersky Endpoint Security überwacht nicht die Anfragen des vertrauenswürdigen Programms nach Objekten, die von der AMSI-Schutzkomponente untersucht werden sollen.
Netzwerkverkehr nicht untersuchen	Der von diesem Programm initiierte Netzwerkverkehr wird von den Untersuchungen durch Kaspersky Endpoint Security ausgeschlossen. Sie können entweder den gesamten Verkehr oder nur den verschlüsselten Verkehr von den Untersuchungen ausschließen. Sie können auch einzelne IP-Adressen und Portnummern von Untersuchungen ausschließen. Kaspersky Endpoint Security Version 14.0 oder früher unterstützt den Ausschluss von Netzwerkverkehr nicht, wenn für ein vertrauenswürdiges Programm anstelle eines Pfads ein Hash angegeben ist.
Dateiänderungen nicht abfangen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Änderungen an Dateien aus dem Bereich der Überwachung der Systemintegrität werden von Kaspersky Endpoint Security nicht überwacht. Das Programm wendet die Ausnahme auf alle Modi für die Überwachung der Systemintegrität an: Echtzeitüberwachung der Systemintegrität und On-Demand-Überwachung der Systemintegrität.
Registrierungsänderungen nicht abfangen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Änderungen an Registrierungsschlüsseln aus dem Bereich der Überwachung der Systemintegrität werden von Kaspersky Endpoint Security nicht überwacht. Das Programm wendet die Ausnahme auf alle Modi für die Überwachung der Systemintegrität an: Echtzeitüberwachung der Systemintegrität und On-Demand-Überwachung der Systemintegrität.
Kommentar	Falls erforderlich, können Sie einen kurzen Kommentar für das vertrauenswürdige Programm eingeben. Kommentare tragen dazu bei, die Suche und Sortierung von vertrauenswürdigen Programmen zu vereinfachen.
Status	Status des vertrauenswürdigen Programms: • **Aktiv** Status bedeutet, dass sich das Programm in der vertrauenswürdigen Zone befindet. • **Inaktiv** Status bedeutet, dass sich das Programm von der vertrauenswürdigen Zone ausgeschlossen ist.

Lokale vertrauenswürdige Zone erstellen

Der Benutzer kann nun eine eigene lokale vertrauenswürdige Zone für einen bestimmten Computer erstellen. Zusätzlich zur allgemeinen vertrauenswürdigen Zone kann der Benutzer in einer Richtlinie seine eigenen lokalen Listen mit Untersuchungsausnahmen und vertrauenswürdigen Anwendungen erstellen. Ein Administrator kann die Verwendung lokaler Ausnahmen oder lokaler vertrauenswürdiger Anwendungen in den Richtlinieneinstellungen zulassen oder sperren. Verwenden Sie dazu die Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben** und **Verwendung lokaler vertrauenswürdiger Programme erlauben** im Richtlinienabschnitt **Ausnahmen**.

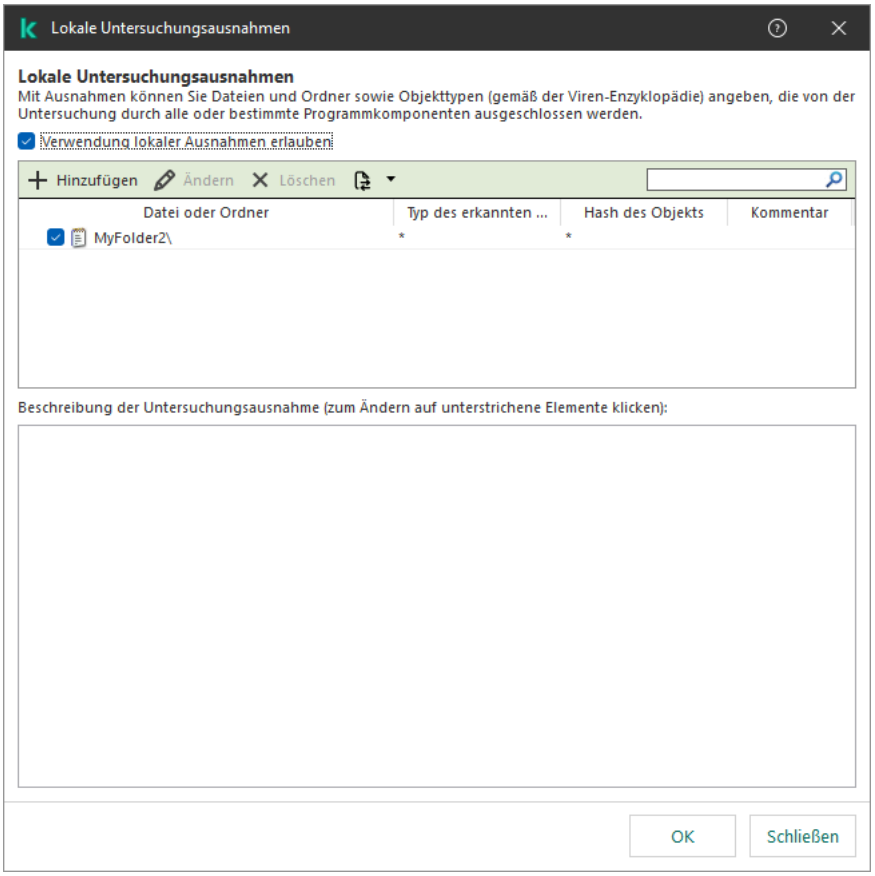
Wenn ein Administrator das Erstellen einer lokalen vertrauenswürdigen Zone erlaubt, kann der Benutzer über die Benutzeroberfläche des Programms eigene Untersuchungsausnahmen und vertrauenswürdige Anwendungen hinzufügen. Der Benutzer kann jedoch keine Objekte aus der vertrauenswürdigen Zone, die in der Richtlinie konfiguriert ist, ändern oder löschen. Der Administrator kann Ausnahmen für einen einzelnen Computer hinzufügen, indem er bestimmte Listenelemente in der Kaspersky Security Center-Konsole anzeigt, hinzufügt, ändert oder löscht.

Kaspersky Endpoint Security blendet die Listen der Untersuchungsausnahmen und vertrauenswürdigen Programme in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration der vertrauenswürdigen Zone (Symbol „geschlossenes Schloss“) in der Konsole blockiert und lokale Untersuchungsausnahmen und vertrauenswürdige Programme verboten sind.

So fügen Sie über die Verwaltungskonsole (MMC) ein Objekt zur lokalen vertrauenswürdigen Liste hinzu

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.
6. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Endpoint Security für Windows (14.2)** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.
7. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
8. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme → Lokale Untersuchungsausnahmen** auf **Einstellungen**.

   Dadurch wird ein Fenster mit einer Liste der lokalen Ausnahmen geöffnet.



Einstellungen der vertrauenswürdigen Zone

9. Erstellen Sie eine Liste mit lokalen Untersuchungsausnahmen.

   Lokale Untersuchungsausnahmen werden nach den gleichen Regeln erstellt wie allgemeine Ausnahmen. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

10. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme → Lokale vertrauenswürdige Programme** auf **Einstellungen**.

    Dadurch wird ein Fenster mit einer Liste der lokalen vertrauenswürdigen Anwendungen geöffnet.

11. Erstellen Sie eine Liste mit lokalen vertrauenswürdigen Anwendungen.

    Für das Hinzufügen von Anwendungen zur Liste der lokalen vertrauenswürdigen Anwendungen gelten die gleichen Regeln wie bei der allgemeinen Liste. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen * und ? bei der Eingabe einer Maske.

12. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie in der Kaspersky Security Center Web Console ein Objekt zur lokalen vertrauenswürdigen Zone hinzu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie dem Benutzer die Ausführung der blockierten Aktion erlauben möchten.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Klicken Sie auf **Kaspersky Endpoint Security für Windows**.

    Die lokalen Programmeinstellungen werden geöffnet.

5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.
7. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf den Link **Lokale Untersuchungsausnahmen**.
8. Erstellen Sie eine Liste mit lokalen Untersuchungsausnahmen.

    Lokale Ausnahmen werden nach den gleichen Regeln erstellt wie allgemeine Ausnahmen. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen * und ? bei der Eingabe einer Maske.

9. Klicken Sie im Block **Untersuchungsausnahmen und vertrauenswürdige Programme** auf den Link **Lokale vertrauenswürdige Programme**.
10. Erstellen Sie eine Liste mit lokalen vertrauenswürdigen Anwendungen.

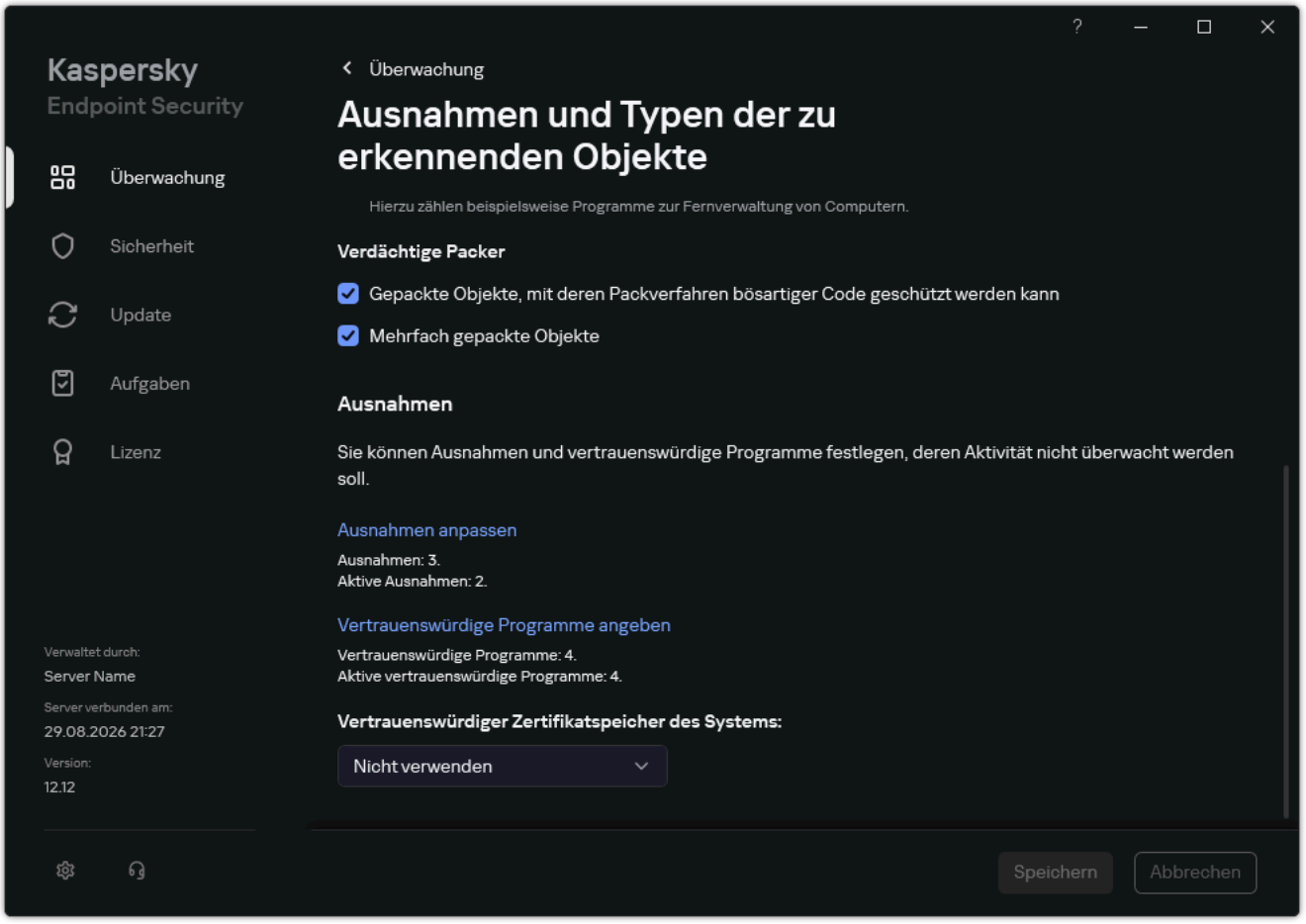
    Für das Hinzufügen von Anwendungen zur Liste der lokalen vertrauenswürdigen Anwendungen gelten die gleichen Regeln wie bei der allgemeinen Liste. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen * und ? bei der Eingabe einer Maske.

11. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine lokale Untersuchungsausnahme über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.

Kaspersky Endpoint Security blendet die Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration von Untersuchungsausnahmen in der Konsole blockiert (Symbol „geschlossenes Schloss“) und lokale Untersuchungsausnahmen verboten sind (das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben** ist deaktiviert).



Einstellungen für Ausnahmen

4. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

   - **Kategorie**. Sie können Untersuchungsausnahmen in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens eine Untersuchungsausnahme hinzu.

   - **Neue Ausnahme**. Kaspersky Endpoint Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält das Programm *vordefinierte Untersuchungsausnahmen*. Außerdem wurden vordefinierte Untersuchungsausnahmen hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte Untersuchungsausnahmen auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

   Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Kategorie und wählen Sie die Option **Neue Ausnahme** aus.

5. Wenn Sie eine Datei oder einen Ordner von Untersuchungen ausschließen möchten, wählen Sie die Datei oder den Ordner aus, indem Sie auf die Schaltfläche **Durchsuchen** klicken.

Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

- 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` funktioniert nicht.

- 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.

  Sie können Masken am Anfang, in der Mitte oder am Ende des Dateipfads verwenden. Wenn Sie beispielsweise einen Ordner für alle Benutzer zu Ausnahmen hinzufügen möchten, geben Sie die Maske `?:\Users\*\Folder\` ein.

  Netzwerkordner können ausgeschlossen werden. Geben Sie dazu den Pfad des Netzwerkordners manuell ein (z. B. `\\Network Share\*`).

6. Wenn Sie einen bestimmten Objekttyp von Untersuchungen ausschließen möchten, geben Sie im Feld **Typ des erkannten Objekts** den Namen des Objekttyps gemäß der Klassifizierung der Kaspersky-Enzyklopädie ein (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`).

   Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt Kaspersky Endpoint Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

7. Wenn Sie eine einzelne Datei von Untersuchungen ausschließen möchten, geben Sie den Dateihash im Feld **Objekt-Hash** ein.

   Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

8. Wählen Sie im Block **Schutzkomponenten** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

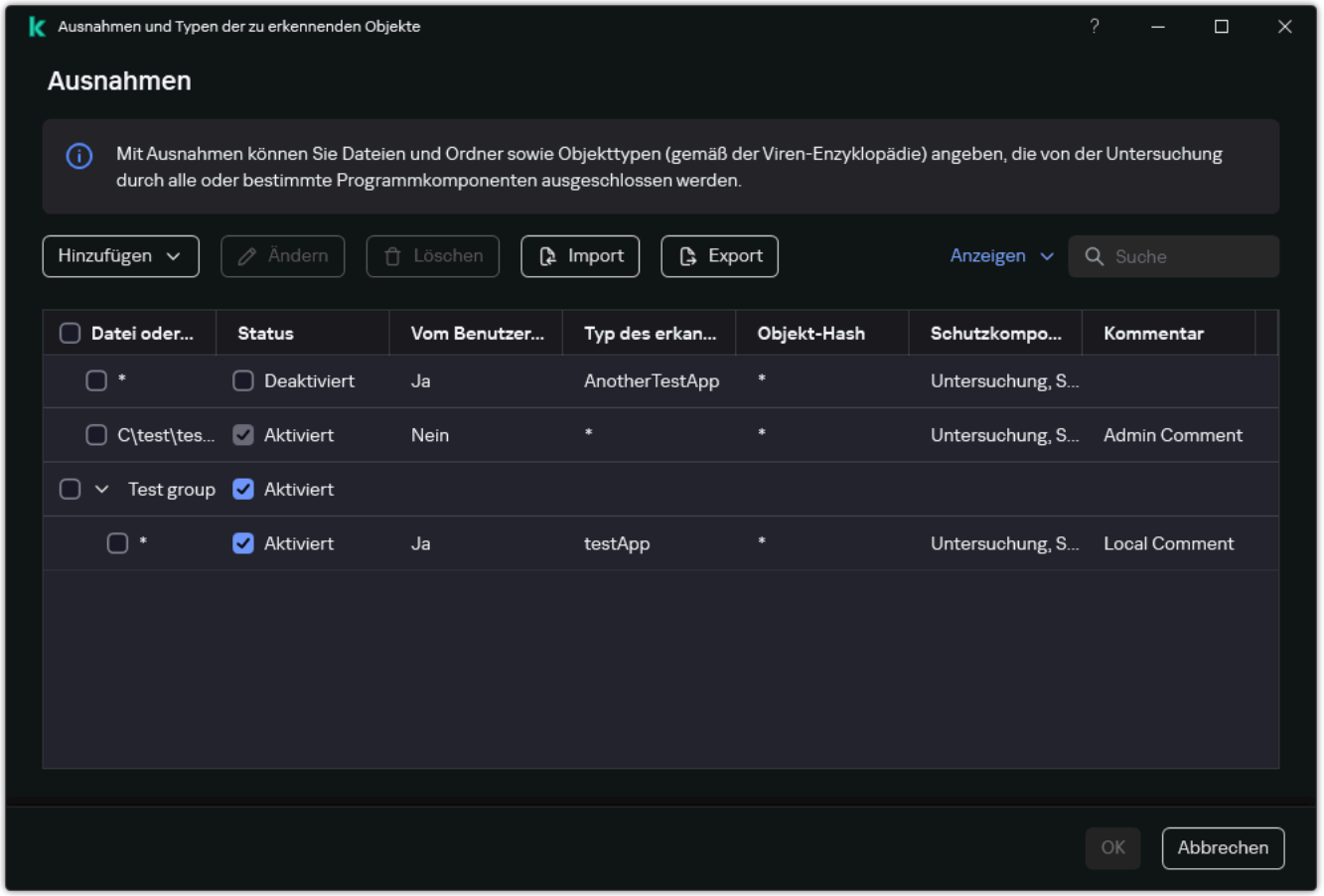
9. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

10. Wählen Sie den Status **Aktiv** für die Ausnahme.

11. Klicken Sie auf **Hinzufügen**.

    Die neue Ausnahme wird der Liste hinzugefügt. Sie können die Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen in der Spalte **Status**.

12. Speichern Sie die vorgenommenen Änderungen.

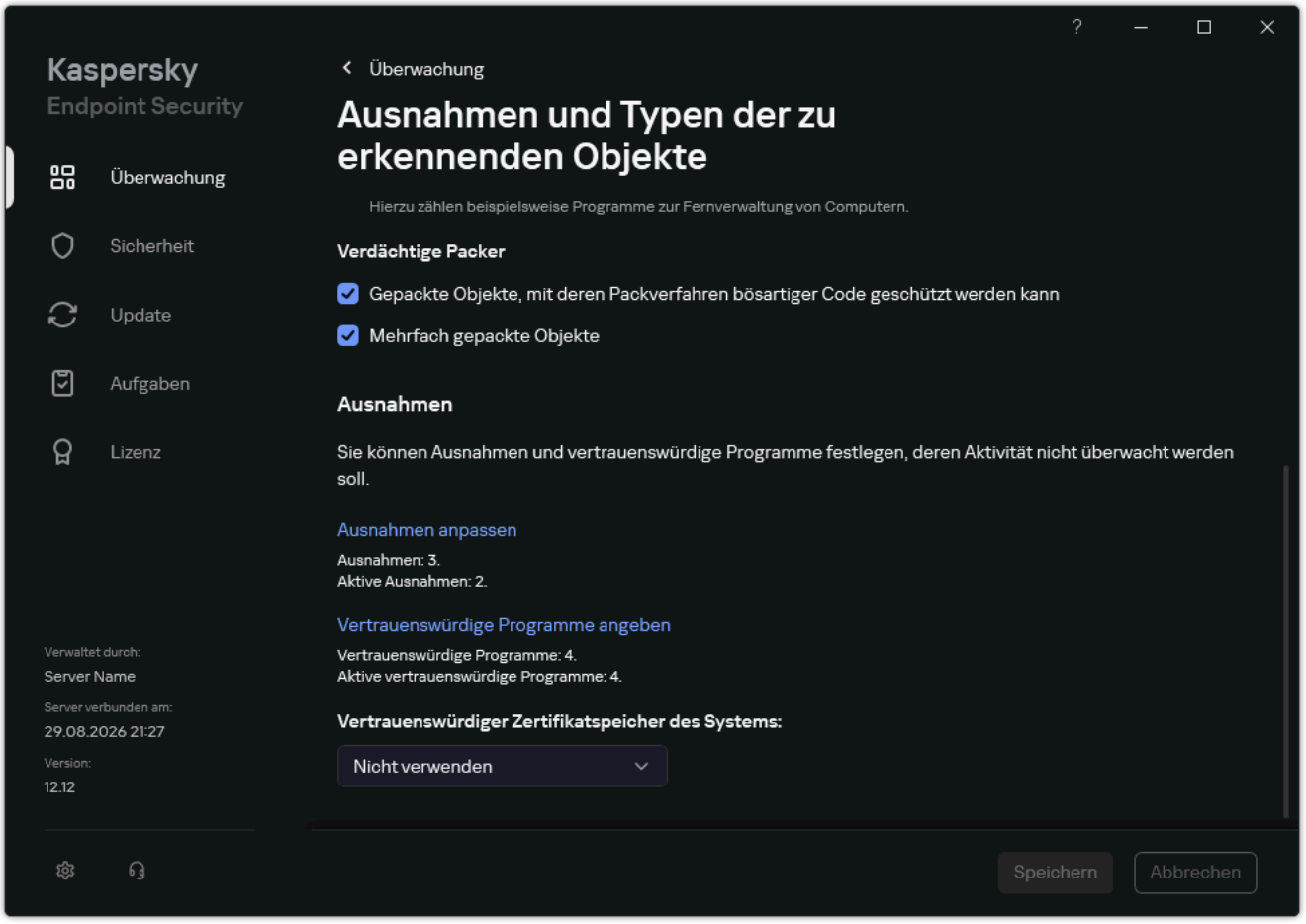


Liste der Ausnahmen

So fügen Sie über die Programmoberfläche eine Anwendung zur Liste der lokalen vertrauenswürdigen Anwendungen hinzu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Ausnahmen und Typen der zu erkennenden Objekte** aus.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.

Kaspersky Endpoint Security blendet die konsolidierte Liste für vertrauenswürdige Programme in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration vertrauenswürdiger Programme in der Konsole blockiert (Symbol „geschlossenes Schloss“) und lokale vertrauenswürdige Programme verboten sind (das Kontrollkästchen **Verwendung lokaler vertrauenswürdiger Programme erlauben** ist deaktiviert).



Einstellungen für Ausnahmen

4. Klicken Sie auf **Hinzufügen** und wählen Sie eine Aktion aus:

- **Kategorie**. Sie können vertrauenswürdige Programme in gesonderten Kategorien zusammenfassen. Um eine neue Kategorie zu erstellen, geben Sie den Namen der Kategorie ein und fügen Sie der Kategorie mindestens ein vertrauenswürdiges Programm hinzu.
- **Neue Ausnahme**. Kaspersky Endpoint Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.
- **Ausnahme aus Liste auswählen**. Zur schnellen Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager enthält die App *vordefinierte vertrauenswürdige Programme*. Außerdem wurden vordefinierte vertrauenswürdige Programme hinzugefügt, um die Einrichtung des Programms in virtuellen Citrix- und VMware-Umgebungen zu unterstützen. Wenn Sie vordefinierte vertrauenswürdige Programme auswählen, müssen Sie den Verwendungszweck des geschützten Servers berücksichtigen.

Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Kategorie und wählen Sie die Option **Neue Ausnahme** aus.

5. Wählen Sie die Vertrauenskriterien aus:

   - **Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen**. Geben Sie den Pfad der ausführbaren Datei des vertrauenswürdigen Programms ein.

     Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.

     Kaspersky Endpoint Security berücksichtigt beim Dateinamen eines vertrauenswürdigen Programms die Groß-/Kleinschreibung. Wenn Sie einen Dateinamen mit fehlerhafter Groß-/Kleinschreibung eingeben, erkennt Kaspersky Endpoint Security das vertrauenswürdige Programm nicht.

   - **Vertrauenswürdigkeit anhand des Prozess-Datei-Hashs bestimmen**.

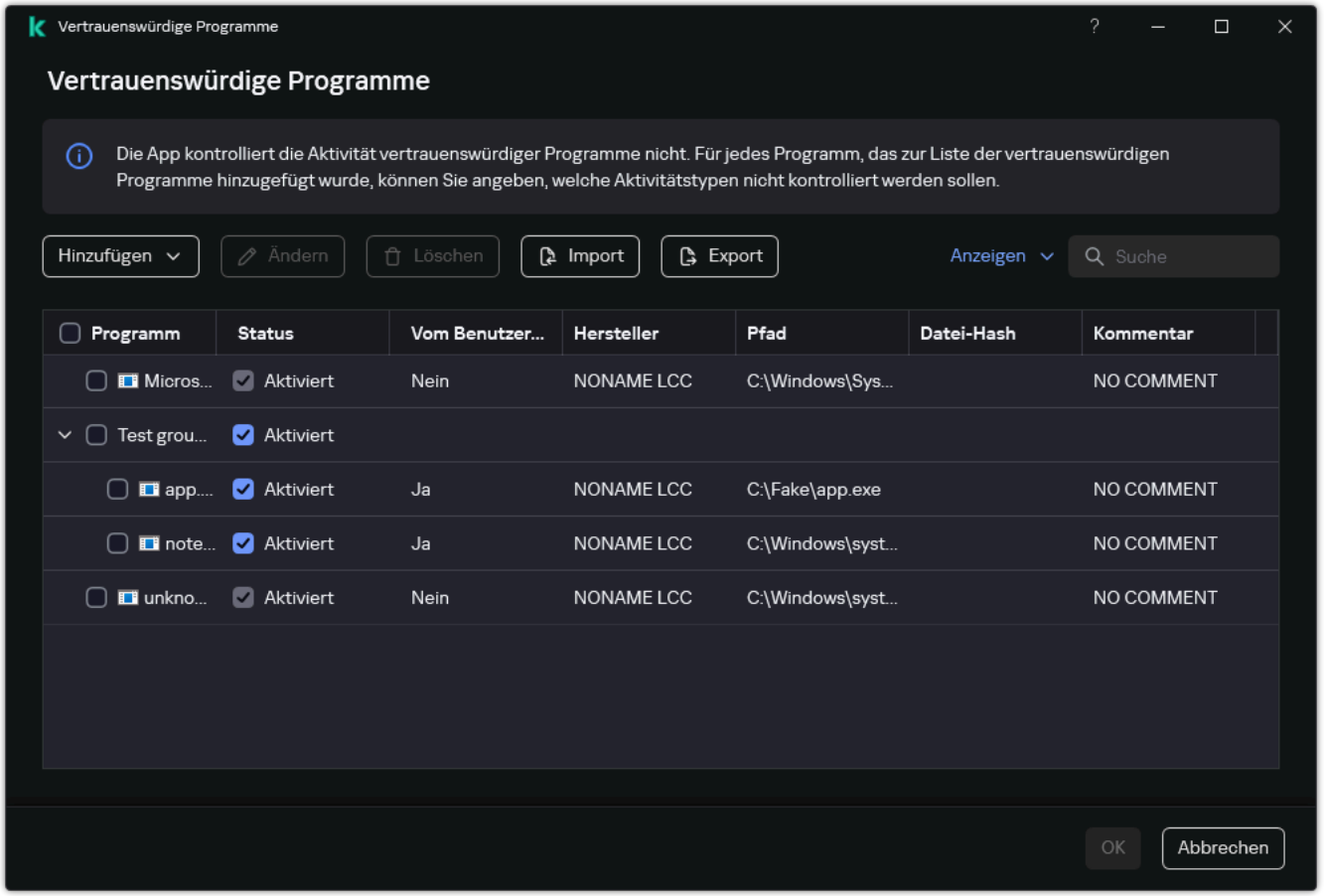
   Kaspersky Endpoint Security unterstützt Umgebungsvariablen und konvertiert den Pfad in der lokalen Programmoberfläche. Mit anderen Worten: Wenn Sie den Dateipfad `%userprofile%\Documents\File.exe` eingeben, wird der Eintrag `C:\Users\Fred123\Documents\File.exe` auf der lokalen Benutzeroberfläche des Programms für den Benutzer Fred123 hinzugefügt. Dementsprechend ignoriert Kaspersky Endpoint Security das vertrauenswürdige Programm `File.exe` für andere Benutzer. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen `*` verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.

6. Konfigurieren Sie im Fenster mit den Eigenschaften der vertrauenswürdigen Anwendung die erweiterten Einstellungen.

7. Klicken Sie auf **OK**.

   Das neue vertrauenswürdige Programm wird der Liste hinzugefügt. Sie können ein Programm jederzeit aus der vertrauenswürdigen Zone ausschließen. Dazu dient das Kontrollkästchen in der Spalte **Status**.

8. Speichern Sie die vorgenommenen Änderungen.



Liste der vertrauenswürdigen Programme

Vertrauenswürdige Zone exportieren und importieren

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 besteht aus den folgenden Listen: *Untersuchungsausnahmen* und *vertrauenswürdige Programme*. Sie können diese Listen in XML-Dateien und andere Formate exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Webadressen desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie auch ein Backup für die Liste für Erweiterungen und die Liste für vertrauenswürdige Programme anlegen oder die Listen auf einen anderen Server migrieren.

Für den Export und Import der *Ausnahmeliste* verwendet die App die folgenden Formate:

- XML ist in der Verwaltungskonsole (MMC), Web Console und Cloud Console verfügbar.
- DAT ist nur für den Import in die Verwaltungskonsole (MMC) verfügbar. Dieses Format dient der Kompatibilität mit älteren App-Versionen. Sie können eine DAT-Datei in der Verwaltungskonsole (MMC) in eine XML-Datei umwandeln, um Ausnahmelisten in die Web Console zu migrieren.
- CSV ist nur in der lokalen Benutzeroberfläche der App verfügbar.

Für den Export und Import von *Liste mit vertrauenswürdigen Apps* verwendet Kaspersky Endpoint Security das XML-Format.

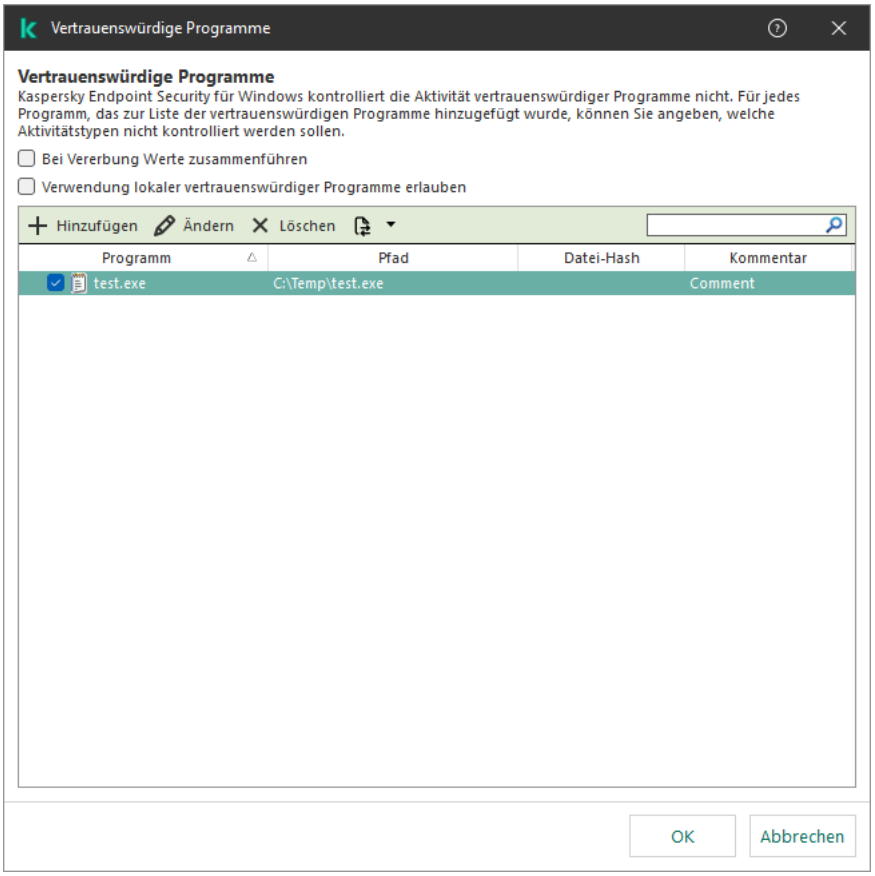
So exportieren und importieren Sie die vertrauenswürdige Zone über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
4. Wählen Sie unter **Untersuchungsausnahmen und vertrauenswürdige Programme** die Komponente der vertrauenswürdigen Zone aus, die Sie exportieren oder importieren möchten: **Untersuchungsausnahmen** oder **Vertrauenswürdige Programme**.
5. Klicken Sie auf **Einstellungen**.
6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:
   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die gesamte Liste der Ausnahmen in die XML-Datei. Kaspersky Endpoint Security unterstützt auch den Export der Ausnahmeliste in eine DAT-Datei.



Liste der vertrauenswürdigen Programme

7. So importieren Sie die Ausnahmeliste:

    a. Klicken Sie auf die Schaltfläche → **Importieren**.

    b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

    c. Öffnen Sie die Datei.

    Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll. Kaspersky Endpoint Security unterstützt auch den Import einer Ausnahmeliste aus einer DAT-Datei.

8. Speichern Sie die vorgenommenen Änderungen.

So exportieren oder importieren Sie die vertrauenswürdige Zone über Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

    Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.
5. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

    a. Klicken Sie auf den Link **Ausnahmen für die Schadsoftware-Untersuchung**.

    b. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten.

    c. Klicken Sie auf die Schaltfläche → **Exportieren**.

    Kaspersky Endpoint Security exportiert die Liste der Ausnahmen in eine json-Datei im standardmäßigen Download-Ordner.

6. Um die Liste der vertrauenswürdigen Apps zu exportieren:

    a. Wählen Sie die vertrauenswürdigen Apps aus, die Sie exportieren möchten.

    b. Klicken Sie auf die Schaltfläche → **Exportieren**.

    Kaspersky Endpoint Security exportiert die Liste der vertrauenswürdigen Programme in eine json-Datei im standardmäßigen Download-Ordner.

7. So importieren Sie die Ausnahmeliste:

    a. Klicken Sie auf den Link **Ausnahmen für die Schadsoftware-Untersuchung**.

    b. Klicken Sie auf die Schaltfläche → **Import**.

    Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

c. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der JSON-Datei ergänzt werden soll.

8. Um eine Liste mit vertrauenswürdigen Apps zu importieren:

a. Klicken Sie auf den Link **Programme**.

b. Klicken Sie auf die Schaltfläche → **Import**.

Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die JSON-Datei aus, aus der Sie die Liste der vertrauenswürdiges Apps importieren möchten.

c. Öffnen Sie die Datei.

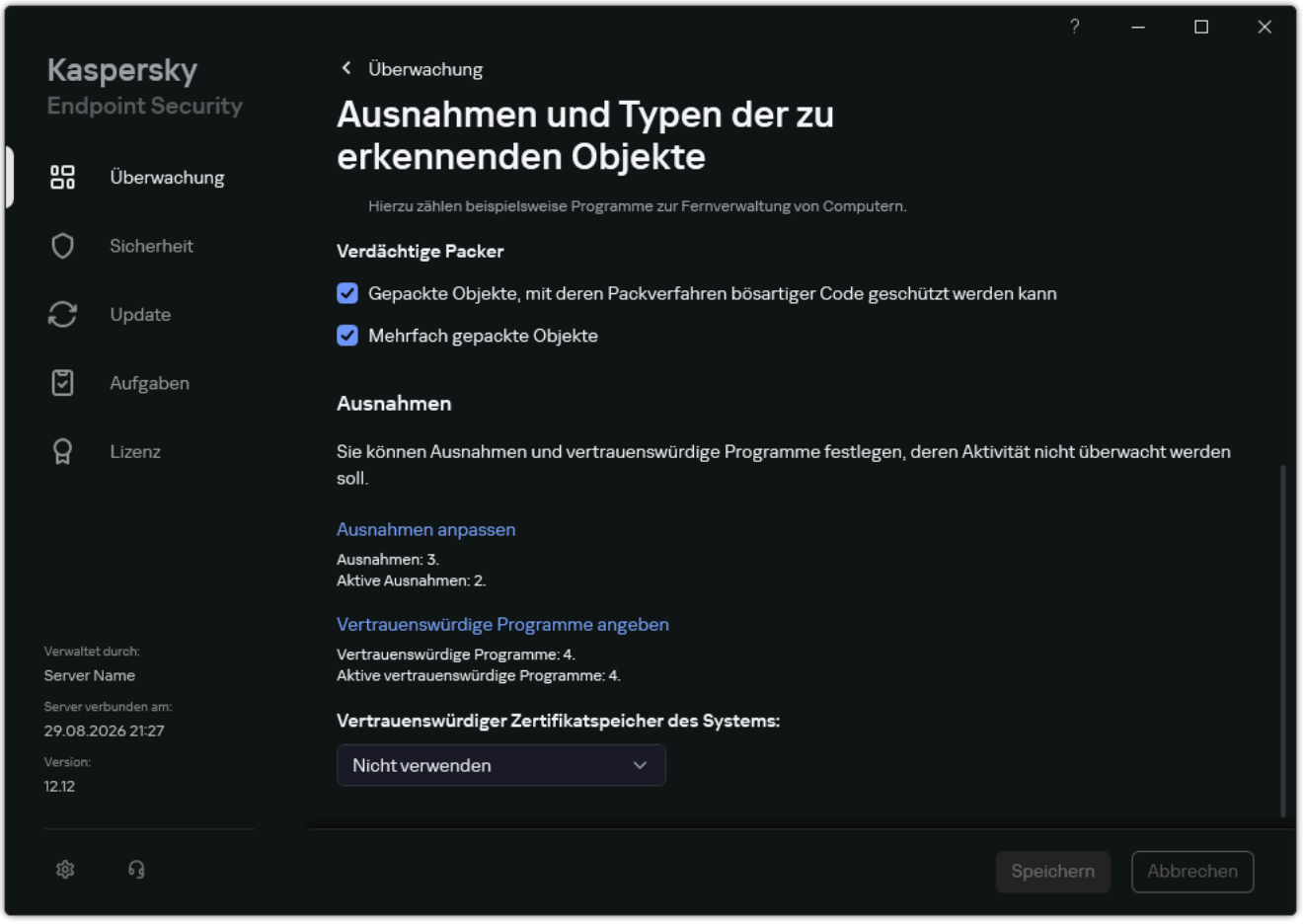
Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Programmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der json-Datei ergänzt werden soll.

9. Speichern Sie die vorgenommenen Änderungen.

So exportieren oder importieren Sie die vertrauenswürdige Zone über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.



Einstellungen für Ausnahmen

3. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.

   b. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten.

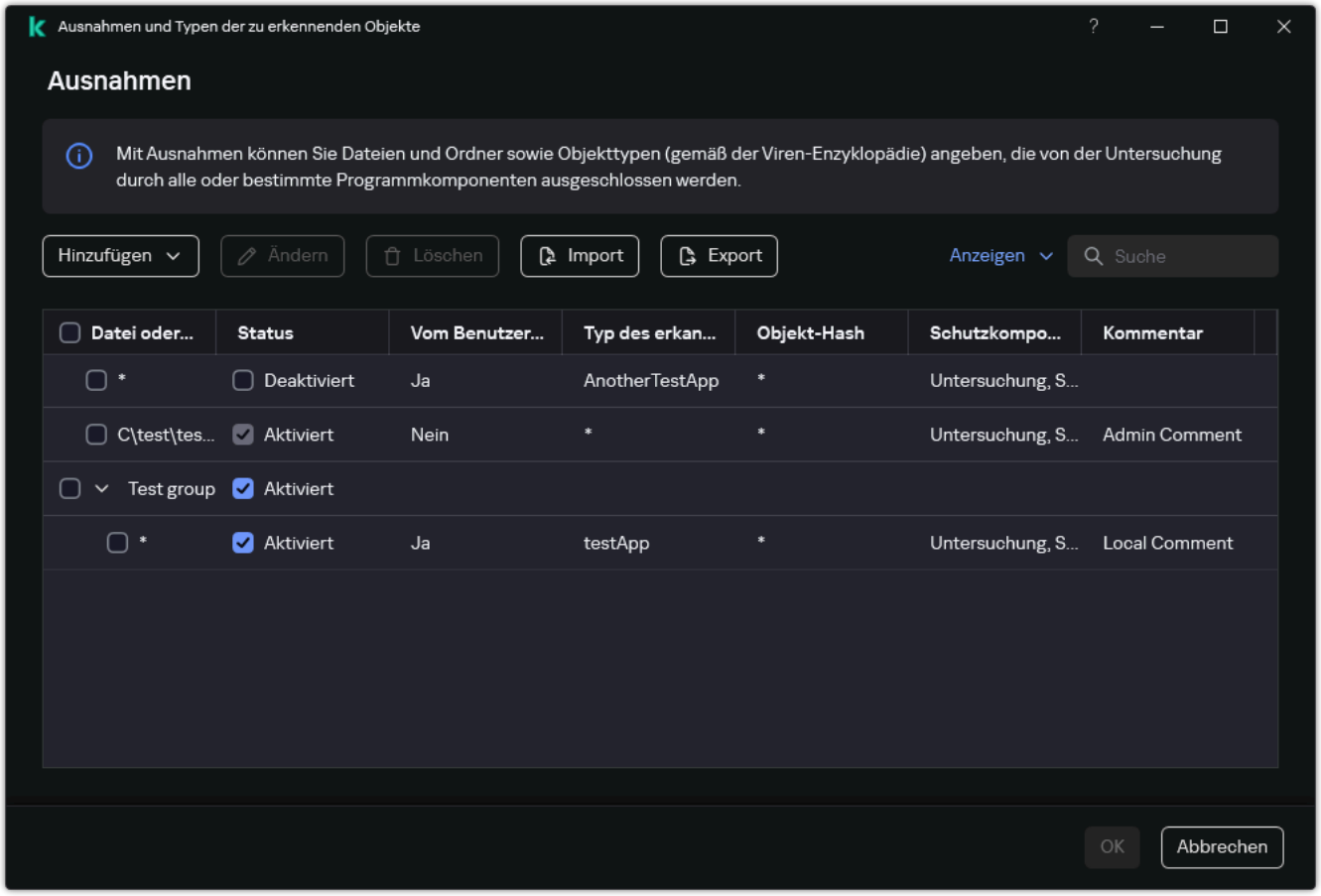
   c. Klicken Sie auf **Export**.

   d. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.

   e. Geben Sie im folgenden Fenster den Namen der CSV-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   f. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Ausnahmen in die CSV-Datei.



Liste der Ausnahmen

4. Um die Liste der vertrauenswürdigen Apps zu exportieren:

   a. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.

   b. Wählen Sie die vertrauenswürdigen Apps aus, die Sie exportieren möchten.

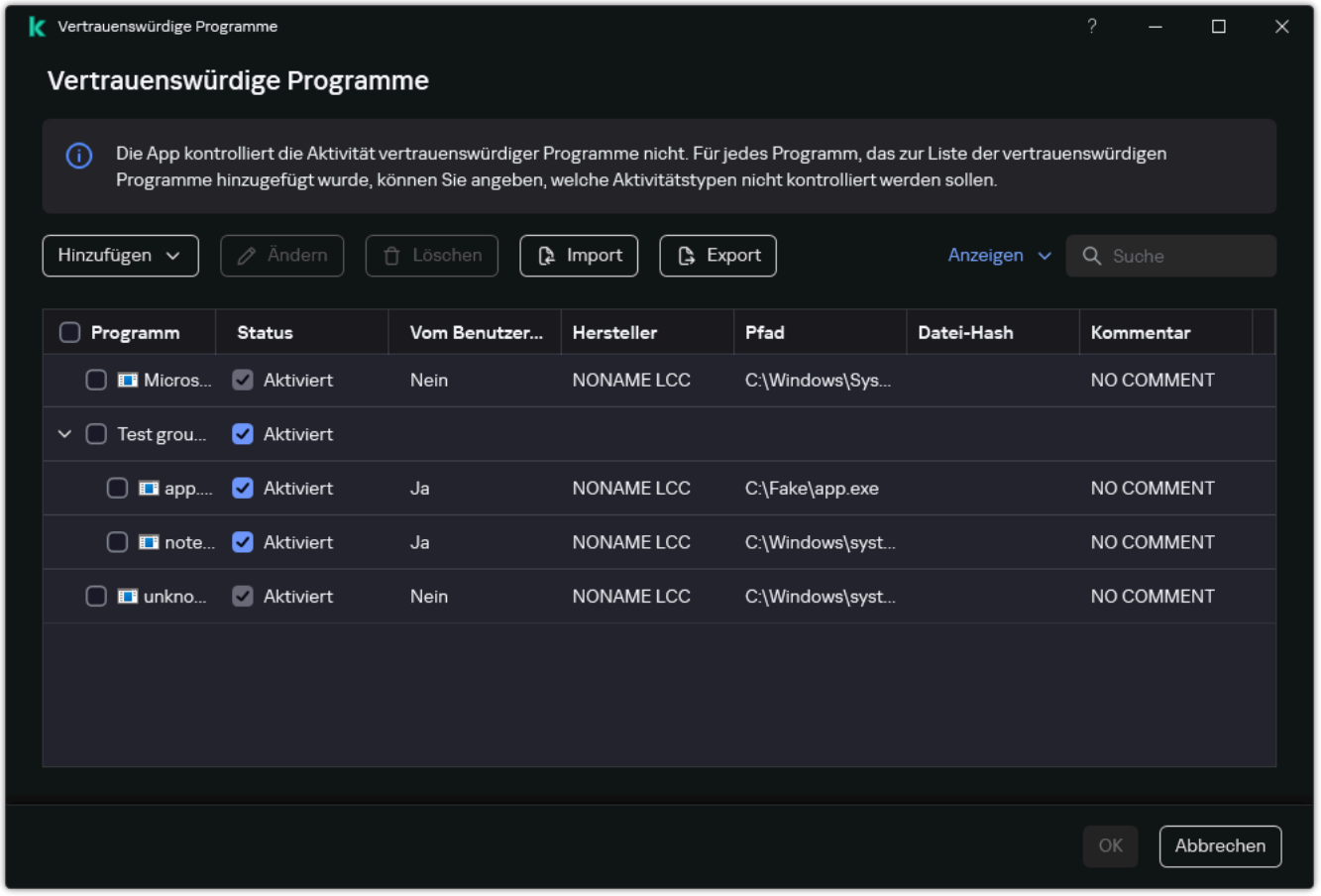
   c. Klicken Sie auf **Export**.

   d. Bestätigen Sie, dass Sie nur die ausgewählten vertrauenswürdigen Apps exportieren möchten, oder exportieren Sie die gesamte Liste.

e. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Namen der XLM-Datei ein, in welche Sie die Liste der vertrauenswürdigen Apps exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

f. Speichern Sie die Datei.

Kaspersky Endpoint Security exportiert die gesamte Liste der vertrauenswürdigen Apps in die XLM-Datei.



Liste der vertrauenswürdigen Programme

5. So importieren Sie die Ausnahmeliste:

a. Klicken Sie im Block **Ausnahmen** auf den Link **Ausnahmen anpassen**.

b. Klicken Sie auf **Import**.

c. Wählen Sie im folgenden Fenster die CSV-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

d. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der CSV-Datei ergänzt werden soll.

6. Um eine Liste mit vertrauenswürdigen Apps zu importieren:

a. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.

b. Klicken Sie auf **Import**.

c. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdiges Apps importieren möchten.

d. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Apps gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

7. Speichern Sie die vorgenommenen Änderungen.

Umgang mit Programmen, die eine vertrauenswürdige digitale Signatur besitzen

Durch die Verwendung des Zertifikatspeichers des Systems können Programme, die eine vertrauenswürdige digitale Signatur besitzen, von der Untersuchung auf Viren ausgeschlossen werden. Kaspersky Endpoint Security weist solche Programme automatisch der Gruppe *Vertrauenswürdig* zu.

So starten Sie die Verwendung des vertrauenswürdigen Systemzertifikatspeichers (in der Verwaltungskonsole (MMC))

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
4. Aktivieren Sie im Block **Vertrauenswürdiger Zertifikatspeicher des Systems** das Kontrollkästchen **Vertrauenswürdigen Zertifikatspeicher des Systems verwenden**.
5. Wählen Sie in der Dropdown-Liste aus, welchen Systemspeicher Kaspersky Endpoint Security als vertrauenswürdig betrachten soll.
6. Speichern Sie die vorgenommenen Änderungen.

So starten Sie die Verwendung des Systemspeichers für vertrauenswürdige Zertifikate (in der Web Console und Cloud Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Vertrauenswürdige Zone**.
5. Klicken Sie im folgenden Fenster auf den Link **Stammzertifikate**.
6. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Vertrauenswürdigen Zertifikatspeicher des Systems verwenden**.

7. Wählen Sie aus, welchen Systemspeicher Kaspersky Endpoint Security als vertrauenswürdig betrachten soll.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So starten Sie die Verwendung des Systemspeichers für vertrauenswürdige Zertifikate (in der Programmoberfläche)

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.

3. Wählen Sie in der Dropdown-Liste **Vertrauenswürdiger Zertifikatspeicher des Systems** aus, welchen Systemspeicher Kaspersky Endpoint Security als vertrauenswürdig betrachten soll.

4. Speichern Sie die vorgenommenen Änderungen.

Anhang. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme

Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Ab Kaspersky Endpoint Security 12.8 für Windows können Sie das Programm im Light Agent-Modus installieren, um virtuelle Umgebungen zu schützen. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren.

Sie haben folgende Möglichkeiten zur Auswahl vordefinierter Ausnahmen und vertrauenswürdiger Programme:

- Programm installieren.
  - Lokale Programminstallation mithilfe des Assistenten
  - Eigenschaften des Installationspakets
- Richtlinieneinstellungen
  - Assistent für neue Richtlinien
  - Richtlinieneinstellungen: Untersuchungsausnahmen und vertrauenswürdige Programme

Microsoft SQL Server

Wenn Sie Kaspersky Endpoint Security auf einem SQL-Server installieren, müssen Sie eine vertrauenswürdige Zone mit vordefinierten Ausnahmen und vertrauenswürdigen Programmen erstellen, damit der Betrieb des Servers nicht beeinträchtigt wird.

Vordefinierte Untersuchungsausnahmen

Pfad	SQL-Version
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange Server

Wenn Sie Kaspersky Endpoint Security auf einem Microsoft Exchange-Server installieren, müssen Sie eine vertrauenswürdige Zone mit vordefinierten Ausnahmen und vertrauenswürdigen Programmen erstellen, damit der Betrieb des Servers nicht beeinträchtigt wird.

Vordefinierte Untersuchungsausnahmen

Pfad	Microsoft Exchange-Version
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019

Pfad	Microsoft Exchange-Version
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

Vordefinierte vertrauenswürdige Programme

Pfad	Microsoft Exchange-Version
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

Wenn Microsoft System Center Configuration Manager im Betriebssystem des geschützten Computers installiert ist, müssen Sie der Liste der Untersuchungsausnahmen eine vordefinierte Ausnahme hinzufügen, um den stabilen Betrieb der Lösung sicherzustellen.

Vordefinierte Untersuchungsausnahmen

Pfad	Version von System Center Configuration Manager
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

Wenn Sie Kaspersky Endpoint Security in einer virtuellen Citrix-Umgebung installieren, müssen Sie eine vertrauenswürdige Zone mit vordefinierten Ausnahmen und vertrauenswürdigen Programmen erstellen, damit der Betrieb des Servers nicht beeinträchtigt wird.

Pfad
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache

Pfad
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

Vordefinierte vertrauenswürdige Programme

Pfad	Citrix-Lösung
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	Virtuelle Apps und Desktops
%SystemRoot%\System32\drivers\CVhdFilter.sys	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\System32\ctxgfx.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	Virtuelle Apps und Desktops
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	Virtuelle Apps und Desktops

Pfad	Citrix-Lösung
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	Virtuelle Apps und Desktops
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	Workspace App
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	Workspace App
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Bereitstellur
%SystemRoot%\System32\drivers\bnistack6.sys	Bereitstellur
%SystemRoot%\System32\drivers\CfsDep2.sys	Bereitstellur
%SystemRoot%\System32\drivers\cnicteam.sys	Bereitstellur

Pfad	Citrix-Lösung
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Bereitstellur
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Bereitstellur
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

Wenn Sie Kaspersky Endpoint Security in einer virtuellen VMware-Umgebung installieren, müssen Sie eine vertrauenswürdige Zone mit vertrauenswürdigen Programmen erstellen, damit der Betrieb des Servers nicht beeinträchtigt wird.

Vordefinierte vertrauenswürdige Programme

Pfad	VMware-Lösung
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon

Pfad	VMware-Lösung
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

Datendeduplizierung in Microsoft Windows Server

Wenn die Datendeduplizierung im Betriebssystem Microsoft Windows Server aktiviert ist, auf dem Kaspersky Endpoint Security installiert ist, müssen Sie ein vordefiniertes vertrauenswürdiges Programm zur Liste Vertrauenswürdige Programme hinzufügen, um Kaspersky Endpoint Security zu optimieren und die CPU-Auslastung zu reduzieren.

Vordefinierte vertrauenswürdige Programme

Pfad	Microsoft Windows Server-Version
%SystemRoot%\system32\fsdmhost.exe	Alle unterstützten Versionen

Arbeit mit dem Backup

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 Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` gespeichert.

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.

In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

Es kann vorkommen, dass Dateien bei der Desinfektion nicht vollständig erhalten bleiben. Wenn wichtige Informationen, die in einer Datei enthalten waren, aufgrund einer Desinfektion vollständig oder teilweise verloren gegangen sind, können Sie versuchen, die Datei aus ihrer Backup-Kopie in den ursprünglichen Ordner der Datei wiederherzustellen.

Wenn Kaspersky Endpoint Security mit Kaspersky Security Center verwaltet wird, können Backup-Kopien für Dateien an den Administrationsserver von Kaspersky Security Center übertragen werden. Details über die Arbeit mit Backup-Kopien für Dateien in Kaspersky Security Center finden Sie im Hilfesystem zu Kaspersky Security Center.

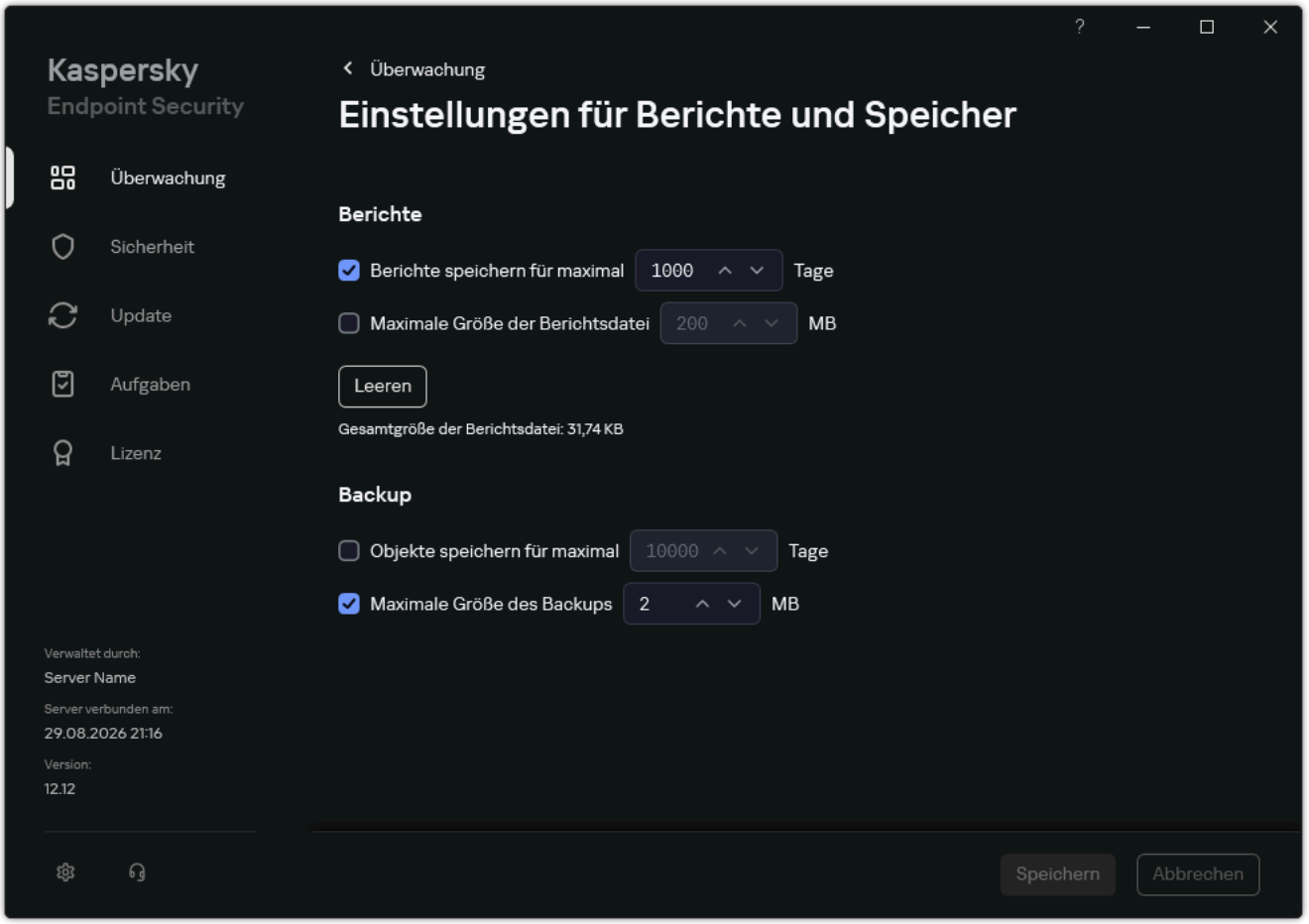
Maximale Speicherdauer für Dateien im Backup anpassen

Die maximale Speicherdauer für Backup-Kopien im Backup beträgt standardmäßig 30 Tage. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup.

Um eine maximale Speicherdauer für Dateien im Backup festzulegen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Allgemeine Einstellungen** auf die Kachel **Berichte und Speicher**.



Backup-Einstellungen

3. Wenn Sie die Speicherdauer für Dateikopien im Backup begrenzen möchten, aktivieren Sie das Kontrollkästchen **Objekte speichern für maximal n Tage** im Block **Backup**. Geben Sie die maximale Speicherdauer für Dateikopien im Backup ein.

4. Speichern Sie die vorgenommenen Änderungen.

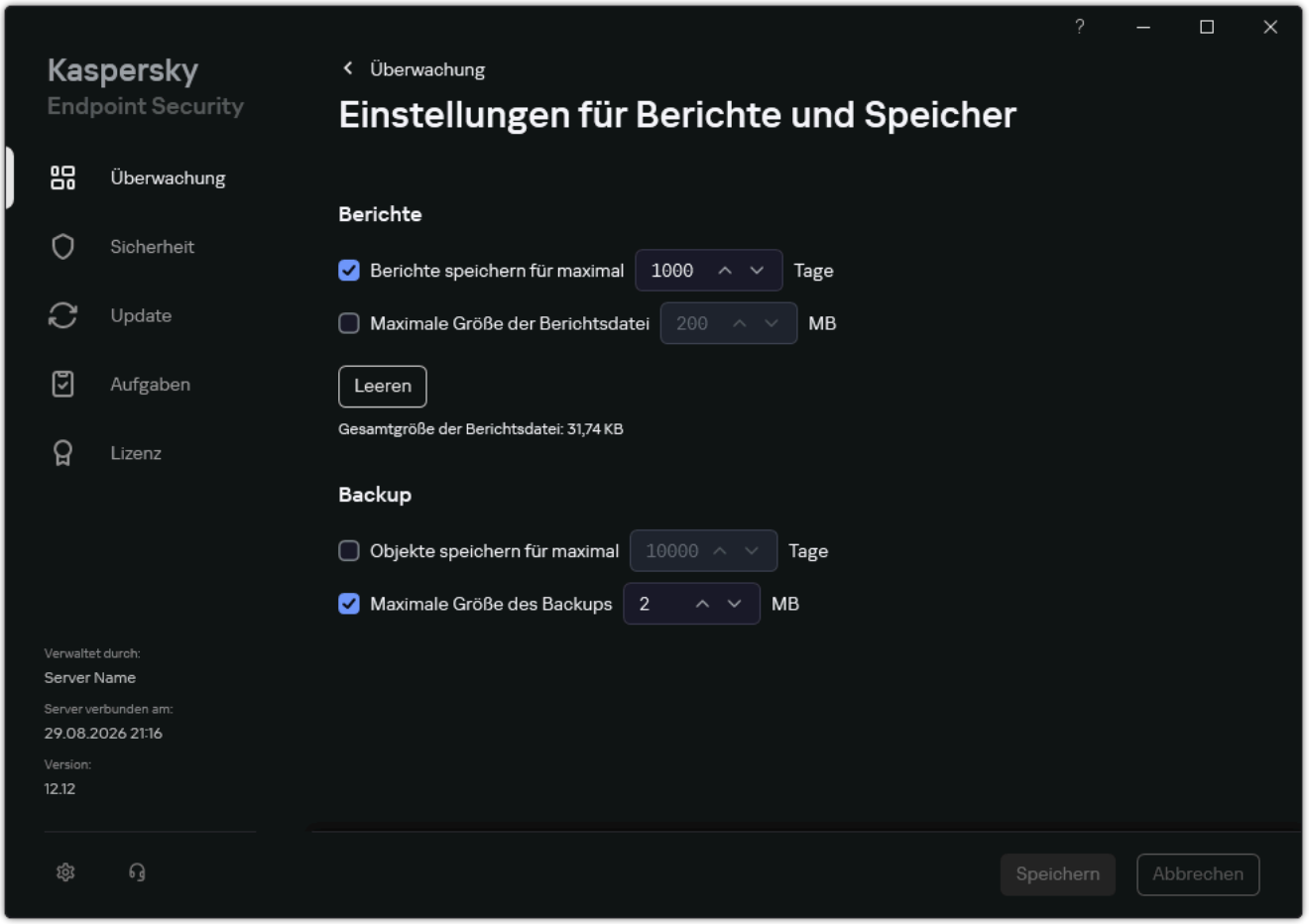
Maximale Größe für das Backup anpassen

Sie können die maximale Größe des Backups angeben. Die Größe des Backups ist standardmäßig nicht beschränkt. Wenn die maximale Größe erreicht wird, löscht Kaspersky Endpoint Security automatisch die ältesten Dateien aus dem Backup.

Um die maximale Größe für das Backup anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Allgemeine Einstellungen** auf die Kachel **Berichte und Speicher**.



Backup-Einstellungen

3. Aktivieren Sie im Block **Backup** das Kontrollkästchen **Maximale Größe des Backups n MB**. Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 1024 MB. 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.

4. Speichern Sie die vorgenommenen Änderungen.

Dateien aus dem Backup wiederherstellen

Wird in einer Datei schädlicher Code gefunden, so blockiert Kaspersky Endpoint Security die Datei, weist Ihr den Status *Nicht desinfiziert* zu, legt eine Backup-Kopie an und führt einen Desinfektionsversuch aus. Wurde die Datei erfolgreich desinfiziert, ändert sich der Status der Backup-Kopie in *Desinfiziert*. Die Datei ist ursprünglichen Speicherordner wieder verfügbar. Falls die Datei nicht desinfiziert werden kann, wird sie von Kaspersky Endpoint Security aus dem Ursprungsordner gelöscht. Sie können die Datei aus einer desinfizierten Backup-Kopie im ursprünglichen Ordner wiederherstellen.

Dateien mit dem Status *Wird beim Neustart des Computers gelöscht* können nicht wiederhergestellt werden. Starten Sie den Computer neu. Danach ändert sich der Dateistatus in *Desinfiziert* oder *Gelöscht*. Nun können Sie die Datei aus ihrer Backup-Kopie im ursprünglichen Ordner wiederherstellen.

Wenn schädlicher Code in einer Datei gefunden wird, die zu einer Anwendung aus dem Windows Store gehört, kopiert Kaspersky Endpoint Security die Datei nicht ins Backup, sondern löscht die Datei sofort. Die Integrität eines Programms aus dem Windows Store kann mithilfe entsprechender Betriebssystem-Tools wiederhergestellt werden (Details über die Wiederherstellung eines Programms aus dem Windows Store finden Sie in der Hilfe zu Microsoft Windows).

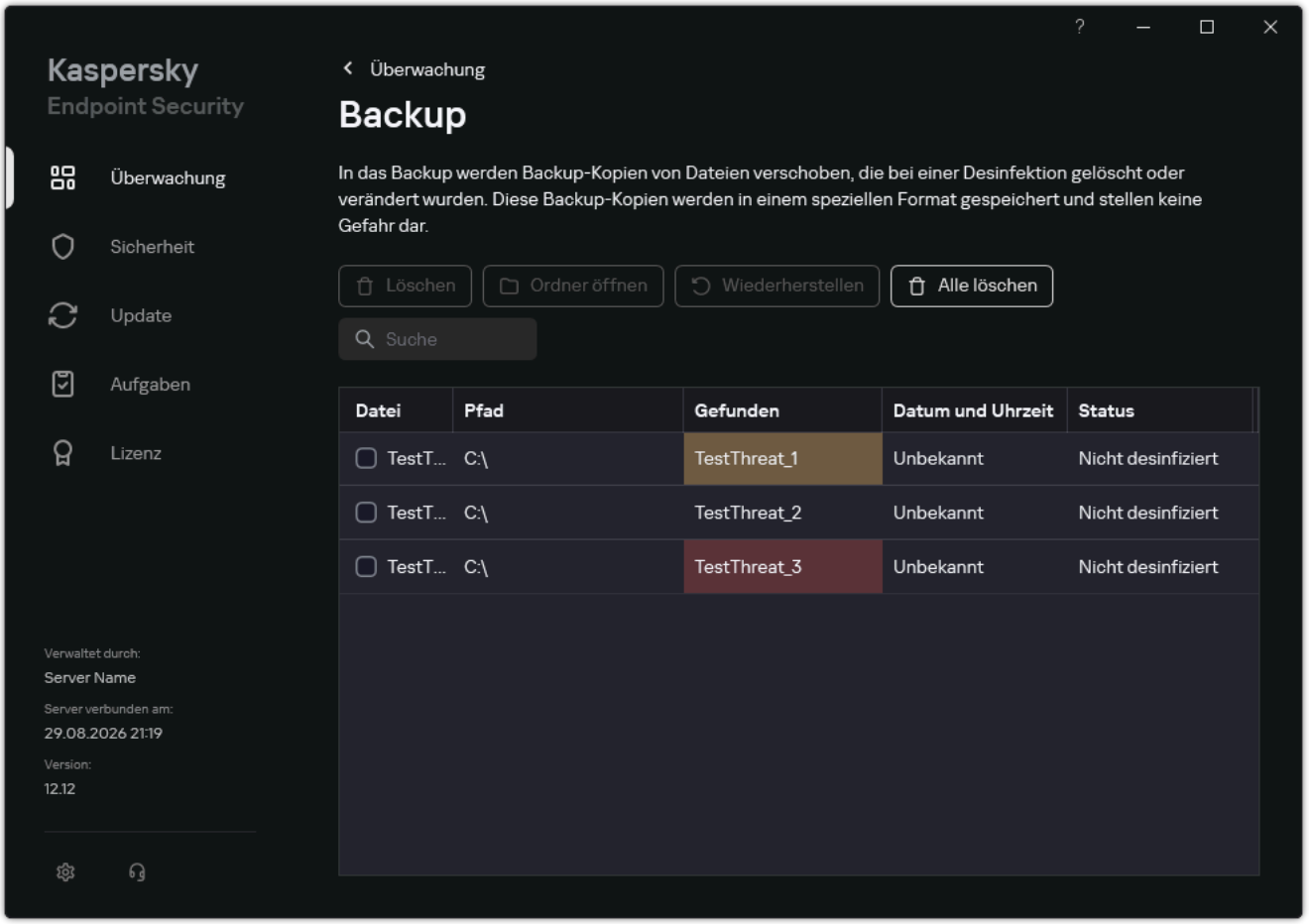
Die Backup-Kopien werden in einer Liste angezeigt. Für die Backup-Kopie einer Datei wird der Pfad des Ordners, an dem diese Datei ursprünglich gespeichert war, angezeigt. Der Pfad des ursprünglichen Ordners der Datei kann persönliche Daten enthalten.

Wenn sich in einem Backup-Ordner mehrere Dateien mit identischen Namen und unterschiedlichen Inhalten befinden, so kann nur jene Datei wiederhergestellt werden, die zuletzt ins Backup verschoben wurde.

Gehen Sie folgendermaßen vor, um Dateien aus dem Backup wiederherzustellen:

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Backup**.
2. Dadurch wird die Liste der Dateien im Backup geöffnet. Wählen Sie in dieser Liste die Dateien aus, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.

Kaspersky Endpoint Security stellt die Dateien aus den ausgewählten Backup-Kopien in den ursprünglichen Ordnern wieder her.



Datenverwaltung

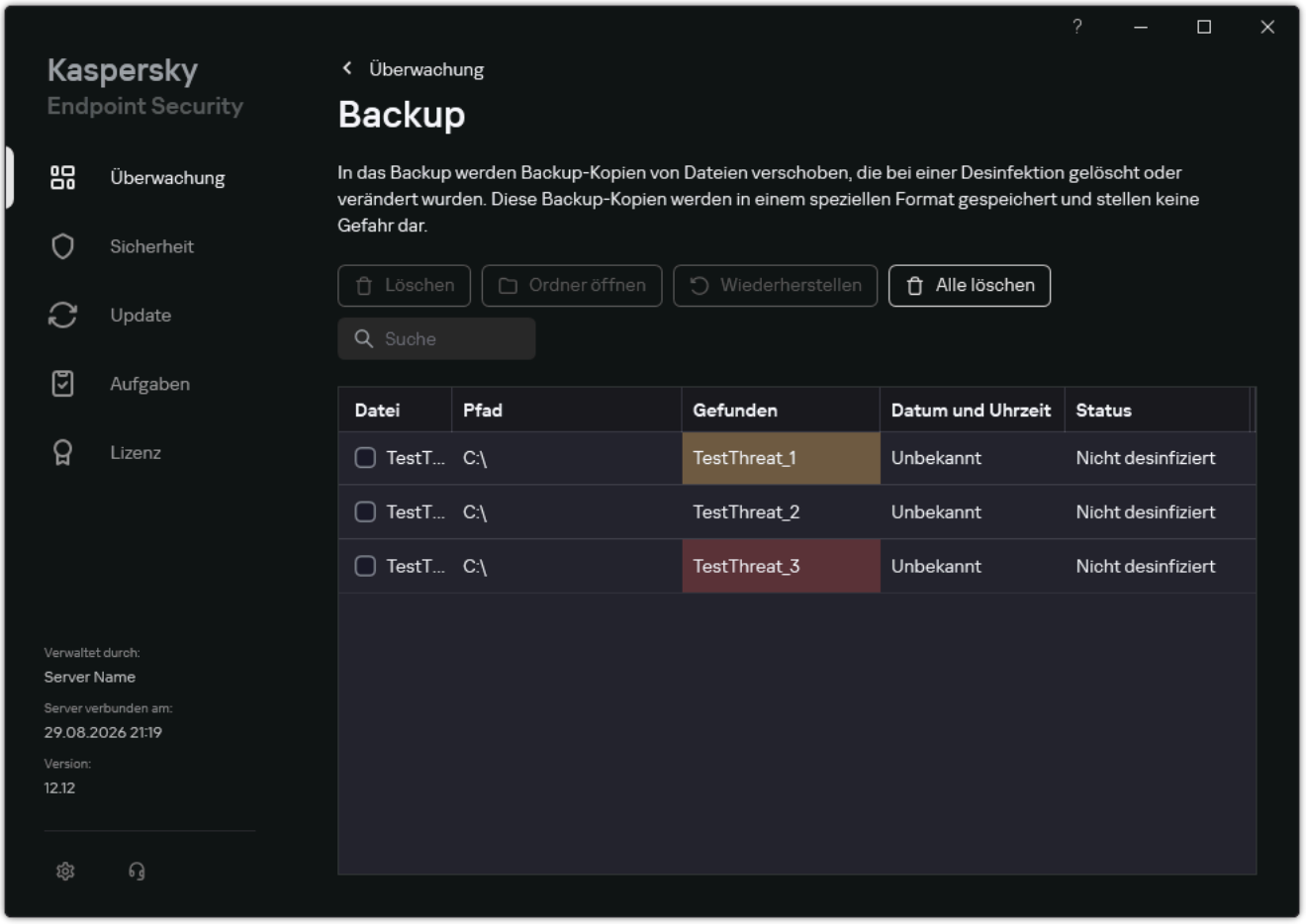
Backup-Kopien von Dateien aus dem Backup löschen

Backup-Kopien, deren maximale Speicherdauer verstrichen ist, werden unabhängig von ihrem Status automatisch aus dem Backup gelöscht. Die Speicherdauer ist in den Programmeinstellungen festgelegt. Sie können eine beliebige Kopie einer Datei auch selbst aus dem Backup löschen.

Gehen Sie folgendermaßen vor, um Backup-Kopien aus dem Backup zu löschen:

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Backup**.
2. Dadurch wird die Liste der Dateien im Backup geöffnet. Wählen Sie in dieser Liste die Dateien aus, die Sie aus dem Backup löschen möchten, und klicken Sie auf **Löschen**.

Kaspersky Endpoint Security löscht die gewählten Backup-Kopien aus dem Backup.



Datenverwaltung

Benachrichtigungsdienst

Während der Ausführung von Kaspersky Endpoint Security treten unterschiedliche Ereignisse ein. Benachrichtigungen über diese Ereignisse können rein informativ sein oder wichtige Informationen enthalten. Eine Benachrichtigung kann beispielsweise über das erfolgreiche Update der Datenbanken und Programm-Module informieren oder auf die Funktionsstörung einer bestimmten Komponente hinweisen, die Sie beheben müssen.

Kaspersky Endpoint Security bietet die Möglichkeit, Informationen über Ereignisse, die im Programm eintreten, im Microsoft Windows-Ereignisbericht und/oder im Bericht für Kaspersky Endpoint Security aufzuzeichnen.

Kaspersky Endpoint Security bietet folgende Optionen für die Zustellung von Benachrichtigungen:

- mithilfe von Pop-up-Benachrichtigungen im Infobereich der Microsoft-Windows-Taskleiste
- per E-Mail

Die Benachrichtigungsmethoden können angepasst werden. Die Benachrichtigungsmethode wird für jeden Ereignistyp konfiguriert.

Wenn Sie mit der Ereignistabelle arbeiten, um den Benachrichtigungsdienst anzupassen, können Sie folgende Aktionen ausführen:

- Filtern der Ereignisse des Benachrichtigungsdienstes nach den Spaltenwerten oder anhand eines komplexen Filters
- Verwenden der Suchfunktion für Ereignisse des Benachrichtigungsdienstes
- Sortieren der Ereignisse des Benachrichtigungsdienstes
- Ändern der Reihenfolge und der Auswahl von Spalten, welche in der Ereignisliste des Benachrichtigungsdienstes angezeigt werden

Einstellungen der Ereignisberichte anpassen

Gehen Sie folgendermaßen vor, um die Einstellungen der Ereignisberichte anzupassen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.
3. Klicken Sie im Block **Meldungen** auf **Benachrichtigungen konfigurieren**.

   Im linken Fensterbereich werden die Komponenten und Aufgaben von Kaspersky Endpoint Security angezeigt. Im rechten Fensterbereich befindet sich eine Ereignisliste für die gewählte Komponente oder für die gewählte Aufgabe.

   In Ereignissen können die folgenden Benutzerdaten enthalten sein:

   - Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden
   - Pfade von Registrierungsschlüsseln, die im Verlauf der Arbeit von Kaspersky Endpoint Security geändert wurden

- Benutzername für Microsoft Windows
- Adressen von Webseiten, die vom Benutzer geöffnet wurden

4. Wählen Sie im linken Fensterbereich die Komponente oder Aufgabe aus, deren Ereignisberichte Sie konfigurieren möchten.
5. Aktivieren Sie für die entsprechenden Ereignisse die Kontrollkästchen in den Spalten **Im lokalen Bericht speichern** und **Im Windows-Ereignisprotokoll speichern**.

   Ereignisse, für welche die Kontrollkästchen in der Spalte **Im lokalen Bericht speichern** aktiviert sind, werden in den Programmberichten angezeigt. Ereignisse, für welche das Kontrollkästchen in der Spalte **Im Windows-Ereignisprotokoll speichern** aktiviert ist, werden in Windows-Protokollen im Kanal `Application` angezeigt.
6. Speichern Sie die vorgenommenen Änderungen.

Anzeige und Versand von Benachrichtigungen anpassen

Um die Anzeige und den Versand von Benachrichtigungen anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.
3. Klicken Sie im Block **Meldungen** auf **Benachrichtigungen konfigurieren**.

   Im linken Fensterbereich werden die Komponenten und Aufgaben von Kaspersky Endpoint Security angezeigt. Im rechten Fensterbereich befindet sich eine Ereignisliste für die gewählte Komponente oder für die gewählte Aufgabe.

   In Ereignissen können die folgenden Benutzerdaten enthalten sein:

   - Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden
   - Pfade von Registrierungsschlüsseln, die im Verlauf der Arbeit von Kaspersky Endpoint Security geändert wurden
   - Benutzername für Microsoft Windows
   - Adressen von Webseiten, die vom Benutzer geöffnet wurden
4. Wählen Sie im linken Fensterbereich die Komponente oder Aufgabe aus, für die der Versand von Meldungen angepasst werden soll.
5. Aktivieren Sie in der Spalte **Auf dem Bildschirm anzeigen** die Kontrollkästchen der entsprechenden Ereignisse.

   Informationen über die gewählten Ereignisse werden auf dem Bildschirm im Infobereich der Microsoft-Windows-Taskleiste als Pop-up-Benachrichtigungen angezeigt.
6. Aktivieren Sie in der Spalte **Per E-Mail benachrichtigen** die Kontrollkästchen der entsprechenden Ereignisse.

   Informationen über die gewählten Ereignisse werden als E-Mail-Nachricht gesendet, wenn die Einstellungen für den Versand von E-Mail-Benachrichtigungen festgelegt sind.
7. Klicken Sie auf **OK**.

8. Wenn Sie E-Mail-Benachrichtigungen aktiviert haben, konfigurieren Sie die Einstellungen für die E-Mail-Zustellung:

   a. Klicken Sie auf **E-Mail-Benachrichtigungen konfigurieren**.

   b. Aktivieren Sie das Kontrollkästchen **Ereignisse melden**, um den Versand zu aktivieren. Benachrichtigungen erfolgen für in Kaspersky Endpoint Security eingetretene Ereignisse, die in der Spalte **Per E-Mail benachrichtigen** markiert sind.

   c. Passen Sie den Versand von E-Mail-Meldungen an.

   d. Klicken Sie auf **OK**.

9. Speichern Sie die vorgenommenen Änderungen.

Anzeige von Warnungen über den Programmstatus im Infobereich anpassen

Um die Anzeige von Warnungen über den Programmstatus im Infobereich der Taskleiste anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.
3. Aktivieren Sie im Block **Programmstatus im Infobereich der Taskleiste anzeigen** die Kontrollkästchen für jene Ereigniskategorien, über die im Infobereich der Microsoft Windows-Taskleiste Benachrichtigungen angezeigt werden sollen.
4. Speichern Sie die vorgenommenen Änderungen.

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 .

Nachrichtenaustausch zwischen Benutzer und Administrator

Die Komponenten Programmkontrolle, Gerätekontrolle, Web-Kontrolle und Adaptive Kontrolle von Anomalien ermöglichen es den Benutzern des lokalen Unternehmensnetzwerks, auf deren Computern das Programm Kaspersky Endpoint Security installiert ist, Nachrichten an den Administrator zu senden.

In folgenden Fällen kann es notwendig sein, dass der Benutzer eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks schicken muss:

- Die Gerätekontrolle hat den Zugriff auf ein Gerät blockiert.

  Eine Nachrichtenvorlage mit einer Zugriffsanfrage für ein blockiertes Gerät steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Gerätekontrolle bereit.

- Die Programmkontrolle hat den Start eines Programms verboten.

  Eine Nachrichtenvorlage mit einer Starterlaubnisanfrage für ein blockiertes Programm steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Programmkontrolle bereit.

- Die Web-Kontrolle hat den Zugriff auf eine Webressource blockiert.

  Eine Nachrichtenvorlage mit einer Zugriffsanfrage für eine blockierte Webressource steht auf der Benutzeroberfläche von Kaspersky Endpoint Security im Abschnitt Web-Kontrolle bereit.

Die Methode für den Nachrichtenversand und die Auswahl der Vorlage hängen davon ab, ob auf dem Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, eine aktive Richtlinie für Kaspersky Security Center vorhanden ist und eine Verbindung mit dem Administrationsserver für Kaspersky Security Center besteht oder nicht. Folgende Szenarien sind möglich:

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, keiner Richtlinie für Kaspersky Security Center, so wird vom Benutzer per E-Mail eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks gesendet.

  Die Nachrichtenfelder werden mit den entsprechenden Werten aus der Vorlage ausgefüllt, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security angegeben ist.

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie für Kaspersky Security Center, so sendet Kaspersky Endpoint Security eine Standardnachricht an den Administrationsserver für Kaspersky Security Center.

  In diesem Fall können die Nachrichten, die von Benutzern stammen, im Ereignisspeicher von Kaspersky Security Center eingesehen werden (s. folgende Anleitung). Die Nachrichtenfelder werden mit den entsprechenden Werten aus der Vorlage ausgefüllt, die in der Richtlinie für Kaspersky Security Center angegeben ist.

- Unterliegt der Computer, auf dem das Programm Kaspersky Endpoint Security installiert ist, einer Richtlinie für Offline-Benutzer für Kaspersky Security Center, so ist die Methode für den Nachrichtenversand davon abhängig, ob eine Verbindung mit Kaspersky Security Center besteht:

  - Besteht eine Verbindung mit Kaspersky Security Center, so sendet Kaspersky Endpoint Security eine Standardnachricht an den Administrationsserver für Kaspersky Security Center.

  - Besteht keine Verbindung mit Kaspersky Security Center, so wird vom Benutzer per E-Mail eine Nachricht an den Administrator des lokalen Unternehmensnetzwerks gesendet.

  In beiden Fällen werden die Nachrichtenfelder mit den entsprechenden Werten aus der Vorlage ausgefüllt, die in der Richtlinie für Kaspersky Security Center angegeben ist.

Um eine vom Benutzer stammende Nachricht im Ereignisspeicher von Kaspersky Security Center anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Ereignisse** aus.

   Im Arbeitsbereich von Kaspersky Security Center werden alle Ereignisse angezeigt, die in Kaspersky Endpoint Security aufgetreten sind. Dazu gehören auch Nachrichten an den Administrator, die von Benutzern des lokalen Unternehmensnetzwerks stammen.

3. Um den Ereignisfilter zu konfigurieren, wählen Sie in der Dropdown-Liste **Ereignisauswahlen** das Element **Benutzeranfragen** aus.

4. Wählen Sie eine Nachricht an den Administrator.

5. Klicken Sie rechts im Arbeitsbereich der Verwaltungskonsole auf **Ereigniseigenschaften öffnen**.

Arbeit mit Berichten

In den 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.

Berichte werden im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\Report` gespeichert.

Die Berichte können die folgenden Benutzerdaten enthalten:

- Pfade von Dateien, die mithilfe von Kaspersky Endpoint Security untersucht wurden
- Pfade von Registrierungsschlüsseln, die im Verlauf der Arbeit von Kaspersky Endpoint Security geändert wurden
- Benutzername für Microsoft Windows
- Adressen von Webseiten, die vom Benutzer geöffnet wurden

Die Daten werden im Bericht als Tabelle angezeigt. Jede Tabellenzeile enthält Informationen zu einem separaten Ereignis. Die Ereignisattribute befinden sich in den Tabellenspalten. Einige Spalten sind nochmals unterteilt und enthalten Unterspalten mit zusätzlichen Attributen. Um zusätzliche Attribute anzuzeigen, klicken Sie auf die Schaltfläche ⊞ neben dem Namen der Spalte. Die Ereignisse, die bei der Ausführung von Komponenten oder bei der Ausführung von Aufgaben registriert werden, besitzen unterschiedliche Attribute.

Folgende Berichte sind verfügbar:

- Bericht für die **Systemaudit**. Enthält Informationen über Ereignisse, welche bei der Interaktion zwischen Benutzer und Programm eintreten, sowie Ereignisse, welche den generellen Programmbetrieb betreffen und sich nicht auf bestimmte Komponenten oder Aufgaben von Kaspersky Endpoint Security beziehen.
- Berichte über die Komponenten von Kaspersky Endpoint Security.
- Berichte über die Ausführung der Aufgaben von Kaspersky Endpoint Security.
- Bericht für die **Datenverschlüsselung**. Enthält Informationen über die Ereignisse, welche bei der Verschlüsselung und Entschlüsselung von Daten auftreten.

In Berichten werden folgenden Prioritätsstufen für Ereignisse verwendet:

ⓘ **Informative Meldungen**. Referenzereignisse mit informativem Charakter, welche in der Regel keine wichtigen Informationen enthalten.

⚠ **Warnungen**. Ereignisse, die beachtet werden müssen, da sie auf wichtige Situationen bei der Ausführung von Kaspersky Endpoint Security hinweisen.

ⓘ **Kritische Ereignisse**. Ereignisse mit kritischer Priorität, die auf Probleme bei der Ausführung von Kaspersky Endpoint Security oder auf Schwachstellen im Schutz des Benutzercomputers hinweisen.

Zur Vereinfachung der Arbeit mit Berichten können Sie die Darstellung der Daten auf dem Bildschirm wie folgt ändern:

- Ereignisliste nach verschiedenen Kriterien filtern
- Funktion zur Suche nach einem bestimmten Ereignis verwenden
- Ausgewähltes Ereignis in einem separaten Block anzeigen
- Ereignisliste nach einer bestimmten Spalte des Berichts sortieren
- Ereignisse, die mithilfe eines Filters gruppiert sind, durch Klick auf die Schaltfläche ⊞ anzeigen und ausblenden
- Reihenfolge und Zusammensetzung der im Bericht angezeigten Spalten ändern

Bei Bedarf können Sie den erstellten Bericht in einer Textdatei speichern. Außerdem können Sie Informationen aus den Berichten löschen. Dazu können die Informationen nach den Komponenten und Aufgaben von Kaspersky Endpoint Security gruppiert werden.

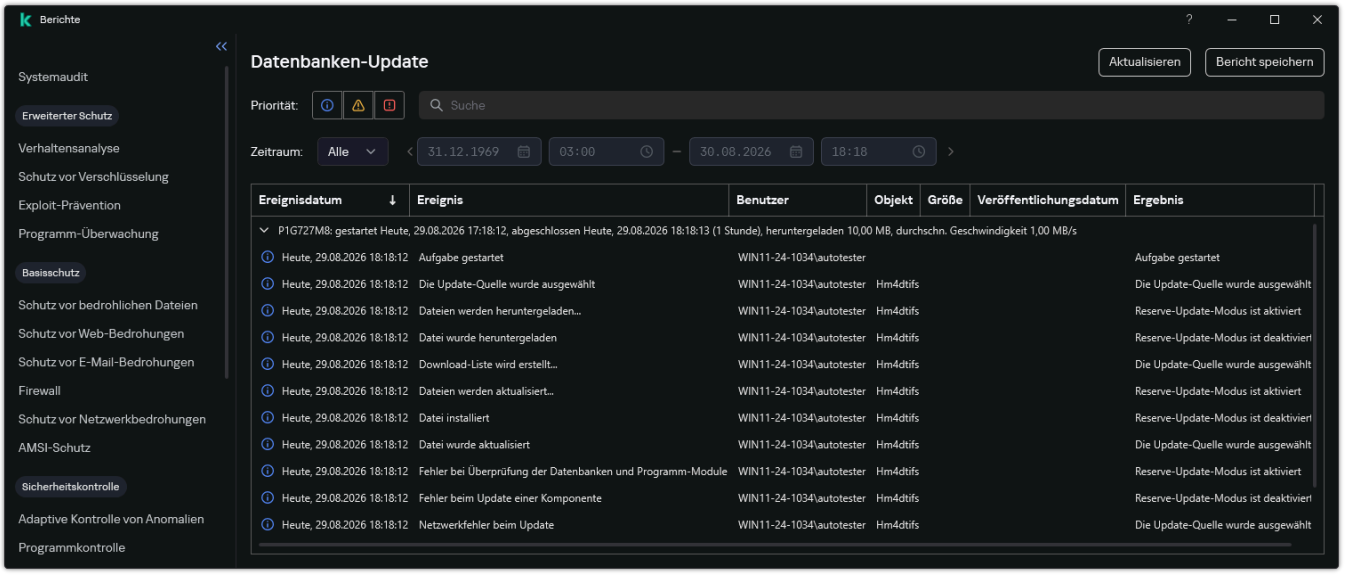
Wenn Kaspersky Endpoint Security mit Kaspersky Security Center verwaltet wird, können Informationen über Ereignisse an den Administrationsserver von Kaspersky Security Center übertragen werden (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

Berichte anzeigen

Ist für einen Benutzer die Anzeige der Berichte verfügbar, so kann dieser Benutzer alle Ereignisse, die in den Berichten vorhanden sind, einsehen.

Um Berichte anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Berichte**.



Berichte

2. Wählen Sie aus der Liste der Komponenten und Aufgaben eine Komponente oder eine Aufgabe aus.

   Im rechten Fensterbereich wird ein Bericht angezeigt, der eine Liste mit Ereignissen für die Ausführungsergebnisse der ausgewählten Komponente oder der ausgewählten Aufgabe von Kaspersky Endpoint Security enthält. Die Ereignisse können im Bericht nach den Werten in den Zellen aus einer der Spalten sortiert werden.

3. Ausführliche Informationen über ein bestimmtes Ereignis finden Sie im Bericht dieses Ereignisses.

Im unteren Fensterbereich wird ein Block mit zusammenfassenden Informationen über das Ereignis angezeigt.

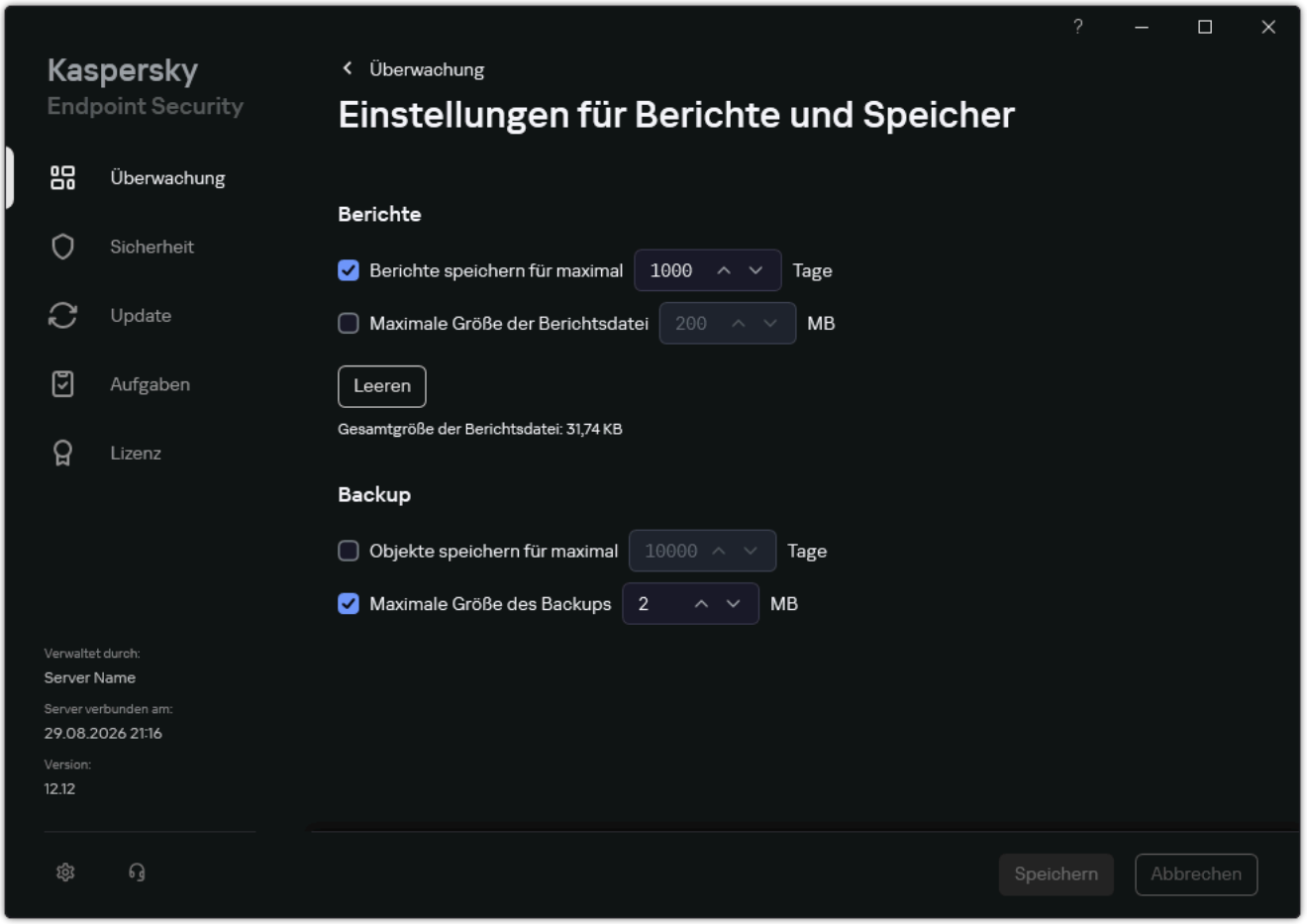
Maximale Speicherdauer für Berichte anpassen

Die standardmäßige Speicherdauer für Berichte über die von Kaspersky Endpoint Security protokollierten Ereignisse beträgt 30 Tage. Nach Ablauf dieses Zeitraums löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei.

Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Ereignisberichte festzulegen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Allgemeine Einstellungen** auf die Kachel **Berichte und Speicher**.



Berichtseinstellungen

3. Wenn Sie die Speicherdauer der Berichte begrenzen möchten, aktivieren Sie das Kontrollkästchen **Berichte speichern für maximal n Tage** im Block **Berichte**. Definieren Sie die maximale Speicherdauer für Berichte.

4. Speichern Sie die vorgenommenen Änderungen.

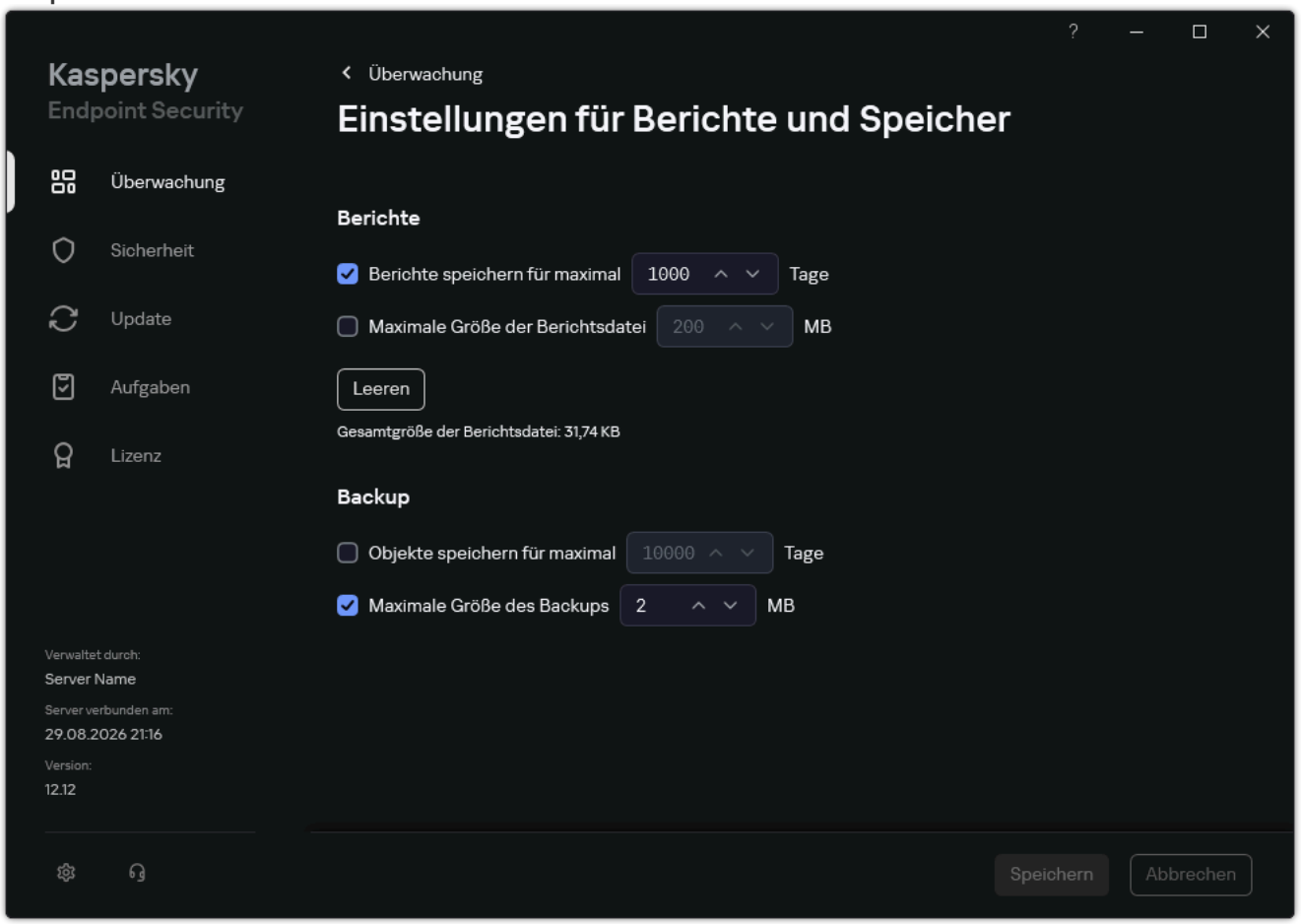
Maximale Größe der Berichtsdatei anpassen

Sie können für die Datei, die den Bericht enthält, eine maximale Größe festlegen. Die maximale Größe der Berichtsdatei ist standardmäßig auf 1024 MB begrenzt. 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.

Gehen Sie folgendermaßen vor, um die maximale Größe einer Berichtsdatei festzulegen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Allgemeine Einstellungen** auf die Kachel **Berichte und Speicher**.



Berichtseinstellungen

3. Aktivieren Sie im Block **Berichte** das Kontrollkästchen **Maximale Größe der Berichtsdatei n MB**, wenn Sie die Größe einer Berichtsdatei begrenzen möchten. Definieren Sie die maximale Größe der Berichtsdatei.

4. Speichern Sie die vorgenommenen Änderungen.

Bericht in Datei speichern

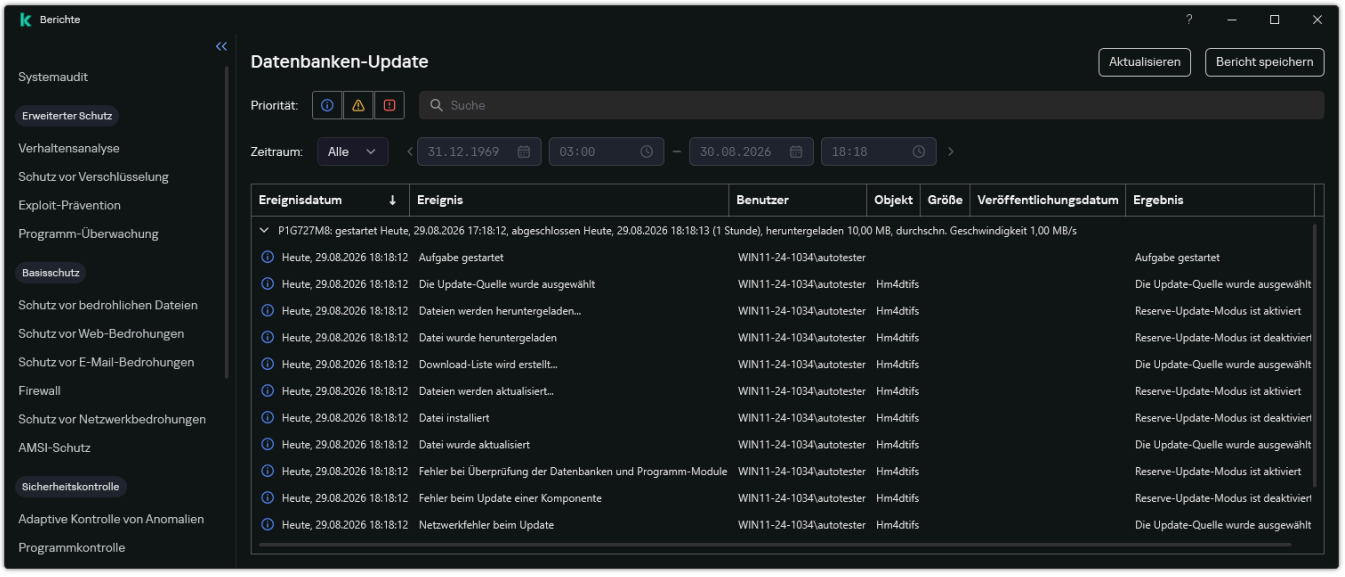
Der Benutzer ist selbst verantwortlich für die Sicherheit der Informationen, welche aus dem Bericht in einer Datei gespeichert werden, und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf diese Informationen.

Der erstellte Bericht kann im Textformat als txt- oder csv-Datei gespeichert werden.

Kaspersky Endpoint Security speichert das Ereignis im Bericht in der gleichen Form, in welcher das Ereignis auf dem Bildschirm angezeigt wird. Die Zusammensetzung und die Reihenfolge der Ereignisattribute bleiben also unverändert.

Gehen Sie folgendermaßen vor, um einen Bericht in einer Datei zu speichern:

1. Klicken Sie im Programmhauptfenster im Abschnitt **Überwachung** auf die Kachel **Berichte**.



Berichte

2. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Komponente oder Aufgabe aus.

   Im rechten Fensterbereich wird ein Bericht angezeigt, der eine Liste mit Ereignissen über die Ausführung der gewählten Komponente oder Aufgabe von Kaspersky Endpoint Security enthält.

3. Die Darstellung der Berichtsdaten kann bei Bedarf mit folgenden Methoden geändert werden:

   - Ereignisse filtern
   - Ereignisse suchen
   - Anordnung der Spalten ändern
   - Ereignisse sortieren

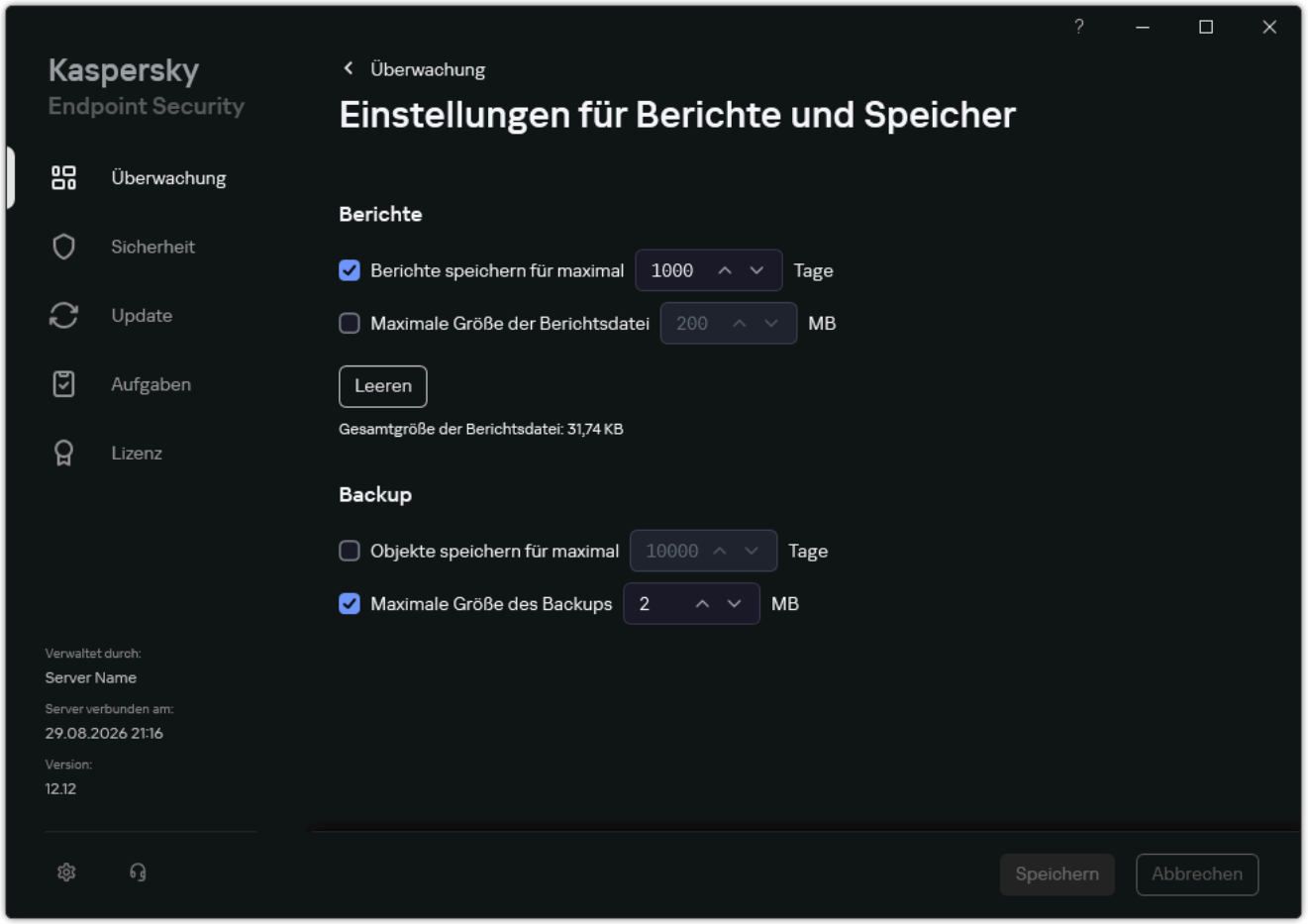
4. Klicken Sie auf die Schaltfläche **Bericht speichern**, die sich rechts oben im Fenster befindet.

5. Geben Sie in dem sich öffnenden Fenster den Zielordner für die Berichtdatei an.
6. Geben Sie den Namen der Berichtsdatei ein.
7. Wählen Sie das gewünschte Format der Berichtsdatei: TXT oder CSV.
8. Speichern Sie die vorgenommenen Änderungen.

Berichte löschen

Gehen Sie folgendermaßen vor, um Informationen aus den Berichten zu löschen.

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Allgemeine Einstellungen** auf die Kachel **Berichte und Speicher**.



Berichtseinstellungen

3. Klicken Sie im Block **Berichte** auf **Leeren**.
4. Wenn der Kennwortschutz aktiviert ist, kann Kaspersky Endpoint Security Sie zur Eingabe der Anmeldedaten für das Benutzerkonto auffordern. Das Programm fordert zur Eingabe der Anmeldedaten für das Konto auf, wenn der Benutzer nicht über die erforderlichen Berechtigung verfügt.

Kaspersky Endpoint Security löscht alle Berichte für alle Programmkomponenten und Aufgaben.

Selbstschutz für Kaspersky Endpoint Security

Der Selbstschutz verhindert, dass andere Programme Aktionen ausführen, die den Betrieb von Kaspersky Endpoint Security beeinträchtigen können. Dazu gehört beispielsweise das Entfernen von Kaspersky Endpoint Security vom Computer. Der Umfang der Selbstschutztechnologien für verfügbaren Kaspersky Endpoint Security hängt davon ab, ob das Betriebssystem 32-Bit oder 64-Bit ist (beachten Sie die folgende Tabelle). Der Selbstschutz umfasst auch den Kennwortschutz und den Verbindungsschutz für den Administrationsserver.

Mit dem *Kennwortschutz* können Sie den Benutzerzugriff auf Kaspersky Endpoint Security gemäß den gewährten Berechtigungen beschränken (z. B. die Berechtigung zum Beenden des Programms).

Der *Verbindungsschutz für den Administrationsserver* verhindert, dass der Computer unerlaubt erneut mit einem nicht vertrauenswürdigen Server verbunden wird.

Selbstschutztechnologien für Kaspersky Endpoint Security

Technologie	Beschreibung	x86-Computer	x64-Computer
Selbstschutz-Modul	Die Technologie blockiert den Zugriff auf die folgenden Anwendungskomponenten: • Dateien im Installationsordner von Kaspersky Endpoint Security und andere Dateien der Anwendung. • Registrierungsschlüssel mit Einträgen, die zur Anwendung gehören. • Prozesse, die von der Anwendung ausgeführt werden.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Die Technologie schützt die Kaspersky Endpoint Security-Prozesse vor schädlichen Aktionen. Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019.	✓	✓
Modul für den Schutz vor externer Steuerung	Diese Technologie verhindert, dass andere Anwendungen (z. B. TeamViewer oder RemotelyAnywhere) Zugriff auf Kaspersky Endpoint Security erhalten.	✓	– (außer Windows 7)

Selbstschutz-Mechanismus aktivieren und deaktivieren

Kaspersky Endpoint Security verhindert, dass App-Dateien auf der Festplatte, Prozesse im Arbeitsspeicher und Einträge in der Systemregistrierung verändert oder gelöscht werden.

Die Technologie blockiert den Zugriff auf die folgenden Anwendungskomponenten:

- Dateien im Installationsordner von Kaspersky Endpoint Security und andere Dateien der Anwendung.
- Registrierungsschlüssel mit Einträgen, die zur Anwendung gehören.
- Prozesse, die von der Anwendung ausgeführt werden.

Die Selbstschutzmechanismen gelten nicht für Prozesse von Kaspersky Endpoint Security, die von nicht vertrauenswürdigen übergeordneten Prozessen initiiert wurden.

Der Selbstschutz-Mechanismus von Kaspersky Endpoint Security ist standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie den Selbstschutz über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
4. Verwenden Sie das Kontrollkästchen **Selbstschutz aktivieren**, um den Selbstverteidigungsmechanismus zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

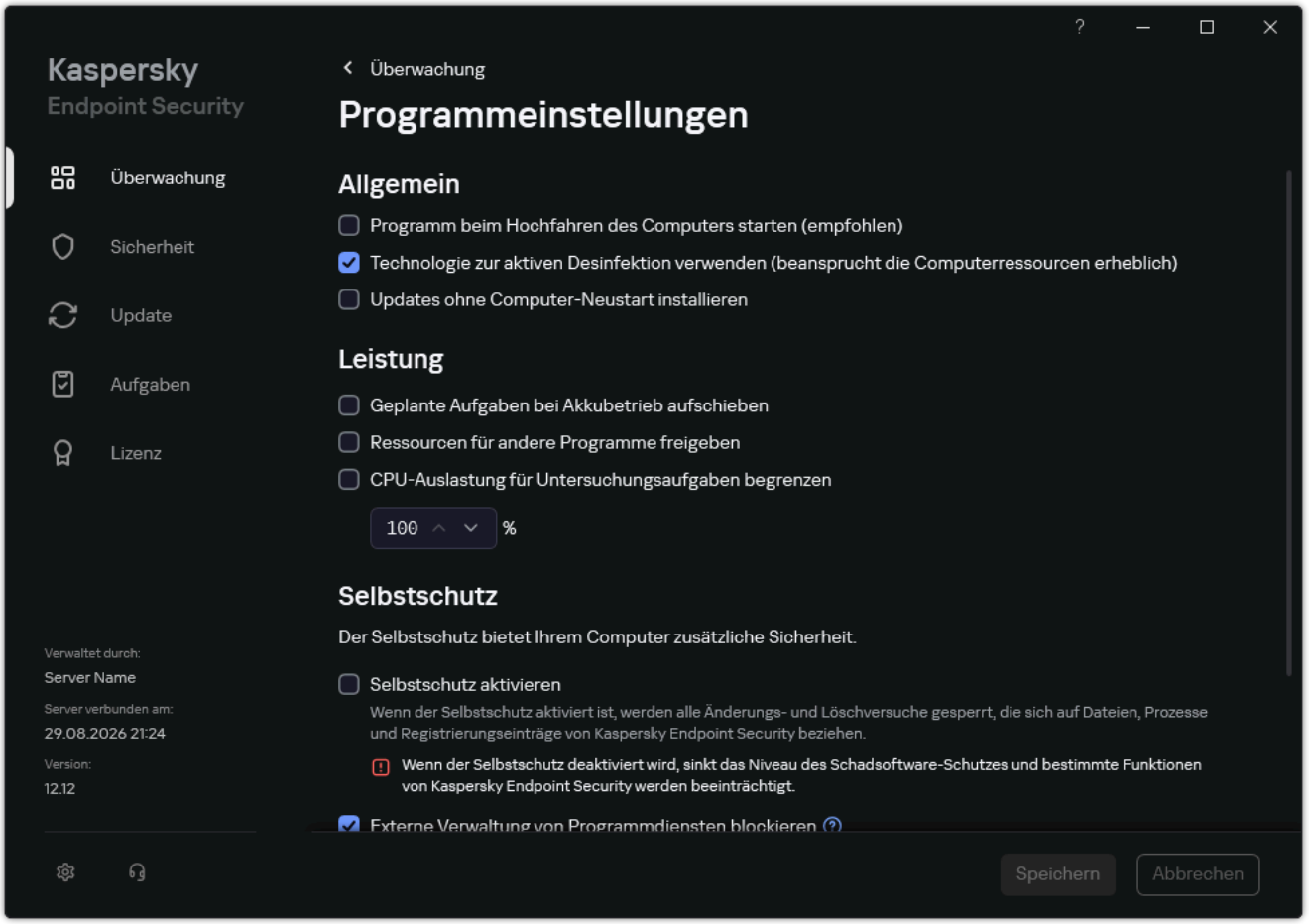
So aktivieren oder deaktivieren Sie den Selbstschutz über die Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Selbstschutz**.
5. Verwenden Sie den Schalter **Selbstschutz AKTIVIERT**, um den Selbstschutz zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie den Selbstschutz über die App-Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Verwenden Sie das Kontrollkästchen **Selbstschutz aktivieren**, um den Selbstverteidigungsmechanismus zu aktivieren oder zu deaktivieren.
4. Speichern Sie die vorgenommenen Änderungen.

Aktivierung und Deaktivierung der AM-PPL-Unterstützung

Kaspersky Endpoint Security unterstützt die Technologie Antimalware Protected Process Light (im Folgenden „AM-PPL“) von Microsoft. AM-PPL schützt die Prozesse von Kaspersky Endpoint Security vor schädlichen Aktionen (z. B. Beenden des Programms). AM-PPL erlaubt nur den Start von vertrauenswürdigen Prozessen. Die Prozesse von Kaspersky Endpoint Security sind gemäß den Anforderungen für die Windows-Sicherheit signiert und sind deshalb vertrauenswürdig. Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Standardmäßig ist die Technologie AM-PPL aktiviert.

Kaspersky Endpoint Security besitzt auch integrierte Schutz-Module für die Programmprozesse. Die AM-PPL-Unterstützung erlaubt es, Funktionen für den Schutz von Prozessen an das Betriebssystem zu delegieren. Dadurch erhöhen Sie die Leistung des Programms und reduzieren den Verbrauch von Computerressourcen.

Die AM-PPL-Technologie muss immer aktiviert sein. AM-PPL ist eine wichtige Komponente für den Schutz des Betriebssystems. Wenn die AM-PPL-Unterstützung deaktiviert wird, funktionieren einige Funktionen von Kaspersky Endpoint Security möglicherweise nicht mehr wie vorgesehen (z. B. die Integration des Programms in Windows Security Center). Die AM-PPL-Unterstützung dar nur in einer separaten Testumgebung zu Fehlerbehebungszwecken deaktiviert werden.

Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019.

Um die AM-PPL-Unterstützung zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Deaktivieren Sie das Modul für den Selbstschutz des Programms.

   Das Selbstschutz-Modul verhindert, dass Programmprozesse im Arbeitsspeicher des Computers verändert und gelöscht werden. Dazu gehört auch eine Änderung des AM-PPL-Status.

2. Starten Sie den Befehlszeileninterpreter cmd als Administrator.

3. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

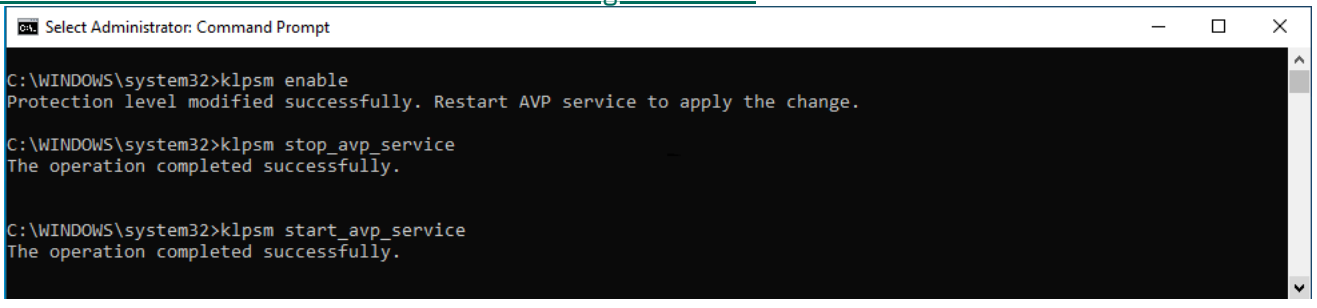
   Den Pfad zur ausführbaren Datei können Sie während der Installation der Anwendung zur Systemvariablen %PATH% hinzufügen.

4. Geben Sie in der Befehlszeile ein:

   - `klpsm.exe enable` – Aktivierung der Unterstützung für die AM-PPL-Technologie (siehe folgende Abb.).
   - `klpsm.exe disable` – Deaktivierung der Unterstützung für die AM-PPL-Technologie.

5. Starten Sie Kaspersky Endpoint Security neu.

6. Setzen Sie das Modul für den Selbstschutz des Programms fort.



Aktivierung der Unterstützung für die AM-PPL-Technologie

Schutz der App-Dienste vor externer Steuerung

Der Schutz der App-Dienste vor externer Steuerung blockiert Versuche von Benutzern und anderen Apps, die Dienste von Kaspersky Endpoint Security zu beenden. Der Schutz bezieht sich auf die folgenden Dienste:

- Kaspersky Endpoint Security-Dienst (AVP.KES.14.2)
- Dienst Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

Um das Programm über die Befehlszeile zu beenden, deaktivieren Sie den Schutz der Kaspersky Endpoint Security-Dienste vor externer Steuerung.

Sie können die externe Verwaltung von Programmdiensten nur auf Computern erlauben, die die AM-PPL-Technologie nicht unterstützen, oder auf Computern, auf denen diese Technologie deaktiviert ist.

So aktivieren oder deaktivieren Sie über die Verwaltungskonsole (MMC) den Schutz der App-Dienste vor externer Steuerung

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
4. Verwenden Sie das Kontrollkästchen **Externe Verwaltung von Programmdiensten blockieren**, um den Schutz der Kaspersky Endpoint Security-Dienste vor externer Steuerung zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie über die Web Console und Cloud Console den Schutz der App-Dienste vor externer Steuerung

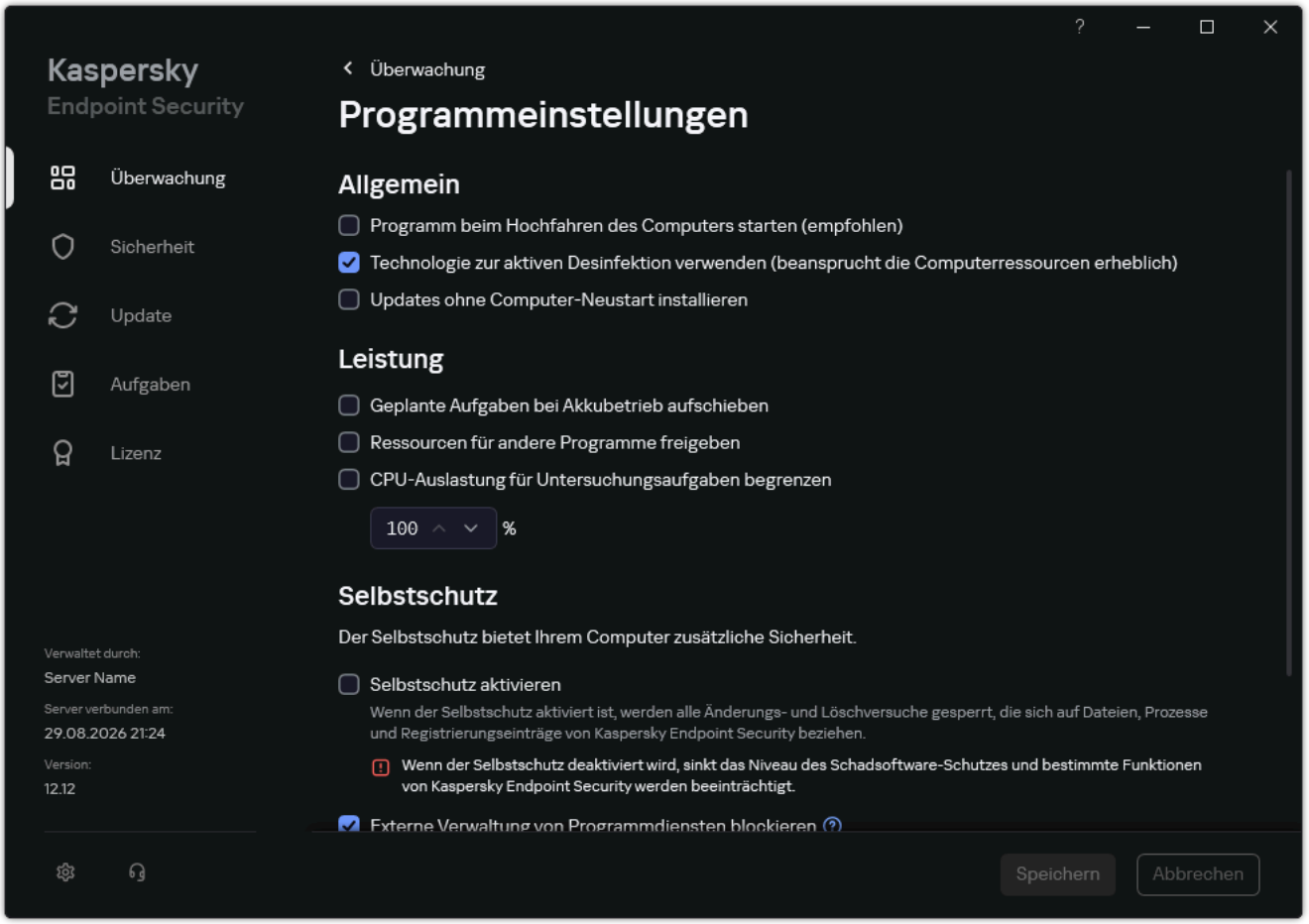
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Selbstschutz**.
5. Verwenden Sie das Kontrollkästchen **Externe Verwaltung von Programmdiensten blockieren**, um den Schutz der Kaspersky Endpoint Security-Dienste vor externer Steuerung zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie über die App-Benutzeroberfläche den Schutz der App-Dienste vor externer Steuerung

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Programmeinstellungen** aus.

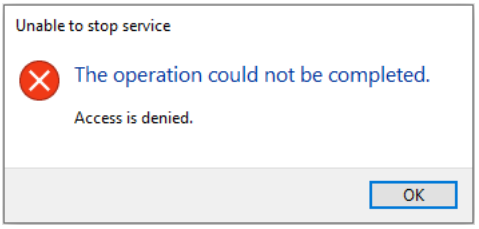


Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Verwenden Sie das Kontrollkästchen **Externe Verwaltung von Programmdiensten blockieren**, um den Schutz der Kaspersky Endpoint Security-Dienste vor externer Steuerung zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Wenn künftig ein Benutzer versucht, die App-Dienste zu beenden, wird ein Systemfenster mit einer Fehlermeldung angezeigt. Der Benutzer kann die App-Dienste nur über die Oberfläche von Kaspersky Endpoint Security verwalten.



Fehler beim Zugriff auf App-Dienste

Gewährleistung der Funktion von Programmen für Remote-Administration

Es kann vorkommen, dass Programme für Remote-Administration eingesetzt werden sollen, während der Schutz vor Fernsteuerung aktiviert ist.

Gehen Sie folgendermaßen vor, um Remote-Administrationsprogramme verwenden zu können:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Ausnahmen und Typen der zu erkennenden Objekte** aus.
3. Klicken Sie im Block **Ausnahmen** auf den Link **Vertrauenswürdige Programme angeben**.
4. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
5. Wählen Sie die ausführbare Datei des Fernverwaltungsprogramms aus.

   Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
6. Aktivieren Sie das Kontrollkästchen **Interaktion mit der Programmoberfläche von Kaspersky Endpoint Security zulassen**.
7. Speichern Sie die vorgenommenen Änderungen.

Kennwortschutz

Es kann sein, dass ein Computer von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern sich unterscheiden. Der uneingeschränkte Zugriff der Benutzer auf Kaspersky Endpoint Security und dessen Einstellungen kann das Sicherheitsniveau des Computers insgesamt beeinträchtigen. Mit dem Kennwortschutz können Sie den Benutzerzugriff auf Kaspersky Endpoint Security gemäß den gewährten Berechtigungen beschränken (z. B. die Berechtigung zum Beenden des Programms).

Wenn ein Benutzer, der die Windows-Sitzung gestartet hat (*Sitzungsbenutzer*), zur Ausführung von Aktionen berechtigt ist, fragt Kaspersky Endpoint Security nicht nach Benutzername und Kennwort oder temporärem Kennwort. Der Benutzer erhält Zugriff auf Kaspersky Endpoint Security gemäß den vorhandenen Berechtigungen.

Wenn der Sitzungsbenutzer nicht zur Ausführung von Aktionen berechtigt ist, kann der Benutzer wie folgt Zugriff auf das Programm erhalten:

- Benutzername und Kennwort eingeben.

  Diese Methode eignet sich für den regulären Einsatz. Um eine kennwortgeschützte Aktion auszuführen, müssen die Daten eines Domänen-Benutzerkontos mit den erforderlichen Berechtigungen eingegeben werden. Dabei muss sich der Computer in einer Domäne befinden. Wenn sich der Computer nicht in einer Domäne befindet, können Sie das Benutzerkonto KLAdmin oder ein manuell hinzugefügtes Benutzerkonto verwenden.

- Temporäres Kennwort eingeben.

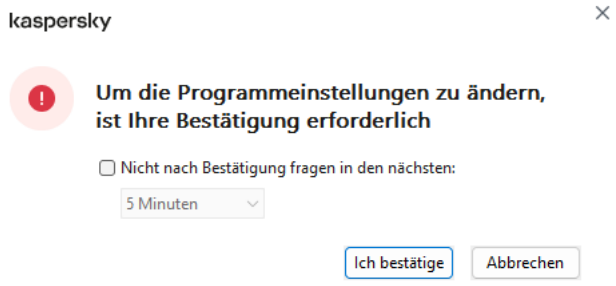
  Diese Methode ist geeignet, wenn sich ein Benutzer außerhalb des Unternehmensnetzwerks befindet und ihm eine temporäre Berechtigung gewährt werden soll, um eine verbotene Aktion auszuführen (z. B. Programm beenden). Nach Ablauf des temporären Kennworts oder nach dem Ende der Sitzung setzt das Programm die Einstellungen von Kaspersky Endpoint Security in den vorherigen Zustand zurück.

- Token.

  Diese Methode eignet sich für privilegierte Benutzer (z. B. Mitarbeiter des Technischen Supports). Die Token-Authentifizierung ermöglicht die Verwendung des Smartcard-Anmeldemodus in Active Directory. Dies erhöht die Sicherheit der Infrastruktur des Unternehmens.

Wenn ein Benutzer versucht, eine kennwortgeschützte Aktion auszuführen, fordert Kaspersky Endpoint Security ihn auf, einen Benutzernamen und ein Kennwort, ein Token-Kennwort oder ein temporäres Kennwort einzugeben (siehe Abbildung unten).

Im Kennworteingabefenster können Sie die Sprache nur mit der Tastenkombination **ALT-UMSCHALT** umschalten. Anderer Tastenkombinationen funktionieren nicht zum Wechseln der Sprache, auch wenn sie im Betriebssystem konfiguriert sind.



Kennwortabfrage für den Zugriff auf Kaspersky Endpoint Security

Benutzername und Kennwort

Um auf Kaspersky Endpoint Security zuzugreifen, müssen Sie die Anmeldedaten des Benutzerkontos eingeben. Der Kennwortschutz unterstützt die Verwendung der folgenden Benutzerkonten:

- **KLAdmin**. Administratorkonto ohne Beschränkungen für den Zugriff auf Kaspersky Endpoint Security. Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen. Die Berechtigung für das KLAdmin-Benutzerkonto kann nicht widerrufen werden. Wenn Sie den Kennwortschutz aktivieren, fordert Kaspersky Endpoint Security Sie auf, ein Kennwort für das KLAdmin-Benutzerkonto festzulegen.

- **Manuell hinzugefügtes Konto**. Ein Benutzerkonto außerhalb der Active Directory-Domäne. Sie können dieses Dienst-Benutzerkonto anstelle von KLAdmin verwenden, wenn Sie das Administratorkennwort nicht mit anderen Personen teilen möchten. Sie können einen beliebigen Benutzernamen und ein Kennwort einrichten und individuelle Berechtigungen konfigurieren.

- **Gruppe „Jeder"**. Windows-Standardgruppe, die alle Benutzer innerhalb des Unternehmensnetzwerks enthält. Die Benutzer aus der Gruppe „Jeder" können gemäß den gewährten Berechtigungen auf das Programm zugreifen.

- **Bestimmte Benutzer oder Gruppen**. Benutzerkonten, für die Sie bestimmte Berechtigungen anpassen können. Wenn beispielsweise eine Aktion für die Gruppe „Jeder“ verboten ist, können Sie die Aktion für einen bestimmten Benutzer oder eine Gruppe erlauben.

- **Sitzungsbenutzer**. Benutzerkonto, unter dem die Windows-Sitzung gestartet wurde. Sie können den Sitzungsbenutzer während der Kennworteingabe ändern (Kontrollkästchen **Kennwort für diese Sitzung speichern**). In diesem Fall weist Kaspersky Endpoint Security anstelle des Benutzers, der die Windows-Sitzung gestartet hat, den Sitzungsbenutzer zu, dessen Anmeldedaten Sie eingegeben haben.

Temporäres Kennwort

Mit dem temporären Kennwort können Sie für einen einzelnen Computer außerhalb des Unternehmensnetzwerks den temporären Zugriff auf Kaspersky Endpoint Security gewähren. Der Administrator erstellt in Kaspersky Security Center in den Eigenschaften des Benutzercomputers ein temporäres Kennwort für einen bestimmten Computer. Der Administrator wählt die Aktionen aus, für die das temporäre Kennwort gilt, und die Gültigkeitsdauer des temporären Kennworts.

Token

Um auf die Funktionen von Kaspersky Endpoint Security zuzugreifen, müssen Sie das entsprechende Benutzerzertifikat aus der Liste der Zertifikate auswählen, die auf dem verbundenen Token gespeichert sind, und Ihre PIN eingeben. Die Token-Authentifizierung ist nur für Benutzer innerhalb der Active Directory-Domäne verfügbar. Der Administrator kann Berechtigungen für einen einzelnen Benutzer oder eine Gruppe konfigurieren. Damit die Token-Authentifizierung funktioniert, müssen Sie eine vertrauenswürdige PKI-Infrastruktur bereitstellen und spezielle Software zur Verwaltung des Tokens installieren.

Kennwortschutz aktivieren

Mit dem Kennwortschutz können Sie den Benutzerzugriff auf Kaspersky Endpoint Security gemäß den gewährten Berechtigungen beschränken (z. B. die Berechtigung zum Beenden des Programms).

So aktivieren Sie den Kennwortschutz über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Benutzeroberfläche** aus.

4. Klicken Sie im Block **Kennwortschutz** auf **Einstellungen**.

   Dadurch wird ein Fenster mit Einstellungen für den Kennwortschutz geöffnet.

5. Verwenden Sie das Kontrollkästchen **Kennwortschutz aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Wählen Sie unter **Berechtigungen** das KLAdmin-Konto aus.

7. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf **Kennwort** und legen Sie ein Kennwort für das KLAdmin-Konto fest.

   Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen.

   > Wenn Sie das Kennwort Ihres KLAdmin-Kontos vergessen haben, können Sie das Kennwort in den Richtlinieneigenschaften zurücksetzen.

8. Gehen Sie zurück zur Kontenliste.

9. Passen Sie Berechtigungen für alle Benutzer im Unternehmensnetzwerk an:

   a. Wählen Sie unter **Berechtigungen** die Gruppe „Jeder“ aus.

      Die *Gruppe „Jeder”* ist die Windows-Standardgruppe, die alle Benutzer innerhalb des Unternehmensnetzwerks enthält.

   b. Aktivieren Sie im angezeigten Fenster die Kontrollkästchen für die Aktionen, die Benutzern ohne vorherige Kennworteingabe zur Verfügung stehen sollen.

      Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **Programm beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

      > Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

10. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie den Kennwortschutz über Web Console und Cloud Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Selbstschutz**.

5. Verwenden Sie unter **Kennwortschutz** den Schalter **Kennwortschutz AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Legen Sie ein Kennwort für das KLAdmin-Benutzerkonto fest und bestätigen Sie es.

   Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen.

Wenn Sie das Kennwort Ihres KLAdmin-Kontos vergessen haben, können Sie das Kennwort in den Richtlinieneigenschaften zurücksetzen.

7. Gehen Sie zurück zur Kontenliste.

8. Passen Sie Berechtigungen für alle Benutzer im Unternehmensnetzwerk an:

   a. Wählen Sie in der Kontentabelle die Gruppe „Jeder“ aus.

      Die *Gruppe „Jeder”* ist die Windows-Standardgruppe, die alle Benutzer innerhalb des Unternehmensnetzwerks enthält.

   b. Aktivieren Sie im angezeigten Fenster die Kontrollkästchen für die Aktionen, die Benutzern ohne vorherige Kennworteingabe zur Verfügung stehen sollen.

      Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **Programm beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

      Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie den Kennwortschutz über der Benutzeroberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.

3. Verwenden Sie den Schalter **Kennwortschutz**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Legen Sie ein Kennwort für das KLAdmin-Benutzerkonto fest und bestätigen Sie es.

   Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen.

   Wenn der Computer einer Richtlinie unterliegt, kann der Administrator das Kennwort für das KLAdmin-Benutzerkonto in den Richtlinieneigenschaften zurücksetzen. Wenn der Computer nicht mit Kaspersky Security Center verbunden ist und Sie das Kennwort für das KLAdmin-Benutzerkonto vergessen haben, kann das Kennwort nicht wiederhergestellt werden.

5. Passen Sie Berechtigungen für alle Benutzer im Unternehmensnetzwerk an:

   a. Klicken Sie in der Tabelle mit Benutzerkonten auf **Ändern**, um die Liste der Berechtigungen für die Gruppe „Jeder“ zu öffnen.

      Die *Gruppe „Jeder”* ist die Windows-Standardgruppe, die alle Benutzer innerhalb des Unternehmensnetzwerks enthält.

   b. Aktivieren Sie die Kontrollkästchen für die Aktionen, die Benutzern ohne Kennworteingabe zur Verfügung stehen sollen.

Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **App beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

6. Speichern Sie die vorgenommenen Änderungen.

Nach der Aktivierung des Kennwortschutzes beschränkt das Programm den Zugriff der Benutzer auf Kaspersky Endpoint Security gemäß den Berechtigungen für die Gruppe „Jeder“. Aktionen, die für die Gruppe „Jeder“ verboten sind, können Sie nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts ausführen.

Sie können den Kennwortschutz nur mithilfe des Benutzerkontos KLAdmin deaktivieren. Der Kennwortschutz kann nicht mithilfe eines anderen Benutzerkontos oder mithilfe eines temporären Kennworts deaktiviert werden.

Während der Kennwortprüfung können Sie das Kontrollkästchen **Kennwort für diese Sitzung speichern** aktivieren. In diesem Fall fordert Kaspersky Endpoint Security keine Kennworteingabe, wenn der Benutzer versucht, während der Sitzung eine andere kennwortgeschützte zulässige Aktion auszuführen.

Berechtigungen für bestimmte Benutzer oder Gruppen gewähren

Mit dem „Kennwortschutz“ können Sie Kaspersky Endpoint Security den Zugriff auf individuelle Active Directory-Benutzerkonten oder manuell hinzugefügte Benutzerkonten gewähren.

Active Directory-Benutzerkonten

Sie können Kaspersky Endpoint Security den Zugriff auf individuelle Benutzer oder Gruppen innerhalb der Active Directory-Domäne gewähren. Wenn beispielsweise die Gruppe „Jeder“ das Programm nicht beenden darf, können Sie einem bestimmten Benutzer die Berechtigung **App beenden** erteilen. In diesem Fall können Sie das Programm nur mithilfe des Kontos dieses Benutzers oder mit dem KLAdmin-Benutzerkonto beenden.

Daten eines Benutzerkontos können nur dann für den Zugriff auf ein Programm verwendet werden, wenn sich der Computer in einer Domäne befindet. Wenn sich der Computer nicht in einer Domäne befindet, können Sie das Benutzerkonto KLAdmin oder ein temporäres Kennwort verwenden.

Manuell hinzugefügte Benutzerkonten

Sie können ein Benutzerkonto erstellen, das in Active Directory nicht vorhanden ist, und diesem Benutzerkonto individuelle Berechtigungen gewähren. Sie können also ein *Dienst-Benutzerkonto* erstellen und es anstelle von KLAdmin verwenden. Dadurch müssen Sie Ihr KLAdmin-Kennwort nicht mit anderen Benutzern teilen oder neue Active Directory-Benutzerkonten erstellen. Sie können einen beliebigen Benutzernamen und ein Kennwort angeben. Beispiel: Sie können dem Dienst-Benutzerkonto die Berechtigung **Berichte anzeigen** gewähren. Wenn das Betrachten von Berichten für die Gruppe „Alle“ verboten ist, können Sie die Berichte mithilfe des Dienst-Benutzerkontos oder des KLAdmin-Benutzerkontos öffnen.

Berechtigungen für bestimmte Benutzer oder Gruppen gewähren

So erteilen Sie über die Verwaltungskonsole (MMC) Berechtigungen für Einzelnutzer oder Gruppen

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Benutzeroberfläche** aus.
4. Klicken Sie im Block **Kennwortschutz** auf **Einstellungen**.

   Dadurch wird ein Fenster mit Einstellungen für den Kennwortschutz geöffnet.
5. Klicken Sie in der Tabelle mit Benutzerkonten auf **Hinzufügen**.
6. Wählen Sie den Typ des Benutzerkontos aus, das Sie hinzufügen möchten:

   - **Benutzer oder Gruppe aus Active Directory auswählen** – Active Directory-Benutzerkonten

     Um ein Benutzerkonto auszuwählen, klicken Sie auf **Auswählen**. Wählen Sie einen Benutzer oder eine Gruppe in Active Directory aus und bestätigen Sie Ihre Auswahl.

   - **Benutzer/Benutzergruppe manuell hinzufügen** für ein manuell hinzugefügtes Dienst-Benutzerkonto.

     Um ein Dienst-Benutzerkonto hinzuzufügen, geben Sie einen Benutzernamen und ein Kennwort ein (z. B. SecureAdmin).

     > Sie können das Kennwort für ein Dienst-Benutzerkonto in den Richtlinieneinstellungen zurücksetzen. Das Dienst-Benutzerkonto muss auf die gleiche Weise zurückgesetzt werden wie das KLAdmin-Kennwort. Wenn die Bearbeitung der Einstellungen für den Kennwortschutz erlaubt ist (das „Schloss“ ist entsperrt) oder keine Richtlinie für den Computer gilt, können Sie das Kennwort des Dienst-Benutzerkontos über die App-Benutzeroberfläche zurücksetzen. Bestätigen Sie dazu mithilfe des KLAdmin-Kennworts die Änderungen der Informationen des Dienst-Benutzerkontos.
7. Aktivieren Sie in der Liste **Berechtigungen** die Kontrollkästchen für jene Aktionen, die dem hinzugefügten Benutzer oder der Gruppe ohne Kennworteingabe zur Verfügung stehen sollen.

Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **Programm beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

> Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

8. Speichern Sie die vorgenommenen Änderungen.

So erteilen Sie einzelnen Benutzern oder Gruppen in der Web Console Berechtigungen

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Selbstschutz**.
5. Klicken Sie im Block **Kennwortschutz** auf den Link **Benutzerberechtigungen**.

   Dadurch wird das Formular geöffnet, in dem Sie Kennwortberechtigungen erteilen können.
6. Klicken Sie auf **Hinzufügen**.
7. Wählen Sie den Typ des Benutzerkontos aus, das Sie hinzufügen möchten:

   - **Aus Active Directory auswählen** – Active Directory-Benutzerkonten

     Um ein Benutzerkonto auszuwählen, klicken Sie auf **Ändern**. Wählen Sie einen Benutzer oder eine Gruppe in Active Directory aus und bestätigen Sie Ihre Auswahl.

   - **Manuell hinzufügen** für ein manuell hinzugefügtes Dienst-Benutzerkonto.

     Um ein Dienst-Benutzerkonto hinzuzufügen, geben Sie einen Benutzernamen und ein Kennwort ein (z. B. SecureAdmin).

     > Sie können das Kennwort für ein Dienst-Benutzerkonto in den Richtlinieneinstellungen zurücksetzen. Das Dienst-Benutzerkonto muss auf die gleiche Weise zurückgesetzt werden wie das KLAdmin-Kennwort. Wenn die Bearbeitung der Einstellungen für den Kennwortschutz erlaubt ist (das „Schloss" ist entsperrt) oder keine Richtlinie für den Computer gilt, können Sie das Kennwort des Dienst-Benutzerkontos über die App-Benutzeroberfläche zurücksetzen. Bestätigen Sie dazu mithilfe des KLAdmin-Kennworts die Änderungen der Informationen des Dienst-Benutzerkontos.
8. Aktivieren Sie in der Liste **Berechtigungen** die Kontrollkästchen für jene Aktionen, die dem hinzugefügten Benutzer oder der Gruppe ohne Kennworteingabe zur Verfügung stehen sollen.

   Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **Programm beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.

9. Klicken Sie auf **Hinzufügen**.
10. Speichern Sie die vorgenommenen Änderungen.

So erteilen Sie über die Benutzeroberfläche der Anwendung Berechtigungen für Einzelnutzer oder Gruppen

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.
3. Klicken Sie in der Tabelle mit Benutzerkonten auf **Hinzufügen**.
4. Wählen Sie den Typ des Benutzerkontos aus, das Sie hinzufügen möchten:
   - **Benutzer oder Gruppe aus Active Directory auswählen** – Active Directory-Benutzerkonten

     Um ein Benutzerkonto auszuwählen, klicken Sie auf **Benutzer oder Gruppe auswählen**. Wählen Sie einen Benutzer oder eine Gruppe in Active Directory aus und bestätigen Sie Ihre Auswahl.
   - **Benutzer manuell hinzufügen** für ein manuell hinzugefügtes Dienst-Benutzerkonto.

     Um ein Dienst-Benutzerkonto hinzuzufügen, geben Sie einen Benutzernamen und ein Kennwort ein (z. B. SecureAdmin).

     Sie können das Kennwort für ein Dienst-Benutzerkonto in den Richtlinieneinstellungen zurücksetzen. Das Dienst-Benutzerkonto muss auf die gleiche Weise zurückgesetzt werden wie das KLAdmin-Kennwort. Wenn die Bearbeitung der Einstellungen für den Kennwortschutz erlaubt ist (das „Schloss“ ist entsperrt) oder keine Richtlinie für den Computer gilt, können Sie das Kennwort des Dienst-Benutzerkontos über die App-Benutzeroberfläche zurücksetzen. Bestätigen Sie dazu mithilfe des KLAdmin-Kennworts die Änderungen der Informationen des Dienst-Benutzerkontos.
5. Aktivieren Sie in der Liste **Berechtigungen** die Kontrollkästchen für jene Aktionen, die dem hinzugefügten Benutzer oder der Gruppe ohne Kennworteingabe zur Verfügung stehen sollen.

   Ist das Kontrollkästchen deaktiviert, so dürfen Benutzer diese Aktion nicht ausführen. Beispiel: Ist das Kontrollkästchen für die Berechtigung **App beenden** deaktiviert, so können Sie das Programm nur mithilfe des KLAdmin-Benutzerkontos, eines separaten Benutzerkontos mit den erforderlichen Berechtigungen oder mithilfe eines temporären Kennworts beenden.

   Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten. Stellen Sie sicher, dass alle Bedingungen für den Zugriff auf Kaspersky Endpoint Security erfüllt sind.
6. Speichern Sie die vorgenommenen Änderungen.

Wenn der Zugriff auf das Programm für die Gruppe „Jeder“ beschränkt ist, können die Benutzer gemäß den Berechtigungen für diese Benutzer auf Kaspersky Endpoint Security zugreifen.

Verwenden eines temporären Kennworts, um Berechtigungen zu gewähren

Mit dem temporären Kennwort können Sie für einen einzelnen Computer außerhalb des Unternehmensnetzwerks den temporären Zugriff auf Kaspersky Endpoint Security gewähren. Dies ist erforderlich, um die Ausführung einer verbotenen Aktion zu erlauben, ohne dem Benutzer die KLAdmin-Anmeldedaten zu übergeben. Um ein temporäres Kennwort zu verwenden, muss der Computer in Kaspersky Security Center hinzugefügt werden.

So erlauben Sie einem Benutzer die Ausführung einer blockierten Aktion mithilfe eines temporären Kennworts über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.
6. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Endpoint Security für Windows (14.2)** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.
7. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Benutzeroberfläche** aus.
8. Klicken Sie im Block **Kennwortschutz** auf **Einstellungen**.
9. Klicken Sie im folgenden Fenster im Block **Temporäres Kennwort** auf die Schaltfläche **Liste der temporären Kennwörter**.

   Das Fenster zur Verwaltung von temporären Kennwörtern wird geöffnet.
10. Klicken Sie auf **Hinzufügen**.
11. Legen Sie im Feld **Gültig bis** die Gültigkeitsdauer für das temporäre Kennwort fest.
12. Aktivieren Sie in der Tabelle **Gültigkeitsbereich des temporären Kennworts** die Kontrollkästchen für jene Vorgänge, auf welche der Benutzer nach der Eingabe des temporären Kennworts zugreifen kann.
13. Klicken Sie auf **Erstellen**.

    Ein Fenster mit einem temporären Kennwort wird geöffnet (siehe Bild unten).
14. Kopieren Sie das Kennwort und übergeben Sie es an den Benutzer.

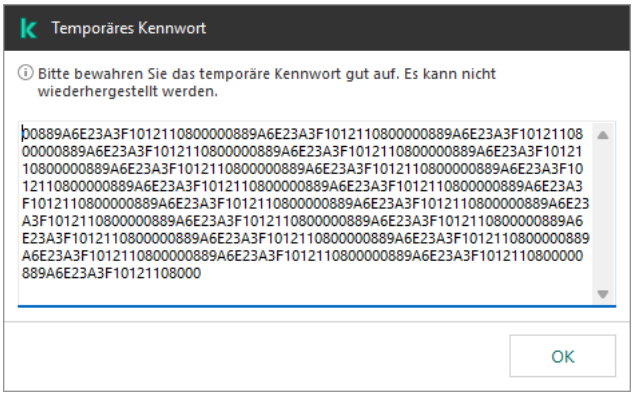
So erlauben Sie einem Benutzer die Ausführung einer blockierten Aktion mithilfe eines temporären Kennworts über die „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie dem Benutzer die Ausführung der blockierten Aktion erlauben möchten.

3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Klicken Sie auf **Kaspersky Endpoint Security für Windows**.

   Die lokalen Programmeinstellungen werden geöffnet.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Benutzeroberfläche** aus.
7. Klicken Sie im Block **Temporäre Kennwörter** auf **Hinzufügen**.
8. Legen Sie im Feld **Gültig bis** die Gültigkeitsdauer für das temporäre Kennwort fest.
9. Aktivieren Sie in der Tabelle **Gültigkeitsbereich des temporären Kennworts** die Kontrollkästchen für jene Vorgänge, auf welche der Benutzer nach der Eingabe des temporären Kennworts zugreifen kann.
10. Klicken Sie auf **Erstellen**.

    Ein Fenster mit dem temporären Kennwort wird geöffnet.
11. Kopieren Sie das Kennwort und übergeben Sie es an den Benutzer.



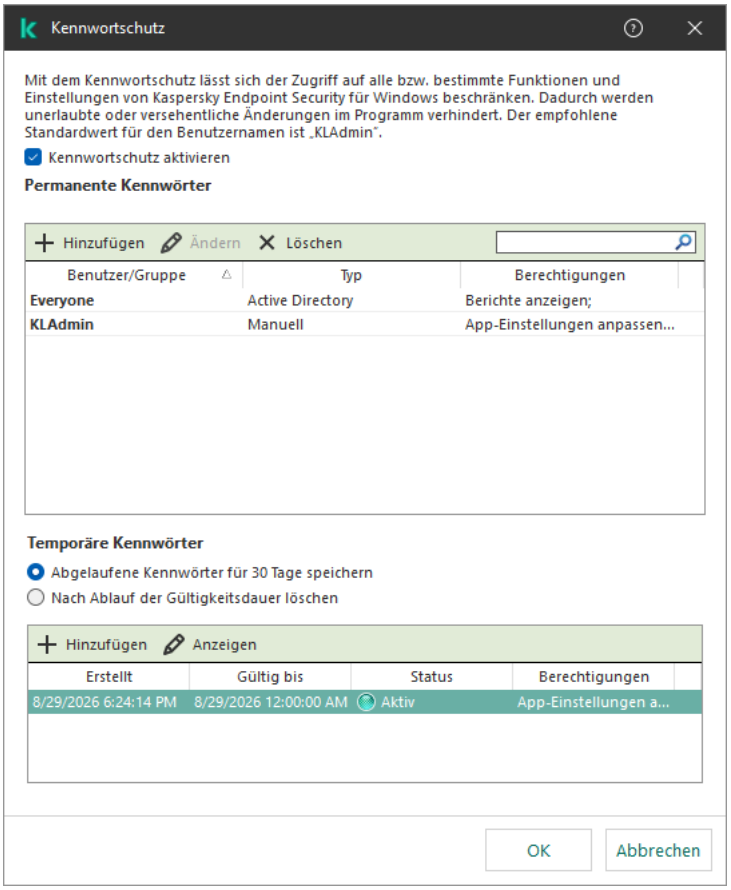
Temporäres Kennwort

Temporäres Kennwort widerrufen

Ab Version 12.9 enthält Kaspersky Endpoint Security für Windows die Funktionalität *Verwaltung temporärer Kennwörter*. Mit der Verwaltung temporärer Kennwörter können Sie die folgenden Aktionen ausführen:

- Kennwortverlauf speichern (bis zu 30 Tage).
- Status des temporären Kennworts überwachen: *Aktiv*, *Abgelaufen*, *Gesperrt*.

- Temporäre Kennwörter widerrufen.



Verwaltung temporärer Kennwörter

Die Verwaltung temporärer Kennwörter aktualisiert den Status des Kennworts und widerruft das Kennwort erst, nachdem der Computer mit Kaspersky Security Center synchronisiert wurde.

So widerrufen Sie ein temporäres Kennwort (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
4. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
5. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.
6. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Endpoint Security für Windows (14.2)** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.
7. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Benutzeroberfläche** aus.
8. Klicken Sie im Block **Kennwortschutz** auf **Einstellungen**.
9. Dadurch wird ein Fenster geöffnet. Passen Sie in diesem Fenster unter **Temporäres Kennwort**, die Einstellungen für das Speichern abgelaufener Kennwörter an.

10. Klicken Sie auf **Liste der temporären Kennwörter**.

    Das Fenster zur Verwaltung von temporären Kennwörtern wird geöffnet. Die Verwaltung temporärer Kennwörter zeigt das Ablaufdatum des Kennworts, den Status des Kennworts und eine Liste mit Berechtigungen an.

11. Wählen Sie das aktive temporäre Kennwort aus, das Sie widerrufen möchten, und doppelklicken Sie auf das Kennwort, um die Eigenschaften zu öffnen.

12. Klicken Sie im angezeigten Fenster auf **Zurückziehen**.

13. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So widerrufen Sie ein temporäres Kennwort (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Klicken Sie auf den Namen des Computers, auf dem Sie dem Benutzer die Ausführung der blockierten Aktion erlauben möchten.

3. Wählen Sie die Registerkarte **Anwendungen** aus.

4. Klicken Sie auf **Kaspersky Endpoint Security für Windows**.

   Die lokalen Programmeinstellungen werden geöffnet.

5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

6. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Benutzeroberfläche** aus.

7. Passen Sie unter **Temporäre Kennwörter** die Speicherung abgelaufener Kennwörter an.

8. Klicken Sie auf den Link **Temporäres Kennwort**.

   Das Fenster zur Verwaltung von temporären Kennwörtern wird geöffnet. Die Verwaltung temporärer Kennwörter zeigt das Ablaufdatum des Kennworts, den Status des Kennworts und eine Liste mit Berechtigungen an.

9. Wählen Sie das aktive temporäre Kennwort aus, das Sie widerrufen möchten.

10. Klicken Sie im angezeigten Fenster auf **Kennwort widerrufen**.

11. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

Dadurch setzt die Verwaltung temporärer Kennwörter den Status des Kennworts auf *Wird zurückgezogen (Synchronisierung mit einem Host)*. Nachdem der Computer mit Kaspersky Security Center synchronisiert wurde, widerruft das Programm das temporäre Kennwort und die gewährten Berechtigungen werden sofort entzogen.

Besonderheiten der Berechtigungen für den Kennwortschutz

Die Berechtigungen für den Kennwortschutz besitzen bestimmte Besonderheiten und Beschränkungen.

App-Einstellungen anpassen

Wenn der Benutzercomputer einer Richtlinie unterliegt, stellen Sie sicher, dass die benötigten Einstellungen in der Richtlinie geändert werden können (dass die Attribute geöffnet sind).

App beenden

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Schutzkomponenten deaktivieren

- Es ist nicht möglich, für die Gruppe „Jeder“ das Deaktivieren von Schutzkomponenten zu erlauben. Um das Deaktivieren von Kontrollkomponenten nicht nur dem Benutzer KLAdmin, sondern auch anderen Benutzern zu erlauben, fügen Sie den Benutzer oder die Gruppe mit der Berechtigung **Schutzkomponenten deaktivieren** in den Einstellungen des „Kennwortschutzes“ hinzu.
- Wenn der Benutzercomputer einer Richtlinie unterliegt, stellen Sie sicher, dass die benötigten Einstellungen in der Richtlinie geändert werden können (dass die Attribute geöffnet sind).
- Um die Schutzkomponenten in den Programmeinstellungen zu deaktivieren, muss der Benutzer über die Berechtigung **App-Einstellungen anpassen** verfügen.
- Zum Deaktivieren von Schutzkomponenten über das Kontextmenü (mit dem Menüpunkt **Schutz anhalten**) muss ein Benutzer neben der Berechtigung **Schutzkomponenten deaktivieren** auch die Berechtigung **Kontrollkomponenten deaktivieren** haben.

Kontrollkomponenten deaktivieren

- Es ist nicht möglich, für die Gruppe „Alle“ das Deaktivieren von Kontrollkomponenten zu erlauben. Um das Deaktivieren von Kontrollkomponenten nicht nur dem Benutzer KLAdmin, sondern auch anderen Benutzern zu erlauben, fügen Sie den Benutzer oder die Gruppe mit der Berechtigung **Kontrollkomponenten deaktivieren** in den Einstellungen des „Kennwortschutzes“ hinzu.
- Wenn der Benutzercomputer einer Richtlinie unterliegt, stellen Sie sicher, dass die benötigten Einstellungen in der Richtlinie geändert werden können (dass die Attribute geöffnet sind).
- Um die Kontrollkomponenten in den Programmeinstellungen zu deaktivieren, muss der Benutzer über die Berechtigung **App-Einstellungen anpassen** verfügen.
- Zum Deaktivieren von Kontrollkomponenten über das Kontextmenü (mit dem Menüpunkt **Schutz anhalten**) muss ein Benutzer neben der Berechtigung **Kontrollkomponenten deaktivieren** auch die Berechtigung **Schutzkomponenten deaktivieren** haben.

Richtlinie für Kaspersky Security Center deaktivieren

Eine Deaktivierung der Richtlinie von Kaspersky Security Center für die Gruppe „Jeder“ kann nicht erlaubt werden. Damit auch andere Benutzer als KLAdmin die Richtlinie deaktivieren können, fügen Sie einen Benutzer oder eine Gruppe mit der Berechtigung **Richtlinie für Kaspersky Security Center deaktivieren** in den „Kennwortschutz“-Einstellungen hinzu.

Schlüssel löschen

Es sind keine Besonderheiten und Beschränkungen vorhanden.

App entfernen/ändern/wiederherstellen

Wenn Sie das Entfernen, Ändern und Wiederherstellen des Programms für die Gruppe „Alle“ erlaubt haben, fordert Kaspersky Endpoint Security kein Kennwort an, wenn der Benutzer versucht, diese Aktionen auszuführen. Daher kann jeder Benutzer, auch Benutzer von außerhalb der Domäne, die Anwendung installieren, ändern oder wiederherstellen.

Zugriff auf Daten auf verschlüsselten Laufwerken wiederherstellen

Sie können den Zugriff auf die Daten auf verschlüsselten Geräten nur mithilfe des KLAdmin-Benutzerkontos wiederherstellen. Es ist nicht möglich, diese Aktion einem anderen Benutzer zu erlauben.

Berichte anzeigen

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Aus dem Backup wiederherstellen

Es sind keine Besonderheiten und Beschränkungen vorhanden.

Einstellungen exportieren

Der Export von Programmeinstellungen in die Gruppe „Alle“ wird standardmäßig verweigert. Sie können Programmeinstellungen mithilfe des Benutzerkontos KLAdmin exportieren. Der Export von Programmeinstellungen umfasst nur das Erstellen einer Konfigurationsdatei mit den Einstellungen von Kaspersky Endpoint Security in der Programmoberfläche. Die Berechtigung erlaubt den Export von Listen mit Untersuchungsausnahmen, vertrauenswürdigen Webadressen, vertrauenswürdigen Geräten oder anderen Listen, die von Programmkomponenten verwaltet werden.

KLAdmin-Kennwort zurücksetzen

Wenn Sie das Kennwort Ihres KLAdmin-Kontos vergessen haben, können Sie das Kennwort in den Richtlinieneigenschaften zurücksetzen. Sie können das Kennwort nicht über die Programmoberfläche zurücksetzen.

Sie können kennwortgeschützte Aktionen mithilfe eines temporären Kennworts ausführen. In diesem Fall müssen Sie die KLAdmin-Anmeldedaten nicht eingeben.

Wenn der Computer nicht mit Kaspersky Security Center verbunden ist und Sie das Kennwort für das KLAdmin-Benutzerkonto vergessen haben, kann das Kennwort nicht wiederhergestellt werden.

So setzen Sie das Kennwort für das KLAdmin-Konto über die Verwaltungskonsole (MMC) zurück

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Benutzeroberfläche** aus.
4. Klicken Sie im Block **Kennwortschutz** auf **Einstellungen**.
5. Deaktivieren Sie im angezeigten Fenster das Kontrollkästchen **Kennwortschutz aktivieren**.
6. Speichern Sie die vorgenommenen Änderungen.
7. Aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** wieder.
8. Klicken Sie auf **OK**.

   Dadurch wird das Administratorkennwort-Fenster geöffnet.
9. Legen Sie ein neues Kennwort für das KLAdmin-Benutzerkonto fest und bestätigen Sie es.
10. Speichern Sie die vorgenommenen Änderungen.

So setzen Sie das Kennwort des KLAdmin-Kontos über die „Web Console“ oder „Cloud Console“ zurück

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.
   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Klicken Sie auf **Kaspersky Endpoint Security für Windows 14.2**.
   Die lokalen Programmeinstellungen werden geöffnet.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Gehen Sie zu **Allgemeine Einstellungen** → **Selbstschutz**.
7. Deaktivieren Sie unter **Kennwortschutz** den Schalter **Kennwortschutz**.
8. Speichern Sie die vorgenommenen Änderungen.
9. Aktivieren Sie den Schalter **Kennwortschutz** wieder.
10. Legen Sie ein neues Kennwort für das KLAdmin-Benutzerkonto fest und bestätigen Sie es.
11. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird das Kennwort Ihres KLAdmin-Kontos aktualisiert, nachdem die Richtlinie angewendet wurde.

Schutz der Verbindung zum Administrationsserver

Die Verbindung des Computers mit dem Administrationsserver erfolgt mithilfe der Kaspersky Security Center-Komponente *Administrationsagent*. Wenn ein Angreifer ausreichende Rechte hat, um die Einstellungen der Serververbindung zu ändern, besteht ein Risiko für die Verbindung des Computers mit einem nicht vertrauenswürdigen Server. Dann könnte der Angreifer seine eigenen Gruppenrichtlinien anwenden und beispielsweise den Selbstschutz der App deaktivieren. Kaspersky Endpoint Security kann eine unerlaubte Wiederverbindung des Computers mit unterschiedlichen Servern verhindern. Zum Schutz der Serververbindung schlägt das Programm vor, ein Kennwort festzulegen und die Funktion Password-Based key Derivation Function (PBKDF2) zu verwenden. Dies hat zur Folge, dass der Zugriff auf die App ohne Kennwort nicht möglich ist.

Um Kaspersky Endpoint Security und den Administrationsagenten umfassend vor unerlaubtem Zugriff zu schützen, empfehlen wir, den zusätzlichen Schutz zu aktivieren. Für Kaspersky Endpoint Security empfehlen wir, den Kennwortschutz zu aktivieren. Für den Schutz der Administrationsagenten zu empfehlen wir, ein Kennwort für die Deinstallation festzulegen. Einzelheiten darüber, wie Sie den Administrationsagenten vor einer Deinstallation schützen, finden Sie in der Hilfe zu Kaspersky Security Center.

Die Verwaltung der Verbindung zwischen dem Computer und dem Administrationsserver erfolgt mithilfe der Aufgabe *Schutz der Verbindung zum Administrationsserver*. Mit dieser Aufgabe können Sie die folgenden Aktionen ausführen:

- Ein Kennwort festlegen, um die Serververbindung zu schützen.
- Das Kennwort ändern.

- Den Computer mit einem anderen Server neu verbinden.
- Den Schutz der Serververbindung deaktivieren.

Authentifizierung des Computers bei der Verbindung mit dem Administrationsserver

Nachdem ein Kennwort festgelegt wurde, erstellt die App ein Daten-Array, wobei das Kennwort mithilfe von PBKDF2 umgewandelt wird. Dann verschlüssel die App dieses Daten-Array mithilfe des Schlüssels des Administrationsagenten. Die App verwendet das verschlüsselte Daten-Array, um Rechte und Berechtigungen des Administrationsservers für spätere Verbindungen zu überprüfen.

Wenn künftig versucht wird, den Computer erneut mit dem Administrationsserver zu verbinden, entschlüsselt die App das Daten-Array mithilfe des Administrationsagenten-Schlüssels und vergleicht es mit der lokalen Kopie. Wenn sie nicht übereinstimmen, wird der Zugriff auf die App beschränkt.

Schutz der Verbindung zum Administrationsserver

So legen Sie über die Verwaltungskonsole (MMC) ein Kennwort zum Schutz der Serververbindung fest

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Schutz der Verbindung zum Administrationsserver** aus.

Schritt 2. Schutz der Verbindung mit dem Administrationsserver

Legen Sie ein Kennwort zum Schutz der Verbindung mit dem Administrationsserver fest:

1. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Durch Kennwort schützen** auswählen.
2. Wählen Sie in der Dropdown-Liste **Administrationsserver** die Option **Neuer Server**.
3. Legen Sie im Feld **Kennwort für die Verbindung zum Administrationsserver** ein Kennwort für die Verbindung zum Administrationsserver fest und bestätigen Sie es.

   Falls Sie das Kennwort vergessen sollten, können Sie es mithilfe einer Aufgabe ändern.

4. Wenn Sie Kaspersky Endpoint Security 12.7 oder eine ältere Version des Programms bereitgestellt haben, aktivieren Sie das Kontrollkästchen **Kompatibilität der Kennwortverschlüsselung für ältere Programmversionen (12.7 und älter) aktivieren**.

   Ab der Version Kaspersky Endpoint Security 12.8 für Windows verwendet das Programm eine stärkere Verschlüsselung für Kennwörter. Wenn Sie Kaspersky Endpoint Security 12.8 oder höher installiert haben, empfehlen wir Ihnen, dieses Kontrollkästchen zu deaktivieren und die stärkere Kennwortverschlüsselung zu verwenden. Ältere Versionen des Programms unterstützen die sichere Kennwortverschlüsselung nicht. Um die Aufgabe auszuführen, müssen Sie das Kontrollkästchen aktivieren.

Schritt 3: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie den Punkt **Standardbenutzerkonto**. Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

Schritt 4. Zeitplan des Aufgabenstarts anpassen

Wählen Sie unter **Start nach Zeitplan** den Punkt **Manuell** auswählen.

Schritt 5. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, z. B. *Kennwort für Verbindung mit Hauptserver*.

Schritt 6. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** oder starten Sie die Aufgabe manuell. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So legen Sie über Web Console oder Cloud Console ein Kennwort zum Schutz der Serververbindung fest

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Schutz der Verbindung zum Administrationsserver**.

c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Kennwort für Verbindung mit Hauptserver*.

d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie ein standardmäßiges Benutzerkonto aus. Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Schutz der Verbindung zum Administrationsserver**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Durch Kennwort schützen** auswählen.

10. Wählen Sie in der Dropdown-Liste **Verbindung zum Administrationsserver** die Option **Neues Kennwort**.

11. Legen Sie im Feld **Kennwort für die Verbindung zum Administrationsserver** ein Kennwort für die Verbindung zum Administrationsserver fest und bestätigen Sie es.

    Falls Sie das Kennwort vergessen sollten, können Sie es mithilfe einer Aufgabe ändern.

12. Wenn Sie Kaspersky Endpoint Security 12.7 oder eine ältere Version des Programms bereitgestellt haben, aktivieren Sie das Kontrollkästchen **Kompatibilität der Kennwortverschlüsselung für ältere Programmversionen (12.7 und älter) aktivieren**.

    Ab der Version Kaspersky Endpoint Security 12.8 für Windows verwendet das Programm eine stärkere Verschlüsselung für Kennwörter. Wenn Sie Kaspersky Endpoint Security 12.8 oder höher installiert haben, empfehlen wir Ihnen, dieses Kontrollkästchen zu deaktivieren und die stärkere Kennwortverschlüsselung zu verwenden. Ältere Versionen des Programms unterstützen die sichere Kennwortverschlüsselung nicht. Um die Aufgabe auszuführen, müssen Sie das Kontrollkästchen aktivieren.

13. Speichern Sie die vorgenommenen Änderungen.

14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf **Starten**.

Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen.

Den Computer mit einem anderen Administrationsserver neu verbinden

Eine erneute Verbindung des Computers mit einem anderen Administrationsserver umfasst die folgenden Schritte:

1. Führen Sie in der Konsole des aktuellen `[KSC1]`-Servers die Aufgabe *Administrationsserver wechseln* für den Administrationsagenten aus.

Nachdem die Aufgabe ausgeführt wurde, wird der Computer mit dem neuen [KSC2]-Server verbunden.

Der Computer wird in der Serverkonsole [KSC1] mit dem Status *Kritisch* angezeigt. Es ist nicht möglich, die App mithilfe von Richtlinien zu konfigurieren oder per Fernzugriff Aufgaben auf dem Computer auszuführen.

2. Erstellen Sie in der Konsole des neuen [KSC2]-Servers einen neue Aufgabe *Schutz der Verbindung zum Administrationsserver* für Kaspersky Endpoint Security. Geben Sie in den Aufgabeneigenschaften das Kennwort des vorherigen Servers ein und legen Sie ein Kennwort für den neuen Server fest.

So legen Sie in der Verwaltungskonsole (MMC) ein neues Kennwort für die Wiederverbindung mit einem neuen Server fest

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2) → Schutz der Verbindung zum Administrationsserver** aus.

Schritt 2. Schutz der Verbindung mit dem Administrationsserver

Legen Sie ein Kennwort fest, um die Verbindung zum neuen Administrationsserver zu schützen:

1. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Durch Kennwort schützen** auswählen.

2. Wählen Sie in der Dropdown-Liste **Administrationsserver** die Option **Von anderem Server wiederverbinden**.

3. Geben Sie im Feld **Aktuelles Kennwort** das Kennwort ein, das für die Verbindung zum zuvor verwendeten vertrauenswürdigen Server festgelegt wurde.

4. Legen Sie im Feld **Neues Kennwort** ein Kennwort für die Verbindung zum neuen Administrationsserver fest und bestätigen Sie das Kennwort.

   Falls Sie das Kennwort vergessen sollten, können Sie es mithilfe einer Aufgabe ändern.

5. Wenn Sie Kaspersky Endpoint Security 12.7 oder eine ältere Version des Programms bereitgestellt haben, aktivieren Sie das Kontrollkästchen **Kompatibilität der Kennwortverschlüsselung für ältere Programmversionen (12.7 und älter) aktivieren**.

   Ab der Version Kaspersky Endpoint Security 12.8 für Windows verwendet das Programm eine stärkere Verschlüsselung für Kennwörter. Wenn Sie Kaspersky Endpoint Security 12.8 oder höher installiert haben, empfehlen wir Ihnen, dieses Kontrollkästchen zu deaktivieren und die stärkere Kennwortverschlüsselung zu verwenden. Ältere Versionen des Programms unterstützen die sichere Kennwortverschlüsselung nicht. Um die Aufgabe auszuführen, müssen Sie das Kontrollkästchen aktivieren.

Schritt 3: Konto zur Ausführung der Aufgabe auswählen

Wählen Sie den Punkt **Standardbenutzerkonto**. Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

Schritt 4. Zeitplan des Aufgabenstarts anpassen

Wählen Sie unter **Start nach Zeitplan** den Punkt **Manuell** auswählen.

Schritt 5. Aufgabennamen festlegen

Geben Sie einen Aufgabennamen ein, z. B. *Kennwort für Verbindung mit Hauptserver*.

Schritt 6. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** oder starten Sie die Aufgabe manuell. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So legen Sie in Web Console und Cloud Console ein neues Kennwort für die Wiederverbindung mit einem neuen Server fest

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Schutz der Verbindung zum Administrationsserver**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Kennwort für Verbindung mit Hauptserver*.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Wählen Sie ein standardmäßiges Benutzerkonto aus. Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Schutz der Verbindung zum Administrationsserver**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Durch Kennwort schützen** auswählen.

10. Wählen Sie in der Dropdown-Liste **Verbindung zum Administrationsserver** die Option **Von anderem Server wiederverbinden**.

11. Geben Sie im Feld **Aktuelles Kennwort** das Kennwort ein, das für die Verbindung zum zuvor verwendeten vertrauenswürdigen Server festgelegt wurde.

12. Legen Sie im Feld **Neues Kennwort** ein Kennwort für die Verbindung zum neuen Administrationsserver fest und bestätigen Sie das Kennwort.

    Falls Sie das Kennwort vergessen sollten, können Sie es mithilfe einer Aufgabe ändern.

13. Wenn Sie Kaspersky Endpoint Security 12.7 oder eine ältere Version des Programms bereitgestellt haben, aktivieren Sie das Kontrollkästchen **Kompatibilität der Kennwortverschlüsselung für ältere Programmversionen (12.7 und älter) aktivieren**.

    Ab der Version Kaspersky Endpoint Security 12.8 für Windows verwendet das Programm eine stärkere Verschlüsselung für Kennwörter. Wenn Sie Kaspersky Endpoint Security 12.8 oder höher installiert haben, empfehlen wir Ihnen, dieses Kontrollkästchen zu deaktivieren und die stärkere Kennwortverschlüsselung zu verwenden. Ältere Versionen des Programms unterstützen die sichere Kennwortverschlüsselung nicht. Um die Aufgabe auszuführen, müssen Sie das Kontrollkästchen aktivieren.

14. Speichern Sie die vorgenommenen Änderungen.

15. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

16. Klicken Sie auf **Starten**.

    Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen.

Stellen Sie nach Abschluss der Aufgabe sicher, dass der Computer in der Konsole des neuen `[KSC2]`-Servers den Status *OK* hat. Testen Sie, ob Sie per Fernzugriff Aufgaben ausführen und die App mithilfe von Richtlinien konfigurieren können.

Kennwort für die Verbindung zum Administrationsserver zurücksetzen

Wenn Sie das Kennwort für die Verbindung zum Administrationsserver vergessen haben oder das Kennwort kompromittiert ist, können Sie das Kennwort in den Aufgabeneigenschaften zurücksetzen. Sie können das Kennwort auch zurücksetzen und ein neues Kennwort für eine Gruppe von Computern festlegen, die unterschiedliche Schutzstatusvarianten für die Verbindung zum Administrationsserver haben. Wenn der Schutz für einige Computer aktiviert und für einige deaktiviert ist, legt die Aufgabe in diesem Fall ein Kennwort für alle Computer fest.

Sie können das Kennwort für die Verbindung zum Administrationsserver nur in der Konsole des vertrauenswürdigen Servers zurücksetzen, mit dem der Computer verbunden ist.

So setzen Sie das Kennwort für die Verbindung zum Administrationsserver über die Verwaltungskonsole (MMC) zurück

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Wählen Sie die Aufgabe **Schutz der Verbindung zum Administrationsserver** aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
5. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Schützen und Kennwort ändern** auswählen.
6. Legen Sie im Feld **Kennwort für die Verbindung zum Administrationsserver** ein neues Kennwort für die Verbindung zum aktuellen vertrauenswürdigen Server fest und bestätigen Sie das Kennwort.
7. Speichern Sie die vorgenommenen Änderungen.
8. Führen Sie die Aufgabe aus.

So setzen Sie das Kennwort für die Verbindung zum Administrationsserver über Web Console oder Cloud Console zurück

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Schutz der Verbindung zum Administrationsserver**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Schützen und Kennwort ändern** auswählen.
5. Legen Sie im Feld **Kennwort für die Verbindung zum Administrationsserver** ein neues Kennwort für die Verbindung zum aktuellen vertrauenswürdigen Server fest und bestätigen Sie das Kennwort.
6. Speichern Sie die vorgenommenen Änderungen.

7. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.
8. Klicken Sie auf **Starten**.

Dies hat zur Folge, dass das Kennwort für die Verbindung zum Administrationsserver nach Abschluss der Aufgabe zurückgesetzt wird.

Schutz der Verbindung zum Administrationsserver deaktivieren

Sie können den Verbindungsschutz für den Administrationsserver nur in der Konsole des vertrauenswürdigen Servers, mit dem der Computer verbunden ist, per Fernzugriff deaktivieren. Sie können den Schutz auch lokal über die Befehlszeile deaktivieren.

So deaktivieren Sie den Schutz der Serververbindung über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.
3. Wählen Sie die Aufgabe **Schutz der Verbindung zum Administrationsserver** aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.
4. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
5. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Nicht schützen** auswählen.
6. Speichern Sie die vorgenommenen Änderungen.
7. Führen Sie die Aufgabe aus.

   Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen.

So deaktivieren Sie den Schutz der Serververbindung über Web Console oder Cloud Console

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Schutz der Verbindung zum Administrationsserver**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie unter **Schutz der Verbindung zum Administrationsserver** den Punkt **Nicht durch Kennwort schützen** auswählen.
5. Speichern Sie die vorgenommenen Änderungen.
6. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

7. Klicken Sie auf **Starten**.

   Sie können den Aufgabenstatus und die Anzahl der Geräte, auf denen die Aufgabe erfolgreich ausgeführt wurde oder fehlgeschlagen ist, einsehen.

So deaktivieren Sie den Schutz für die Serververbindung über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   wobei `<password>` das Kennwort des Benutzerkontos KLAdmin ist oder das Kennwort aus der Aufgabe *Schutz der Verbindung zum Administrationsserver*. Wenn der Parameter nicht angegeben ist, werden Sie von Kaspersky Endpoint Security aufgefordert, in der nächsten Zeile ein Kennwort einzugeben.

   > Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein.

Beispiel

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

Virtuelle Datentresore

Kaspersky Endpoint Security erlaubt die Verschlüsselung von Dateien und Ordnern, die auf lokalen Laufwerken und Wechseldatenträgern gespeichert sind, sowie die Verschlüsselung kompletter Wechseldatenträger und Festplatten. Die Datenverschlüsselung reduziert das Risiko eines Informationsdiebstahls, falls ein Laptop, ein Wechseldatenträger oder eine Festplatte gestohlen wird oder verloren geht, oder falls Dritte oder andere Programme auf Daten zugreifen. Kaspersky Endpoint Security verwendet den Verschlüsselungsalgorithmus Advanced Encryption Standard (AES).

Wenn die Lizenz abgelaufen ist, verschlüsselt das Programm neue Daten nicht mehr. Bereits verschlüsselte Daten bleiben verschlüsselt und es kann weiterhin damit gearbeitet werden. Um neue Daten zu verschlüsseln, muss das Programm mit einer neuen Lizenz aktiviert werden, welche die Verwendung der Verschlüsselung vorsieht.

Wenn Kaspersky Endpoint Security auf einem Arm-basierten Computer installiert ist, ist nur die BitLocker-Laufwerkverschlüsselung verfügbar. Das Programm unterstützt keine anderen Datenverschlüsselungskomponenten.

In den folgenden Fällen kann nicht garantiert werden, dass zuvor die verschlüsselten Dateien auch weiterhin verschlüsselt bleiben: Wenn die Lizenz abgelaufen ist, der Lizenzvertrag verletzt wurde, die Lizenz gelöscht wurde oder das Programm Kaspersky Endpoint Security oder die Verschlüsselungskomponenten vom Computer des Benutzers entfernt wurden. Dies liegt daran, dass einige Programme, wie z. B. Microsoft Office Word, während der Bearbeitung eine temporäre Kopie der Dateien erstellen. Wenn die Originaldatei gespeichert wird, ersetzt die temporäre Kopie die Originaldatei. Ist die Verschlüsselungsfunktionalität auf dem Computer nicht vorhanden oder nicht verfügbar, so bleibt die Datei unverschlüsselt.

Kaspersky Endpoint Security bietet folgende Datenschutzmaßnahmen:

- **Dateiverschlüsselung auf lokalen Festplatten des Computers**. Sie können folgende Listen anlegen: Listen mit Dateien nach Erweiterung oder Erweiterungsgruppen, und Listen mit Ordnern, die sich auf lokalen Laufwerken des Computers befinden. Außerdem können Sie Verschlüsselungsregeln für Dateien definieren, die von bestimmten Programmen erstellt werden. Nachdem die Richtlinie übernommen wurde, verschlüsselt und entschlüsselt Kaspersky Endpoint Security die folgenden Dateien:
  - Dateien, die einzeln zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
  - Dateien, die in Ordnern gespeichert sind, welche zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
  - Dateien, die von bestimmten Programmen erstellt werden
- **Wechseldatenträger verschlüsseln**. Sie können eine Standard-Verschlüsselungsregel festlegen, nach der das Programm für alle Wechseldatenträger die gleiche Aktion ausführt. Außerdem können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.

  Die Standard-Verschlüsselungsregel besitzt eine niedrigere Priorität als die Verschlüsselungsregeln, die für bestimmte Wechseldatenträger erstellt wurden. Verschlüsselungsregeln, die für bestimmte Wechseldatenträger unter Angabe eines Gerätemodells erstellt wurden, besitzen eine niedrigere Priorität als Verschlüsselungsregeln, die für Wechseldatenträger unter Angabe einer Geräte-ID erstellt wurden.

Um zu wählen, welche Regel für die Dateiverschlüsselung auf einem Wechseldatenträger gilt, überprüft Kaspersky Endpoint Security, ob Gerätemodell und Geräte-ID bekannt sind. Anschließend führt das Programm eine der folgenden Aktionen aus:

- Ist nur das Gerätemodell bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit diesem Gerätemodell erstellt wurde, falls eine solche Regel vorhanden ist.
- Ist nur die Geräte-ID bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit dieser Geräte-ID erstellt wurde, falls eine solche Regel vorhanden ist.
- Sind Gerätemodell und Geräte-ID bekannt, so wendet das Programm jene Verschlüsselungsregel an, die für Wechseldatenträger mit dieser Geräte-ID erstellt wurde, falls eine solche Regel vorhanden ist. Ist eine solche Regel nicht vorhanden, es gibt aber eine Verschlüsselungsregel, die für Wechseldatenträger mit diesem Gerätemodell erstellt wurde, so verwendet das Programm diese Regel. Wurde weder für diese Geräte-ID noch für dieses Gerätemodell eine Verschlüsselungsregel festgelegt, so verwendet das Programm die standardmäßige Verschlüsselungsregel.
- Wenn weder das Gerätemodell noch die Geräte-ID bekannt ist, wendet das Programm die Standard-Verschlüsselungsregel an.

Ein Wechseldatenträger kann vom Programm so vorbereitet werden, dass die darauf verschlüsselten Dateien im portablen Modus verwendet werden können. Ist der portable Modus aktiviert, so können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

- **Verwaltung von Regeln für den Zugriff von Programmen auf verschlüsselte Dateien**. Sie können für ein beliebiges Programm eine Regel für den Zugriff auf verschlüsselte Dateien erstellen. Diese Regel kann entweder den Zugriff auf verschlüsselte Dateien verbieten oder nur den Zugriff auf den verschlüsselten Text erlauben, also auf eine Zeichenfolge, die aus der Verschlüsselung hervorgeht.

- **Verschlüsselte Archive erstellen**. Sie können verschlüsselte Archive erstellen und den Zugriff darauf mit einem Kennwort schützen. Der Zugriff auf den Inhalt verschlüsselter Archive wird erst nach Eingabe der Kennwörter gewährt, mit denen Sie den Zugriff auf diese Archive geschützt haben. Solche Archive können gefahrlos über das Internet oder auf Wechseldatenträgern übertragen werden.

- **Vollständige Festplattenverschlüsselung**. Sie können ein Verschlüsselungsverfahren auswählen: Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung (im Folgenden auch „BitLocker“ genannt).

  Die Technologie *BitLocker* ist Bestandteil des Betriebssystems Windows. Wenn ein Computer über ein Trusted Platform Module (TPM) verfügt, verwendet BitLocker das TPM zur Speicherung von Wiederherstellungsschlüsseln, die für den Zugriff auf verschlüsselte Festplatten dienen. Beim Hochfahren des Computers fragt BitLocker bei Trusted Platform Module die Wiederherstellungsschlüssel für die Festplatte ab und entsperrt die Festplatte. Sie können die Verwendung eines Kennworts und/oder eines PIN-Codes für den Zugriff auf die Wiederherstellungsschlüssel festlegen.

  Sie können eine standardmäßige Regel für die vollständige Festplattenverschlüsselung festlegen und eine Liste mit Festplatten erstellen, die von der Verschlüsselung ausgeschlossen werden sollen. Nachdem die Richtlinie für Kaspersky Security Center übernommen wurde, führt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung sektorbasiert aus. Das Programm verschlüsselt alle logischen Partitionen der Festplatten auf einmal.

Nach der Verschlüsselung von Systemfestplatten und einem nachfolgenden Neustart des Computers, sind der Zugriff auf die Festplatten und das Laden des Betriebssystems erst möglich, nachdem der Benutzer sich mithilfe des Authentifizierungsagenten authentifiziert hat. Dazu ist entweder die Eingabe des Kennworts für den Token oder die Smartcard, die mit dem Computer verbunden sind, oder die Eingabe des Namens und Kennworts für das Authentifizierungsagenten-Benutzerkonto erforderlich, das vom Systemadministrator des lokalen Unternehmensnetzwerks mithilfe der Aufgabe *Authentifizierungsagenten-Konten verwalten* erstellt wurde. Diese Konten basieren auf den Benutzerkonten von Microsoft Windows, mit denen sich die Benutzer im Betriebssystem anmelden. Sie können auch die Technologie Single Sign-On (SSO) verwenden. Diese ermöglicht eine automatische Anmeldung im Betriebssystem mit dem Benutzernamen und dem Kennwort des Authentifizierungsagenten-Benutzerkontos.

Wenn für den Computer eine Backup-Kopie erstellt wurde, die Computerdaten dann verschlüsselt wurden, anschließend die Backup-Kopie des Computers wiederhergestellt wurde und die Computerdaten erneut verschlüsselt wurden, so erstellt Kaspersky Endpoint Security Duplikate der Benutzerkonten für den Authentifizierungsagenten. Um die Duplikate zu löschen, muss das Dienstprogramm klmover mit dem Parameter `dupfix` verwendet werden. Das Tool gehört zum Lieferumfang von Kaspersky Security Center. Weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Security Center.

Der Zugriff auf verschlüsselte Festplatten ist nur von jenen Computern aus möglich, auf denen das Programm Kaspersky Endpoint Security installiert ist und die vollständige Festplattenverschlüsselung verfügbar ist. Diese Bedingung gewährleistet ein minimales Risiko von Datendiebstahl von der verschlüsselten Festplatte, falls diese außerhalb des lokalen Unternehmensnetzwerks verwendet wird.

Um Festplatten und Wechseldatenträger zu verschlüsseln, können Sie die Funktion Nur belegten Speicherplatz verschlüsseln verwenden. Es wird empfohlen, diese Funktion nur für neue Geräte zu verwenden, die bisher noch nicht benutzt worden sind. Wenn Sie die Verschlüsselung auf einem Gerät verwenden möchten, das bereits benutzt wurde, so sollte das gesamte Gerät verschlüsselt werden. Dies garantiert den Schutz aller Daten, selbst gelöschter Daten, aus denen noch Informationen entnommen werden könnten.

Vor dem Beginn der Verschlüsselung erhält Kaspersky Endpoint Security eine Sektorenkarte des Dateisystems. Im ersten Datenstrom werden die Sektoren verschlüsselt, die beim Start der Verschlüsselung mit Dateien belegt sind. Im zweiten Datenstrom werden die Sektoren verschlüsselt, die nach dem Beginn der Verschlüsselung geschrieben wurden. Nach dem Abschluss der Verschlüsselung sind alle Sektoren verschlüsselt, die Daten enthalten.

Löscht der Benutzer nach dem Abschluss der Verschlüsselung eine Datei, so werden die Sektoren, in denen diese Datei gespeichert waren, frei und dort können auf Dateisystemebene Informationen geschrieben werden. Dabei bleiben die Sektoren weiterhin verschlüsselt. Wird die Verschlüsselung regelmäßig ausgeführt und die Funktion **Nur belegten Speicherplatz verschlüsseln** ist aktiviert, so werden durch die kontinuierliche Speicherung von Dateien nach und nach alle Sektoren auf dem neuen Gerät verschlüsselt.

Die Daten, die zur Entschlüsselung von Objekten erforderlich sind, werden vom Administrationsserver für Kaspersky Security Center zur Verfügung gestellt, der den Computer zum Zeitpunkt der Verschlüsselung verwaltet. Kommt ein Computer mit verschlüsselten Objekten unter die Kontrolle eines anderen Administrationsservers, so bestehen folgende Möglichkeiten, um Zugriff auf die verschlüsselten Daten zu erhalten:

- Administrationsserver in derselben Hierarchie:
  - Sie müssen keine zusätzlichen Aktionen ausführen. Der Benutzer kann weiterhin auf die verschlüsselten Objekte zugreifen. Die Chiffrierschlüssel gelten für alle Administrationsserver.

- Die Administrationsserver sind verstreut:
  - Administrator des lokalen Unternehmensnetzwerks um die Freigabe der verschlüsselten Objekte bitten.
  - Daten auf verschlüsselten Geräten mithilfe des Reparatur-Tools wiederherstellen.
  - Aus einer Backup-Kopie die Konfiguration des Administrationsservers für Kaspersky Security Center wiederherstellen, von welchem der Computer bei der Verschlüsselung verwaltet wurde, und diese Konfiguration auf dem Administrationsserver verwenden, welcher den Computer mit den verschlüsselten Objekten verwaltet.

Wenn der Zugriff auf verschlüsselte Daten nicht möglich ist, folgen Sie den entsprechenden Anleitungen für die Arbeit mit verschlüsselten Daten (Wiederherstellen des Zugriffs auf verschlüsselte Dateien, Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht).

Beschränkungen der Verschlüsselungsfunktionalität

Die Datenverschlüsselung besitzt die folgenden Beschränkungen:

- Im Verlauf der Verschlüsselung legt das Programm Verwaltungsdateien an. Für deren Speicherung sind etwa 0,5% unfragmentierter freier Speicherplatz auf der Festplatte des Computers erforderlich. Ist auf der Festplatte zu wenig unfragmentierter Speicherplatz verfügbar, so wird die Verschlüsselung erst gestartet, wenn entsprechende Bedingungen vorliegen.
- Alle Datenverschlüsselungskomponenten können in der Verwaltungskonsole für Kaspersky Security Center und in der „Kaspersky Security Center Web Console“ verwaltet werden. Über die Kaspersky Security Center Cloud Console können Sie nur Bitlocker verwalten.
- Die Datenverschlüsselung ist nur verfügbar, wenn Kaspersky Endpoint Security mit dem Administrationssystem Kaspersky Security Center oder Kaspersky Security Center Cloud Console (nur BitLocker) verwendet wird. Eine Datenverschlüsselung ist nicht möglich, wenn Kaspersky Endpoint Security im Offline-Modus verwendet wird, da Kaspersky Endpoint Security die Chiffrierschlüssel in Kaspersky Security Center speichert.
- Ist das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Microsoft Windows für Server installiert, so ist nur die vollständige Festplattenverschlüsselung mithilfe der Technologie BitLocker-Laufwerkverschlüsselung verfügbar. Ist das Programm Kaspersky Endpoint Security auf einem Computer mit Windows für Workstation installiert, so ist die Funktionalität zur Datenverschlüsselung in vollem Umfang verfügbar.
- Wenn Kaspersky Endpoint Security auf einem Arm-basierten Computer installiert ist, ist nur die vollständige Festplattenverschlüsselung mit der Technologie BitLocker-Laufwerkverschlüsselung verfügbar. Andere Verschlüsselungskomponenten werden nicht unterstützt.

Die Funktionalität zur vollständigen Festplattenverschlüsselung mit dem Verfahren Kaspersky-Festplattenverschlüsselung ist nicht verfügbar für Festplatten, welche die Hard- und Softwarevoraussetzungen nicht erfüllen.

Die Kompatibilität zwischen der Funktionalität für die vollständige Festplattenverschlüsselung von Kaspersky Endpoint Security und Kaspersky Anti-Virus für UEFI wird nicht unterstützt. Kaspersky Anti-Virus für UEFI wird vor dem Hochfahren des Betriebssystems gestartet. Bei der vollständigen Festplattenverschlüsselung erkennt das Programm, dass auf dem Computer kein Betriebssystem installiert ist. Als Folge wird Kaspersky Anti-Virus für UEFI mit einem Fehler beendet. Die Verschlüsselung von Dateien (FLE) beeinflusst die Funktion von Kaspersky Anti-Virus für UEFI nicht.

Kaspersky Endpoint Security unterstützt die folgenden Konfigurationen:

- HDD-, SSD- und USB-Laufwerke.

  Die Technologie von Kaspersky Disk Encryption (FDE) unterstützt die Arbeit mit SSD bei Aufrechterhaltung der Leistung und Lebensdauer von SSD-Laufwerken.

- Über den Bus angeschlossene Laufwerke: SCSI, ATA, IEEE1934, USB, RAID, SAS, SATA, NVME.
- Über SD- oder MMC-Bus angeschlossene nicht auswechselbare Laufwerke.
- Laufwerke mit 512-Byte-Sektoren.
- Laufwerke mit 4096-Byte-Sektoren, die 512 Byte emulieren.
- Laufwerke mit den folgenden Partitionstypen: GPT, MBR und VBR (Wechseldatenträger).
- Eingebettete Software des UEFI 64- und Legacy-BIOS-Standards.
- Eingebettete Software des UEFI-Standards mit Secure Boot-Unterstützung.

  Secure Boot ist eine Technologie zur Überprüfung digitaler Signaturen für UEFI-Lader-Programme und -Treiber. Secure Boot blockiert den Start von UEFI-Programmen und -Treibern, die unsigniert oder von unbekannten Herausgebern signiert sind. Kaspersky Disk Encryption (FDE) unterstützt Secure Boot vollständig. Der Authentifizierungsagent ist durch ein Microsoft Windows UEFI-Treiber-Publisher-Zertifikat signiert.

  Auf einigen Geräten (z. B. Microsoft Surface Pro und Microsoft Surface Pro 2) kann eine veraltete Liste von Zertifikaten zur Verifizierung digitaler Signaturen standardmäßig installiert sein. Bevor Sie das Laufwerk verschlüsseln können, müssen Sie die Liste der Zertifikate aktualisieren.

- Eingebettete Software des UEFI-Standards mit Fast Boot-Unterstützung.

  Fast Boot ist eine Technologie, die dem Computer hilft, schneller zu starten. Wenn die Fast Boot-Technologie aktiviert ist, lädt der Computer normalerweise nur den Mindestsatz an UEFI-Treibern, der zum Starten des Betriebssystems erforderlich ist. Wenn die Fast Boot-Technologie aktiviert ist, funktionieren USB-Tastaturen, Mäuse, USB-Token, Touchpads und Touchscreens möglicherweise nicht, während der Authentifizierungsagent ausgeführt wird.

  Um Kaspersky Disk Encryption (FDE) zu verwenden, wird empfohlen, die Fast Boot-Technologie zu deaktivieren. Sie können das FDE-Testprogramm verwenden, um die Funktion von Kaspersky Disk Encryption (FDE) zu testen.

Folgende Konfigurationen werden von Endpoint Security nicht unterstützt:

- Schema, bei dem sich Ladeprogramm und Betriebssystem auf unterschiedlichen Laufwerken befinden
- integrierte Software des Standards UEFI 32
- Das System verfügt über Intel® Rapid Start Technology und Laufwerke, die über eine Hibernation-Partition verfügen, selbst wenn Intel® Rapid Start Technology deaktiviert ist.
- Laufwerke im MBR-Format mit mehr als 10 erweiterten Partitionen.
- Das System verfügt über eine Auslagerungsdatei, die sich auf einem Nicht-Systemlaufwerk befindet.

- Multi-Boot-System mit mehreren gleichzeitig installierten Betriebssystemen.
- dynamische Partitionen (nur primäre Partitionen werden unterstützt)
- Laufwerke, auf denen weniger als 0,5% freier unfragmentierter Speicherplatz vorhanden ist
- Laufwerke mit einer anderen Sektorgröße als 512 Byte oder 4096 Byte mit 512-Byte-Emulation
- Hybridlaufwerke
- Das System verfügt über Fremdlader.
- Laufwerke mit komprimierten NTFS-Verzeichnissen.
- Die Kaspersky Disk Encryption-Technologie (FDE) ist nicht kompatibel mit anderen Festplattenverschlüsselungstechnologien (wie BitLocker, McAfee Drive Encryption und WinMagic SecureDoc).
- Die Technologie Kaspersky-Festplattenverschlüsselung (FDE) ist nicht kompatibel mit der ExpressCache-Technologie.
- Das Erstellen, Löschen und Ändern von Partitionen auf einem verschlüsselten Laufwerk wird nicht unterstützt. Sie könnten Daten verlieren.
- Dateisystemformatierung wird nicht unterstützt. Sie könnten Daten verlieren.

  Wenn Sie ein Laufwerk formatieren müssen, das mit der FDE-Technologie (Kaspersky Disk Encryption) verschlüsselt wurde, formatieren Sie das Laufwerk auf einem Computer, der nicht über Kaspersky Endpoint Security für Windows verfügt, und verwenden Sie nur die vollständige Festplattenverschlüsselung.

  Ein verschlüsseltes Laufwerk, das mit der Schnellformatierungsoption formatiert wurde, kann fälschlicherweise als verschlüsselt erkannt werden, wenn es das nächste Mal an einen Computer angeschlossen wird, auf dem Kaspersky Endpoint Security für Windows installiert ist. Benutzerdaten werden nicht verfügbar sein.
- Der Authentifizierungsagent unterstützt nicht mehr als 100 Konten.
- Die Single-Sign-On-Technologie ist mit anderen Technologien von anderen Entwicklern nicht kompatibel.
- Die Kaspersky Disk Encryption-Technologie (FDE) wird von den folgenden Gerätemodellen nicht unterstützt:
  - Dell Latitude E6410 (UEFI-Modus)
  - HP Compaq nc8430 (Legacy-BIOS-Modus)
  - Lenovo ThinkCentre 8811 (Legacy-BIOS-Modus)
- Der Authentifizierungsagent unterstützt nicht die Arbeit mit USB-Tokens, wenn die Legacy-USB-Unterstützung aktiviert ist. Auf dem Computer wird nur eine kennwortbasierte Authentifizierung möglich sein.
- Beim Verschlüsseln eines Laufwerks im Legacy-BIOS-Modus wird empfohlen, die Legacy-USB-Unterstützung bei den folgenden Gerätemodellen zu aktivieren:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T

- Dell Inspiron 1420
- Dell Inspiron 1545
- Dell Inspiron 1750
- Dell Inspiron N4110
- Dell Latitude E4300
- Dell Studio 1537
- Dell Studio 1569
- Dell Vostro 1310
- Dell Vostro 1320
- Dell Vostro 1510
- Dell Vostro 1720
- Dell Vostro V13
- Dell XPS L502x
- Fujitsu Celsius W370
- Fujitsu LifeBook A555
- HP Compaq dx2450 Microtower PC
- Lenovo G550
- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (Hauptplatine)

Änderung der Länge des Chiffrierschlüssels (AES56 / AES256)

Kaspersky Endpoint Security verwendet den Verschlüsselungsalgorithmus Advanced Encryption Standard (AES). Kaspersky Endpoint Security unterstützt den AES-Verschlüsselungsalgorithmus mit einer effektiven Schlüssellänge von 256 und 56 Bit. Der Algorithmus für die Datenverschlüsselung ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Strong encryption (AES256)* oder *Lite encryption (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.

Die Länge des Chiffrierschlüssels kann nur in Kaspersky Endpoint Security 11.2.0 und höher geändert werden.

Die Länge des Chiffrierschlüssels wird in zwei Schritten geändert:

1. Entschlüsseln Sie die Objekte, die mit dem Programm Kaspersky Endpoint Security verschlüsselt wurden, bevor die Länge des Chiffrierschlüssels geändert wird:

   a. Entschlüsseln Sie die Festplatten.

   b. Entschlüsseln Sie die Dateien auf lokalen Datenträgern.

   c. Entschlüsseln Sie die Wechseldatenträger.

   Nachdem die Länge des Chiffrierschlüssels geändert wurde, sind zuvor verschlüsselte Objekte nicht mehr verfügbar.

2. Entfernen Sie Kaspersky Endpoint Security.

3. Installieren Sie Kaspersky Endpoint Security aus dem Programmpaket für Kaspersky Endpoint Security mit der anderen Verschlüsselungsbibliothek.

Sie können die Länge des Chiffrierschlüssels auch durch ein Programm-Update ändern. Um die Länge des Chiffrierschlüssels durch ein Programm-Update zu ändern, müssen die folgenden Bedingungen erfüllt sein:

- Auf dem Computer ist das Programm Kaspersky Endpoint Security Version 10 Service Pack 2 oder höher installiert.
- Die folgenden Komponenten zur Datenverschlüsselung sind nicht auf dem Computer installiert: Dateiverschlüsselung, Vollständige Festplattenverschlüsselung.

  Komponenten zur Datenverschlüsselung gehören standardmäßig nicht zum Umfang von Kaspersky Endpoint Security. Die Komponente „Verwaltung von BitLocker“ hat keinen Einfluss auf eine Änderung der Länge des Chiffrierschlüssels.

Um die Länge des Chiffrierschlüssels zu ändern, starten Sie die Datei kes_win.msi oder setup_kes.exe aus dem Programmpaket mit der entsprechenden Verschlüsselungsbibliothek. Sie können das Programm auch ferngesteuert mithilfe eines Installationspakets aktualisieren.

Es ist nicht möglich, die Länge des Chiffrierschlüssels mithilfe des Programmpakets für die gleiche Programmversion zu ändern, die auf Ihrem Computer installiert ist, ohne das Programm vorher zu entfernen.

Kaspersky-Festplattenverschlüsselung

Die Kaspersky-Festplattenverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

Die Technologie „Kaspersky-Festplattenverschlüsselung“ ist nur für Computer verfügbar, die ein Windows-Betriebssystem für Workstations verwenden. Verwenden Sie für Computer mit einem Windows-Betriebssystem für Server die Technologie „BitLocker-Laufwerkverschlüsselung“.

Kaspersky Endpoint Security unterstützt die vollständige Festplattenverschlüsselung in den Dateisystemen FAT32, NTFS und exFat.

Bevor die vollständige Festplattenverschlüsselung gestartet wird, überprüft das Programm, ob die Verschlüsselung auf dem Gerät möglich ist. Dabei wird u. a. überprüft, ob die Systemfestplatte mit dem Authentifizierungsagenten oder mit der BitLocker-Verschlüsselungskomponente kompatibel ist. Für die Kompatibilitätsprüfung ist ein Neustart des Computers erforderlich. Nach dem Neustart des Computers nimmt das Programm automatisch alle notwendigen Prüfungen vor. Wenn die Kompatibilitätsprüfung erfolgreich verläuft, startet die vollständige Festplattenverschlüsselung, nachdem das System hochgefahren und das Programm gestartet wurde. Wenn die Überprüfung ergibt, dass die Systemfestplatte nicht mit dem Authentifizierungsagenten oder mit der BitLocker-Verschlüsselungskomponente kompatibel ist, muss der Computer mit dem Reset-Knopf am Computergehäuse neu gestartet werden. Kaspersky Endpoint Security protokolliert Informationen über die Inkompatibilität. Basierend auf diesen Informationen startet das Programm beim Start des Betriebssystems keine vollständige Festplattenverschlüsselung. Die Berichte von Kaspersky Security Center enthalten Informationen über dieses Ereignis.

Wenn die Hardware-Konfiguration des Computers verändert wurde und anschließend die Systemfestplatte auf Kompatibilität mit dem Authentifizierungsagenten und mit der BitLocker-Verschlüsselungskomponente überprüft werden soll, müssen zuerst die Inkompatibilitätsinformationen gelöscht werden, die das Programm bei der vorherigen Überprüfung ermittelt hat. Geben Sie dazu vor der vollständigen Festplattenverschlüsselung in der Befehlszeile folgenden Befehl ein: `avp pbatestreset`. Wenn sich das Betriebssystem nicht mehr hochfahren lässt, nachdem die Kompatibilität der Systemfestplatte mit dem Authentifizierungsagenten überprüft wurde, müssen mithilfe des Reparatur-Tools die Objekte und Daten gelöscht werden, die nach dem Testlauf des Authentifizierungsagenten verblieben sind. Starten Sie danach Kaspersky Endpoint Security und führen Sie erneut den Befehl `avp pbatestreset` aus.

Nach dem Start der vollständigen Festplattenverschlüsselung verschlüsselt Kaspersky Endpoint Security alle Daten, die auf Festplatten geschrieben werden.

Wenn der Benutzer den Computer während der vollständigen Festplattenverschlüsselung ausschaltet oder neu startet, wird der Authentifizierungsagent vor dem nächsten Start des Betriebssystems geladen. Nach der Anmeldung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung fort.

Wechselt das Betriebssystem während der vollständigen Festplattenverschlüsselung in den Ruhezustand (hibernation mode), so wird der Authentifizierungsagent beim Beenden des Ruhezustandes geladen. Nach der Anmeldung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung fort.

Wechselt das Betriebssystem während der vollständigen Festplattenverschlüsselung in den Energiesparmodus (sleep mode), so setzt Kaspersky Endpoint Security die vollständige Festplattenverschlüsselung nach dem Beenden des Energiesparmodus fort, ohne den Authentifizierungsagenten zu laden.

Es gibt zwei Methoden, mit denen sich der Benutzer im Authentifizierungsagenten authentifizieren kann:

- Durch Eingabe von Name und Kennwort eines Benutzerkontos für den Authentifizierungsagenten, wenn das Benutzerkonto vom Administrator des lokalen Unternehmensnetzwerks mit Mitteln von Kaspersky Security Center erstellt wurde.
- Durch Eingabe des Kennworts für einen Token oder eine Smartcard, die mit dem Computer verbunden sind.

  Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

Der Authentifizierungsagent unterstützt Tastaturlayouts für die folgenden Sprachen:

- Englisch (Großbritannien)
- Englisch (USA)
- Arabisch (Algerien, Marokko, Tunesien, AZERTY-Layout)
- Spanisch (Lateinamerika)
- Italienisch
- Deutsch (Deutschland und Österreich)
- Deutsch (Schweiz)
- Portugiesisch (Brasilien, ABNT2-Layout)
- Russisch (für IBM-/Windows-Tastatur mit 105 Tasten und JCUKEN-Tastaturlayout)
- Türkisch (QWERTY-Layout)
- Französisch (Frankreich)
- Französisch (Schweiz)

- Französisch (Belgien, AZERTY-Tastaturlayout)
- Japanisch (für Tastatur mit 106 Tasten und QWERTY-Tastaturlayout)

Ein Tastaturlayout steht im Authentifizierungsagenten zur Verfügung, wenn es in den Einstellungen des Betriebssystems unter Region und Sprache hinzugefügt wurde und auf dem Windows-Begrüßungsbildschirm verfügbar ist.

Wenn der Name des Authentifizierungsagenten-Benutzerkontos Zeichen enthält, die nicht mithilfe der im Authentifizierungsagenten verfügbaren Tastaturlayouts eingegeben werden können, so ist der Zugriff auf verschlüsselte Festplatten erst möglich, nachdem die Festplatten mithilfe des Reparatur-Tools wiederhergestellt wurden oder nachdem der Name und das Kennwort des Authentifizierungsagenten-Benutzerkontos wiederhergestellt wurden.

Besondere Merkmale der SSD-Laufwerksverschlüsselung

Das Programm unterstützt die Verschlüsselung von SSD-Laufwerken, hybriden SSHD-Laufwerken und Laufwerken mit der Intel Smart Response-Funktion. Das Programm unterstützt nicht die Verschlüsselung von Laufwerken mit der Intel Rapid Start Funktion. Deaktivieren Sie die Intel Rapid Start-Funktion vor der Verschlüsselung eines solchen Laufwerks.

Für die Verschlüsselung von SSD-Laufwerken gelten die folgenden Besonderheiten:

- Wenn ein SSD-Laufwerk neu ist und keine vertraulichen Daten enthält, aktivieren Sie die Verschlüsselung nur des belegten Speicherplatzes. Damit können Sie die entsprechenden Laufwerksektoren überschreiben.
- Wenn ein SSD-Laufwerk verwendet wird und vertrauliche Daten enthält, wählen Sie eine der folgenden Optionen:
  - Löschen Sie das SSD-Laufwerk vollständig (Secure Erase), installieren Sie das Betriebssystem und führen Sie die Verschlüsselung des SSD-Laufwerks mit aktivierter Option zur Verschlüsselung nur des belegten Speicherplatzes aus.
  - Führen Sie die Verschlüsselung des SSD-Laufwerks aus, wobei die Option zur Verschlüsselung nur des belegten Speicherplatzes deaktiviert ist.

Die Verschlüsselung eines SSD-Laufwerks erfordert 5-10 GB freien Speicherplatz. Die Anforderungen an den freien Speicherplatz für die Speicherung von Verschlüsselungsverwaltungsdaten sind in der folgenden Tabelle aufgeführt.

Freier Speicherplatzbedarf für die Speicherung von Verschlüsselungsverwaltungsdaten

Größe des SSD-Laufwerks (GB)	Freier Speicherplatz auf der primären Partition des SSD-Laufwerks (MB)	Freier Speicherplatz auf der sekundären Partition des SSD-Laufwerks (MB)
128	250	64
256	250	640
512	300	128

Kaspersky-Festplattenverschlüsselung starten

Es wird empfohlen, vor dem Start der vollständigen Festplattenverschlüsselung sicherzustellen, dass der Computer nicht infiziert ist. Starten Sie dazu eine vollständige Untersuchung oder eine Untersuchung der wichtigen Computerbereiche. Die vollständige Festplattenverschlüsselung auf einem Computer, der von einem Rootkit infiziert ist, kann zur Funktionsuntüchtigkeit des Computers führen.

Bevor Sie die Festplattenverschlüsselung starten, müssen Sie die Einstellungen der Authentifizierungsagenten-Konten überprüfen. Der Authentifizierungsagent wird benötigt, um mit Datenträgern zu arbeiten, die mithilfe der Technologie Kaspersky-Festplattenverschlüsselung (FDE) verschlüsselt sind. Der Benutzer muss vor dem Start des Betriebssystems die Authentifizierung mithilfe des Agenten durchlaufen. In Kaspersky Endpoint Security können vor der Datenträgerverschlüsselung automatisch Authentifizierungsagenten-Benutzerkonten erstellt werden. Das automatische Erstellen von Authentifizierungsagenten-Konten können Sie in den Einstellungen der Richtlinie für die vollständige Festplattenverschlüsselung aktivieren (siehe folgende Anleitung). Sie können auch das Verfahren zur Einmalanmeldung (SSO) verwenden.

Mit Kaspersky Endpoint Security können Sie automatisch einen Authentifizierungsagenten für die folgenden Benutzergruppen erstellen:

- **Alle Benutzerkonten des Computers**. Alle Benutzerkonten auf dem Computer, die zu irgendeinem Zeitpunkt aktiv waren.
- **Alle Domänenkonten des Computers**. Alle Benutzerkonten auf dem Computer, die zu einer Domäne gehören und die zu irgendeinem Zeitpunkt aktiv waren.
- **Alle lokalen Benutzerkonten des Computers**. Alle lokalen Benutzerkonten auf dem Computer, die zu irgendeinem Zeitpunkt aktiv waren.
- **Dienstkonto mit Einmalkennwort**. Das Dienstkonto wird beispielsweise benötigt, um Zugriff auf den Computer zu erhalten, wenn der Benutzer das Kennwort vergisst. Sie können das Dienstkonto auch als Reservekonto verwenden. Sie müssen den Namen des Benutzerkontos eingeben (Standardwert `ServiceAccount`). Kaspersky Endpoint Security erstellt automatisch ein Kennwort. Das Kennwort finden Sie in der Kaspersky Security Center-Konsole.
- **Lokaler Administrator**. Kaspersky Endpoint Security erstellt ein Authentifizierungsagenten-Konto für den lokalen Administrator des Computers.
- **Manager des Computers**. Kaspersky Endpoint Security erstellt ein Authentifizierungsagenten-Konto für das Benutzerkonto des Computermanagers. Welches Benutzerkonto die Rolle „Computermanager“ hat, können Sie in den Active Directory-Computereigenschaften nachsehen. Standardmäßig ist die Rolle „Computermanager“ nicht definiert, d. h. diese Rolle entspricht keinem Benutzerkonto.
- **Aktives Benutzerkonto**. Kaspersky Endpoint Security erstellt automatisch ein Authentifizierungsagenten-Konto für das Benutzerkonto, das zum Zeitpunkt der Festplattenverschlüsselung aktiv ist.

Die Einstellungen für die Authentifizierung von Benutzern können mit der Aufgabe *Authentifizierungsagenten-Konten verwalten* angepasst werden. Sie können diese Aufgabe verwenden, um neue Benutzerkonten hinzuzufügen, die Einstellungen bestehender Benutzerkonten zu ändern oder Benutzerkonten zu entfernen. Sie können sowohl lokale Aufgaben für einzelne Computer als auch Gruppenaufgaben für Computer aus bestimmten Administrationsgruppen oder für bestimmte Computer verwenden.

So führen Sie die Kaspersky-Festplattenverschlüsselung über die Verwaltungskonsole (MMC) aus

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Option **Kaspersky-Festplattenverschlüsselung**.

   Das Verfahren „Kaspersky-Festplattenverschlüsselung“ kann nicht verwendet werden, wenn auf dem Computer Festplatten vorhanden sind, die mithilfe von BitLocker verschlüsselt sind.

5. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Alle Festplatten verschlüsseln**.

   Wenn auf einem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung aller Festplatten nur noch jenes Betriebssystem ausführen, in dem das Programm installiert ist.

   Wenn bestimmte Festplatten von der Verschlüsselung ausgenommen werden sollen, müssen Sie diese in einer Liste angeben.

6. Passen Sie die erweiterten Einstellungen der Kaspersky-Festplattenverschlüsselung an (siehe folgende Tabelle).
7. Speichern Sie die vorgenommenen Änderungen.

So führen Sie die Kaspersky-Festplattenverschlüsselung über die „Web Console“ und „Cloud Console“ aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Datenverschlüsselung → Vollständige Festplattenverschlüsselung**.
5. Wählen Sie die Technologie **Kaspersky-Festplattenverschlüsselung** aus.

   Das Verfahren „Kaspersky-Festplattenverschlüsselung“ kann nicht verwendet werden, wenn auf dem Computer Festplatten vorhanden sind, die mithilfe von BitLocker verschlüsselt sind.

6. Wählen Sie im Block **Aktion mit Geräten** die Variante **Alle Festplatten verschlüsseln** aus.

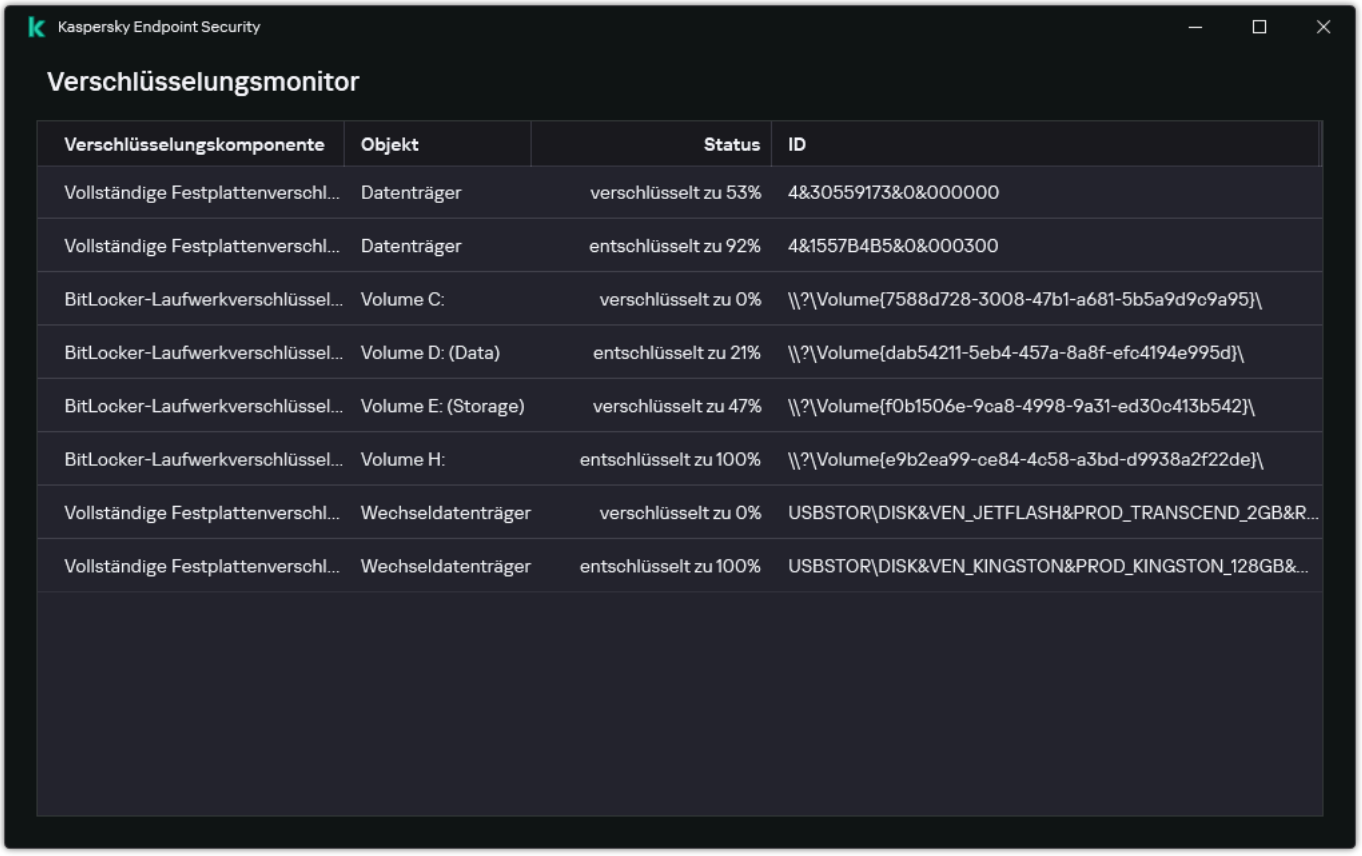
   Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem die Verschlüsselung ausgeführt wurde.

Wenn bestimmte Festplatten von der Verschlüsselung ausgenommen werden sollen, müssen Sie diese in einer Liste angeben.

7. Passen Sie die erweiterten Einstellungen der Kaspersky-Festplattenverschlüsselung an (siehe folgende Tabelle).

8. Speichern Sie die vorgenommenen Änderungen.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool „Encryption Monitor“ kann über das Programmhauptfenster ausgeführt werden.



Verschlüsselungsmonitor

Sind die Systemfestplatten verschlüsselt, so wird vor dem Laden des Betriebssystems der Authentifizierungsagent geladen. Authentifizieren Sie sich mithilfe des Authentifizierungsagenten, damit die verschlüsselten Systemfestplatten freigegeben werden und das Betriebssystem hochgefahren wird. Nach erfolgreicher Authentifizierung wird das Betriebssystem hochgefahren. Bei jedem nachfolgenden Neustart des Betriebssystems ist eine erneute Authentifizierung erforderlich.

Einstellungen der Komponente „Kaspersky-Festplattenverschlüsselung"

Einstellung	Beschreibung
Während der Verschlüsselung automatisch Authentifizierungsagenten-Konten für Benutzer auf diesem Computer erstellen	Wenn dieses Kontrollkästchen aktiviert ist, erstellt das Programm Benutzerkonten des Authentifizierungsagenten basierend auf der Liste der Windows-Benutzerkonten auf dem Computer. Kaspersky Endpoint Security verwendet standardmäßig alle lokalen und Domänen-Benutzerkonten, mit denen sich der Benutzer in den letzten 30 Tagen am Betriebssystem angemeldet hat.
Bei der Anmeldung die Authentifizierungsagenten-Konten für alle Benutzer dieses Computers automatisch erstellen	Wenn dieses Kontrollkästchen aktiviert ist, überprüft das Programm Informationen zu Windows-Benutzerkonten auf dem Computer, bevor der Authentifizierungsagent gestartet wird. Wenn Kaspersky Endpoint Security ein Windows-Benutzerkonto erkennt, das kein Benutzerkonto des Authentifizierungsagenten besitzt, erstellt das Programm ein neues Konto für den Zugriff auf verschlüsselte Laufwerke. Das neue Benutzerkonto des Authentifizierungsagenten verfügt über die folgenden Standardeinstellungen: nur kennwortgeschützte Anmeldung, Kennwortänderung bei der ersten Authentifizierung. Es ist also nicht nötig, für Computer mit bereits verschlüsselten Laufwerken mithilfe der Aufgabe *Authentifizierungsagenten-Konten verwalten* manuell Authentifizierungsagenten-Benutzerkonten hinzuzufügen.
Benutzername speichern, der im Authentifizierungsagenten eingegeben wurde	Wenn das Kontrollkästchen aktiviert ist, speichert das Programm den Namen des Authentifizierungsagenten-Kontos. Wenn im Authentifizierungsagenten das nächste Mal eine Authentifizierung mit demselben Benutzerkonto erfolgt, muss der Benutzername nicht eingegeben werden.
Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt. Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Das Kontrollkästchen ist standardmäßig deaktiviert.
Legacy USB Support verwenden (nicht empfohlen)	Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktionalität Legacy USB Support. *Legacy USB Support* **ist eine** BIOS-/UEFI-Funktion, die es ermöglicht, USB-Geräte (z. B. ein Token) zu verwenden, wenn der Computer gestartet wird und das Betriebssystem noch nicht gestartet wurde (BIOS-Modus). Nach dem Start des Betriebssystems beeinflusst die Funktion „Legacy USB Support" die Unterstützung von USB-Geräten nicht mehr. Ist das Kontrollkästchen aktiviert, so wird die Unterstützung von USB-Geräten zu Beginn des Startvorgangs des Computers aktiviert. Wenn die Funktion Legacy USB Support aktiviert ist, unterstützt der Authentifizierungsagent im BIOS-Modus die Verwendung von USB-Tokens nicht. Die Funktion sollte nur beim Auftreten von Hardware-Kompatibilitätsproblemen verwendet werden und ausschließlich für jene Computer aktiviert werden, auf welchen das Problem aufgetreten ist.

Liste mit Festplatten erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen

Eine Ausnahmeliste für die Verschlüsselung kann nur für das Verfahren „Kaspersky-Festplattenverschlüsselung“ erstellt werden.

Gehen Sie wie folgt vor, um eine Liste mit Festplatten zu erstellen, die aus der Verschlüsselung ausgeschlossen werden sollen:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Option **Kaspersky-Festplattenverschlüsselung**.

   In der Tabelle **Folgende Festplatten nicht verschlüsseln** werden Einträge mit Festplatten angezeigt, die nicht vom Programm verschlüsselt werden. Wenn Sie noch keine Liste mit Festplatten für die Ausnahme aus der Verschlüsselung erstellt haben, ist diese Tabelle leer.
5. Gehen Sie wie folgt vor, um der Liste mit Festplatten neue Festplatten hinzuzufügen, die nicht vom Programm verschlüsselt werden sollen:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie im sich öffnenden Fenster die Werte an für **Gerätename**, **Computer**, **Datenträgertyp**, **Kaspersky-Festplattenverschlüsselung**.

   c. Klicken Sie auf **Aktualisieren**.

   d. Aktivieren Sie in der Spalte **Name** die Kontrollkästchen in den Tabellenzeilen für jene Festplatten, die zur Liste der nicht zu verschlüsselnden Festplatten hinzugefügt werden sollen.

   e. Klicken Sie auf **OK**.

   Die ausgewählten Festplatten werden in der Tabelle **Folgende Festplatten nicht verschlüsseln** angezeigt.
6. Speichern Sie die vorgenommenen Änderungen.

Exportieren und Importieren einer Liste von Festplatten, die von der Verschlüsselung ausgenommen wurden

Sie können die Liste der Ausnahmen der Festplattenverschlüsselung in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Webadressen desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup für die Listen der überwachten Ports anzulegen oder die Listen auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Ausnahmen der Festplattenverschlüsselung in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Option **Kaspersky-Festplattenverschlüsselung**.

   In der Tabelle **Folgende Festplatten nicht verschlüsseln** werden Einträge mit Festplatten angezeigt, die nicht vom Programm verschlüsselt werden.
5. So exportieren Sie die Liste der Ausnahmen:

   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

   Wenn Sie keine Ausnahme ausgewählt haben, exportiert Kaspersky Endpoint Security alle Ausnahmen.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie die Liste der Ausnahmen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die gesamte Liste der Ausnahmen in die XML-Datei.
6. So importieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Klicken Sie auf die Schaltfläche → **Importieren**.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   c. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.
7. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste von Ausnahmen der Festplattenverschlüsselung in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Datenverschlüsselung → Vollständige Festplattenverschlüsselung**.

   Wählen Sie die Technologie **Kaspersky-Festplattenverschlüsselung** aus.

5. Klicken Sie auf den Link **Ausnahmen**.

   Die Liste der Ausnahmen öffnet sich.

6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

      Kaspersky Endpoint Security exportiert die Liste der Ausnahmen in eine json-Datei im standardmäßigen Download-Ordner.

7. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie im folgenden Fenster die JSON-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der JSON-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

Verwendung der Technologie zur Einmalanmeldung (SSO) aktivieren

Die Technologie Single Sign-On (SSO) ermöglicht eine automatische Anmeldung am Betriebssystem mithilfe der Anmeldedaten des Authentifizierungsagenten. Der Benutzer muss sein Kennwort also nur ein einziges Mal eingeben, und zwar bei der Windows-Anmeldung (Kennwort für das Authentifizierungsagenten-Konto). Die Technologie zur Einmalanmeldung bietet eine weitere Möglichkeit: Das Kennwort für das Authentifizierungsagenten-Konto kann automatisch aktualisiert werden, wenn das Kennwort für das Windows-Konto geändert wird.

Wenn das Verfahren zur Einmalanmeldung verwendet wird, ignoriert der Authentifizierungsagent die Anforderungen an die Kennwortkomplexität, die in Kaspersky Security Center festgelegt sind. Die Anforderungen an die Kennwortkomplexität können Sie in den Betriebssystemeinstellungen festlegen.

Verwendung der Technologie zur Einmalanmeldung aktivieren

Verwendung des Verfahrens zur Einmalanmeldung in der Verwaltungskonsole (MMC) aktivieren

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Allgemeine Verschlüsselungseinstellungen** aus.

4. Klicken Sie im Block **Einstellungen für Kennwörter** auf **Einstellungen**.

5. Aktivieren Sie im angezeigten Fenster auf der Registerkarte **Authentifizierungsagent** das Kontrollkästchen **Technologie zur Einmalanmeldung (SSO) verwenden**.

6. Wenn Sie einen Drittanbieter für Anmeldeinformationen verwenden, aktivieren Sie das Kontrollkästchen **Anmeldedaten von Drittanbietern verpacken**.

7. Speichern Sie die vorgenommenen Änderungen.

Dadurch muss der Benutzer die Authentifizierung mithilfe des Agenten nur ein Mal durchlaufen. Für den Start des Betriebssystems ist kein Authentifizierungsvorgang erforderlich. Das Betriebssystem wird automatisch gestartet.

In der „Web Console“ die Verwendung des Verfahrens zur Einmalanmeldung aktivieren

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Datenverschlüsselung → Vollständige Festplattenverschlüsselung**.

5. Wählen Sie die Technologie **Kaspersky-Festplattenverschlüsselung** aus.

6. Aktivieren Sie im Block **Einstellungen für Kennwörter** das Kontrollkästchen **Technologie zur Einmalanmeldung (SSO) verwenden**.

7. Wenn Sie einen Drittanbieter für Anmeldeinformationen verwenden, aktivieren Sie das Kontrollkästchen **Anmeldedaten von Drittanbietern verpacken**.

8. Speichern Sie die vorgenommenen Änderungen.

Dadurch muss der Benutzer die Authentifizierung mithilfe des Agenten nur ein Mal durchlaufen. Für den Start des Betriebssystems ist kein Authentifizierungsvorgang erforderlich. Das Betriebssystem wird automatisch gestartet.

Damit das Verfahren zur Einmalanmeldung funktioniert, müssen das Kennwort des Windows-Kontos und das Kennwort des Authentifizierungsagenten-Benutzerkontos identisch sein. Wenn die Kennwörter unterschiedlich sind, muss der Benutzer die Authentifizierung zwei Mal ausführen: auf der Benutzeroberfläche des Authentifizierungsagenten und vor dem Start des Betriebssystems. Diese Aktionen müssen nur einmal durchgeführt werden, um die Kennwörter zu synchronisieren. Anschließend ersetzt Kaspersky Endpoint Security das Kennwort des Authentifizierungsagenten-Benutzerkontos mit dem Kennwort des Windows-Kontos. Wenn das Kennwort des Windows-Kontos geändert wird, aktualisiert das Programm automatisch das Kennwort für das Authentifizierungsagenten-Konto.

Drittanbieter für Anmeldeinformationen

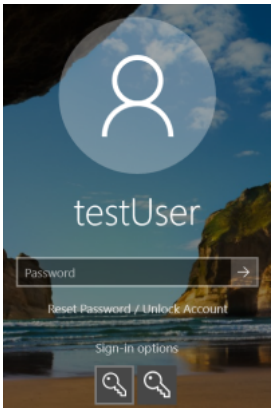
Kaspersky Endpoint Security unterstützt den Drittanbieter für Anmeldeinformationen ADSelfService Plus.

Bei der Verwendung von Drittanbietern für Anmeldeinformationen fängt der Authentifizierungsagent das Kennwort ab, bevor das Betriebssystem geladen wird: Der Benutzer muss sein Kennwort also nur ein einziges Mal eingeben, und zwar bei der Windows-Anmeldung. Nach der Anmeldung bei Windows kann der Benutzer die Optionen des Drittanbieters für Anmeldeinformationen nutzen, z. B. für die Anmeldung bei Unternehmensdiensten. Drittanbieter für Anmeldeinformationen bieten Benutzern auch die Möglichkeit, ihre Kennwörter unabhängig zurückzusetzen. In diesem Fall aktualisiert Kaspersky Endpoint Security automatisch das Kennwort für den Authentifizierungsagenten.

Wenn Sie einen Drittanbieter für Anmeldeinformationen verwenden, der vom Programm nicht unterstützt wird, sind die Funktionen der Einmalanmeldung möglicherweise eingeschränkt. Bei der Windows-Anmeldung kann der Benutzer zwischen zwei Profilen wählen: Systemanmeldeinformationsanbieter und Drittanbieter für Anmeldeinformationen. Die Symbole dieser Profile sind identisch (siehe Bild unten). Der Benutzer hat die folgenden Möglichkeiten:

- Wenn der Benutzer den *Drittanbieter für Anmeldeinformationen* auswählt, kann der Authentifizierungsagent das Kennwort nicht mit dem Windows-Konto synchronisieren. Wenn der Benutzer das Kennwort des Windows-Kontos geändert hat, kann Kaspersky Endpoint Security deshalb das Kennwort für das Authentifizierungsagenten-Konto nicht aktualisieren. Darum muss sich der Benutzer zwei Mal authentifizieren: auf der Benutzeroberfläche des Authentifizierungsagenten und vor dem Start des Betriebssystems. In diesem Fall kann der Benutzer die Optionen des Drittanbieters für Anmeldeinformationen nutzen, z. B. für die Anmeldung bei Unternehmensdiensten.

- Wenn der Benutzer den *Systemanmeldeinformationsanbieter* auswählt, synchronisiert der Authentifizierungsagent die Kennwörter mit dem Windows-Konto. In diesem Fall kann der Benutzer die Optionen des Drittanbieters für Anmeldeinformationen beispielsweise nicht zur Anmeldung bei Unternehmensdiensten nutzen.



System-Authentifizierungsprofil und Drittanbieter-Authentifizierungsprofil für die Windows-Anmeldung

Authentifizierungsagenten-Konten verwalten

Der Authentifizierungsagent wird benötigt, um mit Datenträgern zu arbeiten, die mithilfe der Technologie Kaspersky-Festplattenverschlüsselung (FDE) verschlüsselt sind. Der Benutzer muss vor dem Start des Betriebssystems die Authentifizierung mithilfe des Agenten durchlaufen. Die Einstellungen für die Authentifizierung von Benutzern können mit der Aufgabe *Authentifizierungsagenten-Konten verwalten* angepasst werden. Sie können sowohl lokale Aufgaben für einzelne Computer als auch Gruppenaufgaben für Computer aus bestimmten Administrationsgruppen oder für bestimmte Computer verwenden.

Für die Aufgabe *Authentifizierungsagenten-Konten verwalten* kann kein Startzeitplan eingerichtet werden. Außerdem kann die Ausführung dieser Aufgabe nicht zwangsweise abgebrochen werden.

Erstellen der Aufgabe „Benutzerkonten des Authentifizierungsagenten verwalten“ in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2) → Authentifizierungsagenten-Konten verwalten** aus.

Schritt 2. Befehl für die Verwaltung der Authentifizierungsagenten-Benutzerkonten auswählen

Erstellen Sie eine Liste mit den Befehlen für die Verwaltung der Authentifizierungsagenten-Benutzerkonten. Mit Verwaltungsbefehlen kann ein Authentifizierungsagenten-Benutzerkonto hinzugefügt, geändert oder gelöscht werden (s. Anleitung unten). Nur jene Benutzer, die ein Authentifizierungsagenten-Benutzerkonto haben, können den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgabe ein, z. B. *Benutzerkonten für Administratoren*.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Nachdem die Aufgabe ausgeführt wurde, kann der neue Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Erstellen der Aufgabe „Benutzerkonten des Authentifizierungsagenten verwalten“ in der „Web Console”

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Authentifizierungsagenten-Konten verwalten**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Administrator-Benutzerkonten*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

Schritt 2. Benutzerkonten des Authentifizierungsagenten verwalten

Erstellen Sie eine Liste mit den Befehlen für die Verwaltung der Authentifizierungsagenten-Benutzerkonten. Mit Verwaltungsbefehlen kann ein Authentifizierungsagenten-Benutzerkonto hinzugefügt, geändert oder gelöscht werden (s. Anleitung unten). Nur jene Benutzer, die ein Authentifizierungsagenten-Benutzerkonto haben, können den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Schritt 3. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Die neue Aufgabe wird in der Aufgabenliste angezeigt.

Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**, um die Aufgabe auszuführen.

Nachdem die Aufgabe ausgeführt wurde, kann der neue Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Um ein Authentifizierungsagenten-Benutzerkonto hinzuzufügen, muss ein spezieller Befehl zur Aufgabe *Authentifizierungsagenten-Konten verwalten* hinzugefügt werden. Eine Gruppenaufgabe ist beispielsweise geeignet, um auf allen Computern ein Administratorkonto hinzuzufügen.

In Kaspersky Endpoint Security können vor der Datenträgerverschlüsselung automatisch Authentifizierungsagenten-Benutzerkonten erstellt werden. Sie können das automatische Erstellen von Authentifizierungsagenten-Benutzerkonten in den Einstellungen der Richtlinie für die vollständige Festplattenverschlüsselung aktivieren. Sie können auch das Verfahren zur Einmalanmeldung (SSO) verwenden.

Hinzufügen eines Authentifizierungsagenten-Benutzerkontos über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Eigenschaften der Aufgabe *Authentifizierungsagenten-Konten verwalten*.
2. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen**.
3. Klicken Sie auf **Hinzufügen → Befehl zum Hinzufügen eines Benutzerkontos**.
4. Geben Sie im folgenden Fenster im Feld **Windows-Benutzerkonto** den Namen des Microsoft Windows-Kontos an, auf dessen Basis das Authentifizierungsagenten-Benutzerkonto erstellt werden soll.
5. Wenn Sie den Namen des Windows-Kontos eingetippt haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Mithilfe der Sicherheits-ID des Windows-Kontos wird überprüft, ob der Name des Windows-Kontos richtig eingegeben wurde. Wenn das Windows-Konto nicht auf dem Computer oder in der vertrauenswürdigen Domäne vorhanden ist, wird die Aufgabe *Authentifizierungsagenten-Konten verwalten* mit einem Fehler abgeschlossen.

6. Aktivieren Sie das Kontrollkästchen **Vorhandenes Benutzerkonto ersetzen**, wenn Sie möchten, dass ein bereits für den Authentifizierungsagenten erstelltes Benutzerkonto mit demselben Namen durch das neu hinzugefügte Benutzerkonto ersetzt wird.

   > Dieser Schritt ist verfügbar, wenn Sie den Befehl zum Erstellen eines Benutzerkontos für den Authentifizierungsagenten in den Eigenschaften einer Gruppenaufgabe zur Verwaltung von Benutzerkonten für den Authentifizierungsagenten hinzufügen. Dieser Schritt ist nicht verfügbar, wenn Sie den Befehl zum Erstellen eines Benutzerkontos für den Authentifizierungsagenten der lokalen Aufgabe *Authentifizierungsagenten-Konten verwalten* hinzufügen.

7. Geben Sie im Feld **Benutzername** den Namen des Benutzerkontos für den Authentifizierungsagenten ein, der zur Authentifizierung für den Zugriff auf verschlüsselte Festplatten dient.
8. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Kennwort erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort des Benutzerkontos für den Authentifizierungsagenten abfragt. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest. Bei Bedarf können Sie den Benutzer nach der ersten Authentifizierung nach dem neuen Kennwort fragen.

9. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Zertifikat erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten dazu auffordert, einen Token oder eine Smartcard mit dem Computer zu verbinden. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus.

10. Geben Sie erforderlichenfalls im Feld **Beschreibung des Befehls** die Informationen des Benutzerkontos für den Authentifizierungsagenten ein, welche Sie für die Verwendung des Befehls benötigen.

11. Konfigurieren Sie im Block **Zugriff auf die Anmeldung im Authentifizierungsagenten** den Zugriff auf die Anmeldung im Authentifizierungsagenten für den Benutzer, der das im Befehl angegebene Benutzerkonto verwendet.

12. Speichern Sie die vorgenommenen Änderungen.

Hinzufügen eines Authentifizierungsagenten-Benutzerkontos über „Web Console"

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Authentifizierungsagenten-Konten verwalten**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Klicken Sie in der Liste der Benutzerkonten des Authentifizierungsagenten auf die Schaltfläche **Hinzufügen** und wählen Sie den Befehlstyp **Benutzerkonto hinzufügen** aus.

5. Wählen Sie ein Benutzerkonto aus. Sie können das Benutzerkonto aus der Liste der Domänen-Benutzerkonten auswählen oder den Benutzerkonto-Namen eintippen. Weiter zum nächsten Schritt

   Kaspersky Endpoint Security ermittelt die Sicherheits-ID des Benutzerkontos (Security Identifier, SID). Dies ist für die Überprüfung des Benutzerkontos erforderlich. Wenn Sie den Benutzernamen falsch eingegeben haben, schließt Kaspersky Endpoint Security die Aufgabe mit einem Fehler ab.

6. Passen Sie die Einstellungen des Authentifizierungsagenten-Benutzerkontos an.

   - **Neues Authentifizierungsagenten-Benutzerkonto erstellen anstelle des vorhandenen Kontos**. Kaspersky Endpoint Security überprüft die vorhandenen Authentifizierungsagent-Benutzerkonten auf dem Computer. Wenn die Sicherheits-ID des Benutzers auf dem Computer und in der Aufgabe übereinstimmen, ändert Kaspersky Endpoint Security die Benutzerkonto-Einstellungen in Übereinstimmung mit der Aufgabe.

   - **Benutzername**. Der Benutzername des Authentifizierungsagenten-Benutzerkontos entspricht standardmäßig dem Domänennamen des Benutzers.

   - **Anmeldung mit Kennwort erlauben**. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest. Bei Bedarf können Sie den Benutzer nach der ersten Authentifizierung nach dem neuen Kennwort fragen. Dadurch hat jeder Benutzer ein einmaliges Kennwort. Außerdem können Sie in der Richtlinie die Anforderungen an die Kennwortkomplexität für das Authentifizierungsagenten-Benutzerkonto festlegen.

   - **Anmeldung mit Zertifikat erlauben**. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus. Dadurch wird festgelegt, dass der Benutzer das Kennwort der Smartcard oder des Tokens eingeben muss.

- **Zugriff des Benutzerkontos auf verschlüsselte Daten**. Passen Sie den Zugriff des Benutzers auf einen verschlüsselten Datenträger an. Sie können beispielsweise die Benutzerauthentifizierung vorübergehend verbieten, ohne das Authentifizierungsagenten-Benutzerkonto zu löschen.

- **Kommentar**. Geben Sie bei Bedarf eine Beschreibung für das Benutzerkonto ein.

7. Speichern Sie die vorgenommenen Änderungen.

8. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

Nachdem die Aufgabe ausgeführt wurde, kann der neue Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang durchlaufen, das Betriebssystem starten und Zugriff auf einen verschlüsselten Datenträger erhalten.

Um das Kennwort und andere Einstellungen des Authentifizierungsagenten-Benutzerkontos zu ändern, muss ein spezieller Befehl zur Aufgabe *Authentifizierungsagenten-Konten verwalten* hinzugefügt werden. Eine Gruppenaufgabe ist beispielsweise geeignet, um das Token-Zertifikat des Administrators auf allen Computern zu ändern.

Ändern eines Authentifizierungsagenten-Benutzerkontos über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Eigenschaften der Aufgabe *Authentifizierungsagenten-Konten verwalten*.

2. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen**.

3. Klicken Sie auf **Hinzufügen → Befehl zum Ändern eines Benutzerkontos**.

4. Geben Sie im folgenden Fenster **Windows-Benutzerkonto** den Namen des Microsoft Windows-Benutzerkontos an, das Sie ändern möchten.

5. Wenn Sie den Namen des Windows-Kontos eingetippt haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   Mithilfe der Sicherheits-ID des Windows-Kontos wird überprüft, ob der Name des Windows-Kontos richtig eingegeben wurde. Wenn das Windows-Konto nicht auf dem Computer oder in der vertrauenswürdigen Domäne vorhanden ist, wird die Aufgabe *Authentifizierungsagenten-Konten verwalten* mit einem Fehler abgeschlossen.

6. Aktivieren Sie das Kontrollkästchen **Benutzername ändern** und geben Sie einen neuen Namen für das Benutzerkonto des Authentifizierungsagenten ein, damit Kaspersky Endpoint Security den Benutzernamen in den Namen aus dem darunter angebrachten Feld ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

7. Aktivieren Sie das Kontrollkästchen **Einstellungen für die Anmeldung mit Kennwort ändern**, um Zugriff auf die Einstellungen für die Anmeldung mit einem Kennwort zu erhalten.

8. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Kennwort erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort des Benutzerkontos für den Authentifizierungsagenten abfragt. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest.

9. Aktivieren Sie das Kontrollkästchen **Regel für die Kennwortänderung bei der Anmeldung im Authentifizierungsagenten ändern**, damit Kaspersky Endpoint Security den Wert für die Kennwortänderung in den darunter angegebenen Wert ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

10. Legen Sie einen Wert für die Kennwortänderung bei der Anmeldung über den Authentifizierungsagenten fest.

11. Aktivieren Sie das Kontrollkästchen **Einstellungen für die Anmeldung mit Zertifikat ändern**, um Zugriff auf die Einstellungen für die Anmeldung mit einem elektronischen Token- oder Smartcard-Zertifikat zu erhalten.

12. Aktivieren Sie das Kontrollkästchen **Anmeldung mit Zertifikat erlauben**, damit das Programm bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten das Kennwort für einen angeschlossenen Token oder eine Smartcard abfragt. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus.

13. Aktivieren Sie das Kontrollkästchen **Beschreibung des Befehls ändern** und ändern Sie die Beschreibung des Befehls, damit Kaspersky Endpoint Security die Beschreibung ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Microsoft-Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

14. Aktivieren Sie das Kontrollkästchen **Regel für den Zugriff auf die Anmeldung im Authentifizierungsagenten ändern**, damit Kaspersky Endpoint Security die Zugriffsregel für die Anmeldung über den Authentifizierungsagenten in die darunter angegebene Regel ändert. Die Änderung erfolgt für alle Benutzerkonten des Authentifizierungsagenten, die auf Basis des Windows-Benutzerkontos erstellt wurden, dessen Name im Feld **Windows-Benutzerkonto** angegeben ist.

15. Legen Sie eine Regel für den Zugriff auf die Authentifizierung im Authentifizierungsagenten fest.

16. Speichern Sie die vorgenommenen Änderungen.

Ändern eines Authentifizierungsagenten-Benutzerkontos über „Web Console"

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Authentifizierungsagenten-Konten verwalten**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Klicken Sie in der Liste der Benutzerkonten des Authentifizierungsagenten auf die Schaltfläche **Hinzufügen** und wählen Sie den Befehlstyp **Benutzerkonto ändern** aus.

5. Wählen Sie ein Benutzerkonto aus. Sie können das Benutzerkonto aus der Liste der Domänen-Benutzerkonten auswählen oder den Benutzerkonto-Namen eintippen. Weiter zum nächsten Schritt

   Kaspersky Endpoint Security ermittelt die Sicherheits-ID des Benutzerkontos (Security Identifier, SID). Dies ist für die Überprüfung des Benutzerkontos erforderlich. Wenn Sie den Benutzernamen falsch eingegeben haben, schließt Kaspersky Endpoint Security die Aufgabe mit einem Fehler ab.

6. Aktivieren Sie die Kontrollkästchen neben den Einstellungen, die Sie ändern möchten.

7. Passen Sie die Einstellungen des Authentifizierungsagenten-Benutzerkontos an.

   - **Neues Authentifizierungsagenten-Benutzerkonto erstellen anstelle des vorhandenen Kontos**. Kaspersky Endpoint Security überprüft die vorhandenen Authentifizierungsagent-Benutzerkonten auf dem Computer. Wenn die Sicherheits-ID des Benutzers auf dem Computer und in der Aufgabe übereinstimmen, ändert Kaspersky Endpoint Security die Benutzerkonto-Einstellungen in Übereinstimmung mit der Aufgabe.

   - **Benutzername**. Der Benutzername des Authentifizierungsagenten-Benutzerkontos entspricht standardmäßig dem Domänennamen des Benutzers.

   - **Anmeldung mit Kennwort erlauben**. Legen Sie ein Kennwort für das Authentifizierungsagenten-Benutzerkonto fest. Bei Bedarf können Sie den Benutzer nach der ersten Authentifizierung nach dem neuen Kennwort fragen. Dadurch hat jeder Benutzer ein einmaliges Kennwort. Außerdem können Sie in der Richtlinie die Anforderungen an die Kennwortkomplexität für das Authentifizierungsagenten-Benutzerkonto festlegen.

   - **Anmeldung mit Zertifikat erlauben**. Wählen Sie eine Zertifikatsdatei für die Authentifizierung mithilfe einer Smartcard oder eines Tokens aus. Dadurch wird festgelegt, dass der Benutzer das Kennwort der Smartcard oder des Tokens eingeben muss.

   - **Zugriff des Benutzerkontos auf verschlüsselte Daten**. Passen Sie den Zugriff des Benutzers auf einen verschlüsselten Datenträger an. Sie können beispielsweise die Benutzerauthentifizierung vorübergehend verbieten, ohne das Authentifizierungsagenten-Benutzerkonto zu löschen.

   - **Kommentar**. Geben Sie bei Bedarf eine Beschreibung für das Benutzerkonto ein.

8. Speichern Sie die vorgenommenen Änderungen.

9. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

Um ein Authentifizierungsagenten-Benutzerkonto zu löschen, muss ein spezieller Befehl zur Aufgabe *Authentifizierungsagenten-Konten verwalten* hinzugefügt werden. Eine Gruppenaufgabe ist beispielsweise geeignet, um das Benutzerkonto eines entlassenen Mitarbeiters zu löschen.

Löschen eines Authentifizierungsagenten-Benutzerkontos über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Eigenschaften der Aufgabe *Authentifizierungsagenten-Konten verwalten*.

2. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen**.

3. Klicken Sie auf **Hinzufügen → Befehl zum Löschen eines Benutzerkontos**.

4. Geben Sie im folgenden Fenster im Feld **Windows-Benutzerkonto** den Namen des Windows-Kontos an, auf dessen Basis das zu löschende Authentifizierungsagenten-Benutzerkonto erstellt wurde.

5. Wenn Sie den Namen des Windows-Kontos eingetippt haben, klicken Sie auf **Erlauben**, um die Sicherheits-ID (SID, Security Identifier) zu ermitteln.

   Wenn Sie die Sicherheits-ID nicht mithilfe der Schaltfläche **Erlauben** ermitteln, wird sie ermittelt, wenn die Aufgabe auf dem Computer ausgeführt wird.

   > Mithilfe der Sicherheits-ID des Windows-Kontos wird überprüft, ob der Name des Windows-Kontos richtig eingegeben wurde. Wenn das Windows-Konto nicht auf dem Computer oder in der vertrauenswürdigen Domäne vorhanden ist, wird die Aufgabe *Authentifizierungsagenten-Konten verwalten* mit einem Fehler abgeschlossen.

6. Speichern Sie die vorgenommenen Änderungen.

Löschen eines Authentifizierungsagenten-Benutzerkontos über „Web Console"

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **Authentifizierungsagenten-Konten verwalten**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Klicken Sie in der Liste der Benutzerkonten des Authentifizierungsagenten auf die Schaltfläche **Hinzufügen** und wählen Sie den Befehlstyp **Benutzerkonto löschen** aus.

5. Wählen Sie ein Benutzerkonto aus. Sie können das Benutzerkonto aus der Liste der Domänen-Benutzerkonten auswählen oder den Benutzerkonto-Namen eintippen.

6. Speichern Sie die vorgenommenen Änderungen.

7. Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**.

   Nachdem die Aufgabe ausgeführt wurde, kann der Benutzer beim nächsten Start des Computers den Authentifizierungsvorgang nicht durchlaufen und das Betriebssystem nicht starten. Kaspersky Endpoint Security verbietet den Zugriff auf die verschlüsselten Daten.

Eine Liste der Benutzer, welche die Authentifizierung mithilfe des Assistenten durchlaufen und das Betriebssystem starten können, können Sie in den Eigenschaften des verwalteten Computers einsehen.

Anzeigen einer Liste der Authentifizierungsagenten-Benutzerkonten über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Geräte** aus.

3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.

4. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Aufgaben** aus.

5. Wählen Sie in der Aufgabenliste **Authentifizierungsagenten-Konten verwalten** aus und doppelklicken Sie auf die Aufgabeneigenschaften.

6. Wählen Sie in den Aufgabeneigenschaften den Abschnitt **Einstellungen**.

   Eine Liste der Authentifizierungsagenten-Benutzerkonten auf diesem Computer wird angezeigt. Nur die Benutzer aus dieser Liste können die Authentifizierung mithilfe des Assistenten durchlaufen und das Betriebssystem starten.

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Klicken Sie auf den Namen des Computers, auf dem Sie die Liste der Authentifizierungsagenten-Benutzerkonten einsehen möchten.

3. Wählen Sie in den Computereigenschaften die Registerkarte **Aufgaben** aus.

4. Wählen Sie in der Aufgabenliste den Punkt **Authentifizierungsagenten-Konten verwalten** aus.

5. Wählen Sie in den Eigenschaften der Aufgabe die Registerkarte **Anwendungseinstellungen** aus.

Eine Liste der Authentifizierungsagenten-Benutzerkonten auf diesem Computer wird angezeigt. Nur die Benutzer aus dieser Liste können die Authentifizierung mithilfe des Assistenten durchlaufen und das Betriebssystem starten.

Verwendung eines Tokens oder einer Smartcard bei der Arbeit mit dem Authentifizierungsagenten

Bei der Authentifizierung für den Zugriff auf verschlüsselte Festplatten kann ein Token oder eine Smartcard verwendet werden. Dazu muss die Datei des elektronischen Token- oder Smartcard-Zertifikats zur Aufgabe *Authentifizierungsagenten-Konten verwalten* hinzugefügt werden.

Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

Kaspersky Endpoint Security unterstützt folgende Tokens, Smartcard-Lesegeräte und Smartcards:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Um die Datei des elektronischen Zertifikats für einen Token oder eine Smartcard zu dem Befehl hinzuzufügen, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird, muss die Datei zuerst mithilfe des Zertifikatsverwaltungsprogramms eines Drittanbieters gespeichert werden.

Das Zertifikat für den Token oder die Smartcard muss folgende Eigenschaften besitzen:

- Das Zertifikat entspricht dem Standard X.509 und die Zertifikatsdatei besitzt die Codierung DER.
- Das Zertifikat enthält einen RSA-Schlüssel mit einer Mindestlänge von 1024 Bit.

Wenn das elektronische Token- oder Smartcard-Zertifikat diese Voraussetzungen nicht erfüllt, ist es nicht möglich, die Zertifikatsdatei in den Befehl zu laden, mit dem das Authentifizierungsagenten-Benutzerkonto erstellt wird.

Außerdem muss der Parameter `KeyUsage` des Zertifikats den Wert `keyEncipherment` oder `dataEncipherment` besitzen. Der Parameter `KeyUsage` bestimmt den Zweck des Zertifikats. Wenn der Parameter einen anderen Wert hat, lädt Kaspersky Security Center die Zertifikatsdatei zwar, es erscheint aber eine Warnung.

Hat der Benutzer den Token oder die Smartcard verloren, so muss der Administrator die elektronische Zertifikatdatei des neuen Tokens oder der neuen Smartcard zum Befehl für das Erstellen des Authentifizierungsagenten-Benutzerkontos hinzufügen. Anschließend muss der Benutzer den Vorgang zur Freigabe von verschlüsselten Geräten oder zur Datenwiederherstellung auf verschlüsselten Geräten durchführen.

Entschlüsselung von Festplatten

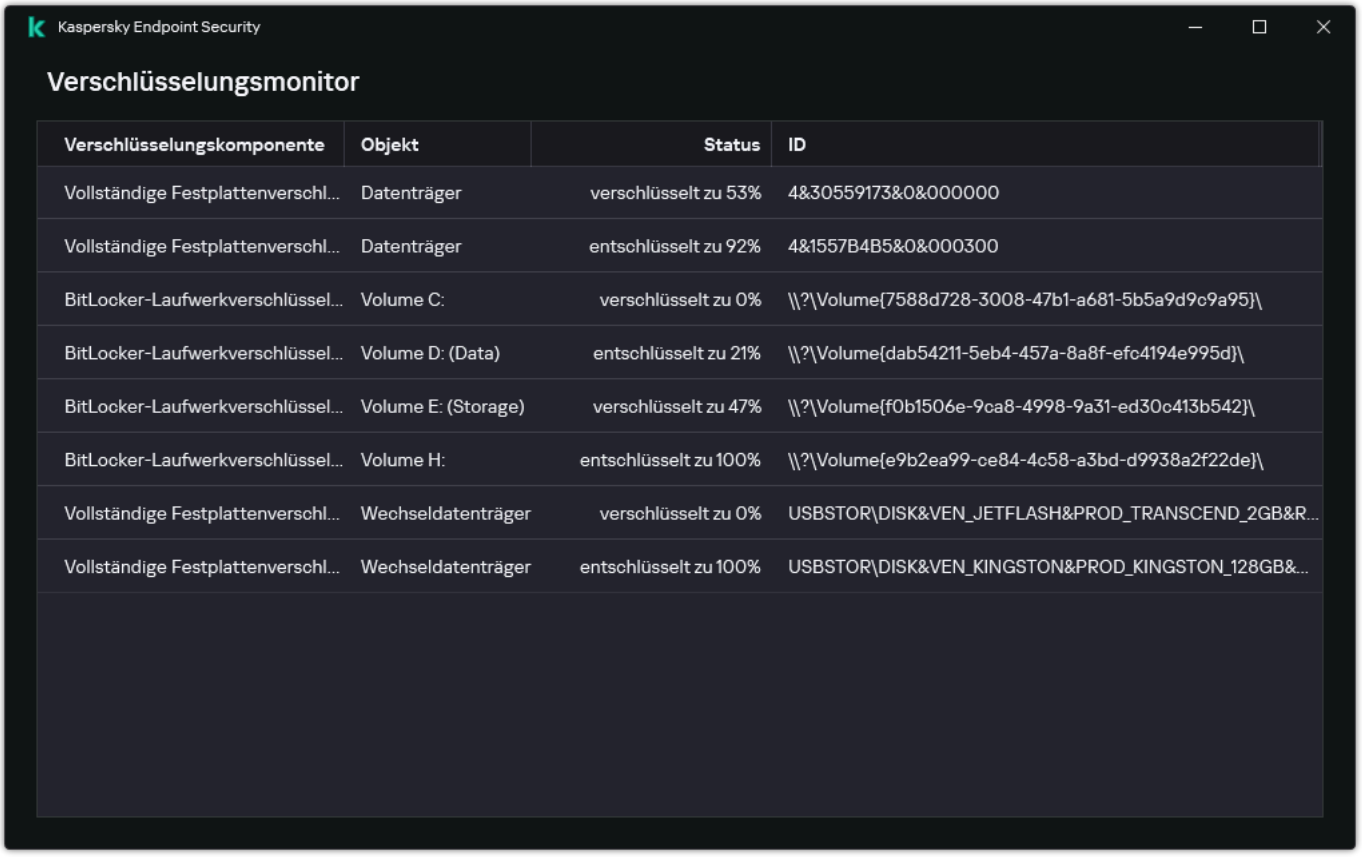
Sie können Festplatten auch dann entschlüsseln, wenn keine aktuelle Lizenz vorliegt, welche die Datenverschlüsselung zulässt.

Gehen Sie folgendermaßen vor, um Festplatten zu entschlüsseln:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** das Verfahren, mit dem die Festplatten verschlüsselt wurden.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** das Element **Alle Festplatten entschlüsseln**, wenn Sie alle verschlüsselten Festplatten entschlüsseln möchten.
   - Fügen Sie in der Tabelle **Folgende Festplatten nicht verschlüsseln** alle verschlüsselten Festplatten hinzu, die Sie entschlüsseln möchten.

     Diese Variante ist nur für das Verschlüsselungsverfahren „Kaspersky-Festplattenverschlüsselung“ verfügbar.
6. Speichern Sie die vorgenommenen Änderungen.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool „Encryption Monitor“ kann über das Programmhauptfenster ausgeführt werden.



Verschlüsselungsmonitor

Wenn der Benutzer während der Entschlüsselung von Festplatten, die mit dem Verfahren Kaspersky-Festplattenverschlüsselung verschlüsselt wurden, den Computer ausschaltet oder neu startet, wird der Authentifizierungsagent vor dem nächsten Start des Betriebssystems geladen. Nach der Authentifizierung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die Entschlüsselung der Festplatten fort.

Wechselt das Betriebssystem während der Entschlüsselung von Festplatten, die mit dem Verfahren Kaspersky-Festplattenverschlüsselung verschlüsselt wurden, in den Ruhezustand (hibernation mode), so wird der Authentifizierungsagent beim Beenden des Ruhezustandes geladen. Nach der Authentifizierung im Agenten und dem Hochfahren des Betriebssystems setzt Kaspersky Endpoint Security die Entschlüsselung der Festplatten fort. Nach der Entschlüsselung der Festplatten ist der Ruhezustand erst wieder verfügbar, nachdem das Betriebssystem neu gestartet wurde.

Wechselt das Betriebssystem während der Festplattenentschlüsselung in den Energiesparmodus (sleep mode), so setzt Kaspersky Endpoint Security beim Beenden des Energiesparmodus die Festplattenentschlüsselung fort, ohne den Authentifizierungsagenten zu laden.

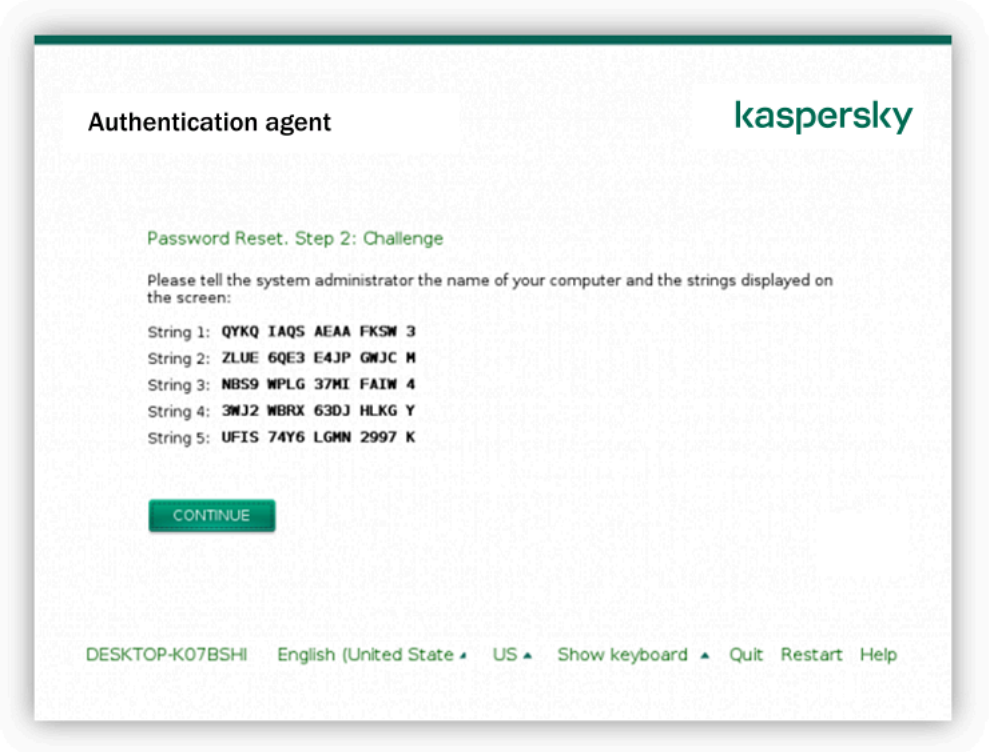
Wiederherstellen des Zugriffs auf einen Datenträger, der mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist

Wenn der Benutzer das Kennwort für den Zugriff auf eine Festplatte vergessen hat, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist, muss ein Wiederherstellungsvorgang („Anfrage-Frage“) ausgeführt werden. Sie können auch das Dienstkonto verwenden, um Zugriff auf die Festplatte zu erhalten, falls diese Funktion in den Einstellungen der Festplattenverschlüsselung aktiviert ist.

Wiederherstellen des Zugriffs auf eine Systemfestplatte

Um den Zugriff auf eine Systemfestplatte wiederherzustellen, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist, sind folgende Schritte erforderlich:

1. Der Benutzer übermittelt die Anfrageblöcke an den Administrator (s. Abb. unten).
2. Der Administrator gibt die Anfrageblöcke in Kaspersky Security Center ein, erhält Antwortblöcke und übermittelt die Antwortblöcke an den Benutzer.
3. Der Benutzer gibt die Antwortblöcke auf der Benutzeroberfläche des Authentifizierungsagenten ein und erhält Zugriff auf die Festplatte.



Wiederherstellen des Zugriffs auf eine Systemfestplatte, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist

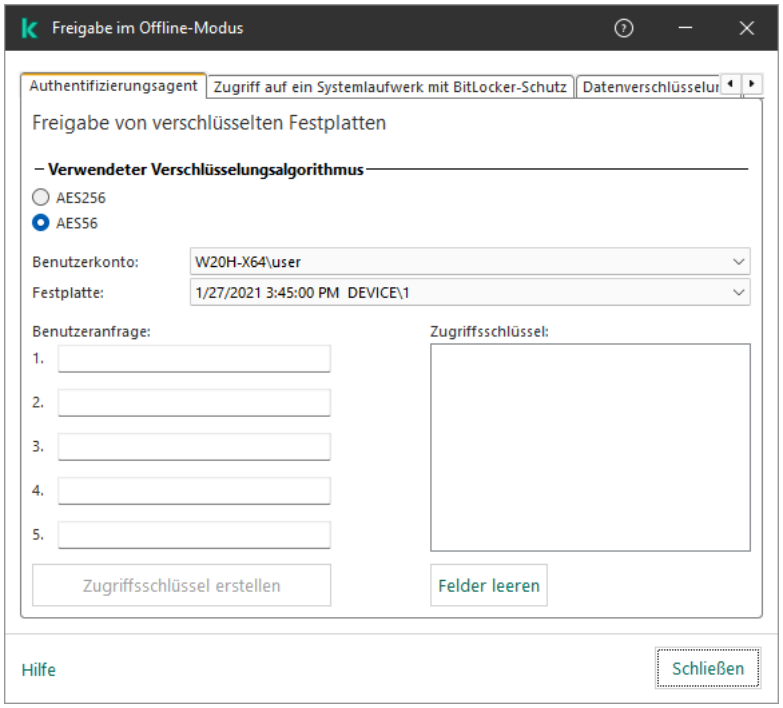
Um den Wiederherstellungsvorgang zu starten, muss der Benutzer auf der Benutzeroberfläche des Authentifizierungsagenten auf die Schaltfläche **Forgot your password** klicken.

In der Verwaltungskonsole (MMC) die Antwortblöcke für eine Systemfestplatte anfordern, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Geräte** aus.
3. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der den Zugriff auf verschlüsselte Daten wiederherstellen möchte, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
4. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Authentifizierungsagent**-Registerkarte aus.
6. Wählen Sie im Block **Verwendeter Verschlüsselungsalgorithmus** einen Verschlüsselungsalgorithmus aus: **AES56** oder **AES256**.

   Der Datenverschlüsselungsalgorithmus ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Starke Verschlüsselung (AES256)* oder *Leichte Verschlüsselung (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.
7. Wählen Sie in der Dropdown-Liste **Benutzerkonto** das Authentifizierungsagenten-Konto des Benutzers aus, der die Zugriffswiederherstellung für das Laufwerk angefordert hat.
8. Wählen Sie in der Dropdown-Liste **Festplatte** die verschlüsselte Festplatte, auf welche der Zugriff wiederhergestellt werden soll.
9. Geben Sie im Block **Benutzeranfrage** die Anfrageblöcke ein, die Ihnen der Benutzer diktiert hat.

Im Feld **Zugriffsschlüssel** wird der Inhalt der Antwortblöcke für die Benutzeranfrage angezeigt, die der Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto dient. Übermitteln Sie den Inhalt der Antwortblöcke an den Benutzer.



Zugriff im Offline-Modus gewähren

In der „Web Console“ die Antwortblöcke für eine Systemfestplatte anfordern, die mit der Technologie „Kaspersky-Festplattenverschlüsselung“ geschützt ist

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Assets (Geräte)** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Laufwerkszugriff wiederherstellen möchten.
3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.
4. Wählen Sie im folgenden Fenster den Abschnitt **Authentifizierungsagent**.
5. Wählen Sie in der Liste **Benutzerkonto** den Namen des Authentifizierungsagenten-Benutzerkontos, das für jenen Benutzer erstellt wurde, der die Wiederherstellung des Benutzernamens und Kennworts für das Authentifizierungsagenten-Benutzerkonto beantragt hat.
6. Geben Sie die Anfrageblöcke ein, die Ihnen der Benutzer diktiert hat.

   Der Inhalt der Antwortblöcke für die Benutzeranfrage, die zur Wiederherstellung des Benutzernamens und des Kennworts für das Authentifizierungsagenten-Benutzerkonto dient, wird im unteren Fensterbereich angezeigt. Übermitteln Sie den Inhalt der Antwortblöcke an den Benutzer.

Nach erfolgreichem Wiederherstellungsvorgang fordert der Authentifizierungsagent den Benutzer auf, das Kennwort zu ändern.

Wiederherstellen des Zugriffs auf eine Nicht-Systemfestplatte

Um den Zugriff auf eine Nicht-Systemfestplatte wiederherzustellen, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt ist, sind die folgenden Schritte erforderlich:

1. Der Benutzer sendet eine Zugriffsanfrage-Datei an den Administrator.
2. Der Administrator fügt die Zugriffsanfrage-Datei in Kaspersky Security Center hinzu, erstellt eine Zugriffsschlüsseldatei und sendet diese Datei an den Benutzer.
3. Der Benutzer fügt die Zugriffsschlüsseldatei in Kaspersky Endpoint Security hinzu und erhält Zugriff auf die Festplatte.

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer auf die Festplatte zugreifen. Dann erstellt Kaspersky Endpoint Security eine Zugriffsanfrage-Datei (Datei mit der Erweiterung kesdc), die beispielsweise per E-Mail an den Administrator übermittelt werden muss.

In der Verwaltungskonsole (MMC) eine Zugriffsschlüsseldatei für eine verschlüsselte Nicht-Systemfestplatte anfordern

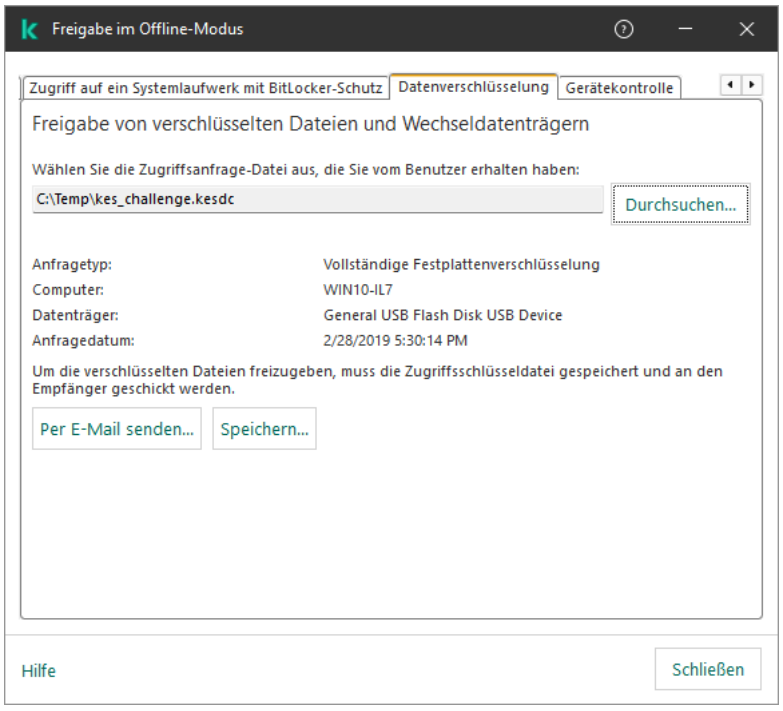
1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Geräte** aus.
3. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der den Zugriff auf verschlüsselte Daten wiederherstellen möchte, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
4. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus**.

5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Datenverschlüsselung**-Registerkarte aus.

6. Klicken Sie auf der Registerkarte **Datenverschlüsselung** auf **Durchsuchen**.

7. Geben Sie im Auswahlfenster der Zugriffsanfrage-Datei den Pfad der Datei an, die Sie vom Benutzer erhalten haben.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.



Zugriff im Offline-Modus gewähren

In der „Web Console“ eine Zugriffsschlüsseldatei für eine verschlüsselte Nicht-Systemfestplatte anfordern

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Datenzugriff wiederherstellen möchten.

3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.

4. Wählen Sie den Punkt **Datenverschlüsselung**.

5. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung kesdc).

   Die „Web Console“ zeigt Informationen über die Anfrage an. Unter anderem den Namen des Computers, auf dem der Benutzer Zugriff auf eine Datei anfordert.

6. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung kesdr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Anmeldung mit dem Authentifizierungsagenten-Dienstkonto

In Kaspersky Endpoint Security können Sie ein Authentifizierungsagenten-Dienstkonto hinzufügen, wenn Sie eine Festplatte verschlüsseln. Das Dienstkonto wird beispielsweise benötigt, um Zugriff auf den Computer zu erhalten, wenn der Benutzer das Kennwort vergisst. Sie können das Dienstkonto auch als Reservekonto verwenden. Um ein Benutzerkonto hinzuzufügen, wählen Sie in den Einstellungen der Festplattenverschlüsselung ein Dienstkonto aus und geben Sie den Namen des Benutzerkontos ein (Standardwert `ServiceAccount`). Zur Authentifizierung über den Agenten benötigen Sie ein Einmalkennwort.

So erhalten Sie das Einmalkennwort über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
4. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Aufgaben** aus.
5. Wählen Sie in der Aufgabenliste **Authentifizierungsagenten-Konten verwalten** aus und doppelklicken Sie auf die Aufgabeneigenschaften.
6. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Einstellungen** aus.
7. Wählen Sie in der Kontenliste das Authentifizierungsagenten-Dienstkonto aus (z. B. `WIN10-USER\ServiceAccount`).
8. Wählen Sie in der Dropdown-Liste **Aktion** die Option **Benutzerkonto anzeigen**.
9. Aktivieren Sie in den Kontoeigenschaften das Kontrollkästchen **Ursprüngliches Kennwort anzeigen**.
10. Kopieren Sie das Einmalkennwort zur Anmeldung bei dem Dienstkonto.

So erhalten Sie das Einmalkennwort über die „Web Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die Liste der Authentifizierungsagenten-Benutzerkonten einsehen möchten.

   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie in den Computereigenschaften die Registerkarte **Aufgaben** aus.
4. Wählen Sie in der Aufgabenliste den Punkt **Authentifizierungsagenten-Konten verwalten** aus.
5. Wählen Sie in den Eigenschaften der Aufgabe die Registerkarte **Anwendungseinstellungen** aus.
6. Wählen Sie in der Kontenliste das Authentifizierungsagenten-Dienstkonto aus (z. B. `WIN10-USER\ServiceAccount`).

7. Aktivieren Sie in den Kontoeigenschaften das Kontrollkästchen **Kennwort anzeigen**.

8. Kopieren Sie das Einmalkennwort zur Anmeldung bei dem Dienstkonto.

Kaspersky Endpoint Security aktualisiert das Kennwort jedes Mal automatisch, wenn sich ein Benutzer beim Dienstkonto authentifiziert. Nach der Authentifizierung mithilfe des Agenten müssen Sie das Kennwort für das Windows-Konto eingeben. Bei der Anmeldung mit dem Dienstkonto können Sie die SSO-Technologie nicht verwenden.

Update des Betriebssystems

Ein Update des Betriebssystems eines Computers, der mithilfe der vollständigen Festplattenverschlüsselung (FDE) geschützt ist, besitzt bestimmte Besonderheiten. Gehen Sie beim Update des Betriebssystems schrittweise vor: Aktualisieren Sie zuerst das Betriebssystem auf einem Computer, dann auf einigen weiteren Computern, und schließlich auf allen Computern des Netzwerks.

Wenn Sie die Kaspersky-Verschlüsselungstechnologie verwenden, wird vor dem Systemstart der „Authentifizierungsagent“ geladen. Mithilfe des „Authentifizierungsagenten“ meldet sich der Benutzer beim System an und erhält Zugriff auf die verschlüsselten Datenträger. Danach beginnt der Start des Betriebssystems. Wenn das Update des Betriebssystems auf einem Computer gestartet wird, der mithilfe der Technologie „Kaspersky-Festplattenverschlüsselung“ geschützt ist, so kann der Betriebssystem-Update-Assistent den „Authentifizierungsagenten“ entfernen. Dadurch wird der Computer möglicherweise gesperrt, da das Ladeprogramm des Betriebssystems nicht auf den verschlüsselten Datenträger zugreifen kann.

Funktionen des Betriebssystem-Updates:

- **Aktualisierung des Betriebssystems über WSUS**. Sie können das Betriebssystem wie gewohnt aktualisieren.
- **Aktualisierung des Betriebssystems aus einem ISO-Image**. Zur Aktualisierung des Betriebssystems müssen Sie den Ordner mit den Treibern für die Kaspersky-Festplattenverschlüsselung angeben. Das Programm kopiert die Treiber automatisch in einen speziellen Ordner. Gehen Sie wie folgt vor:

  1. Binden Sie das ISO-Image ein.

  2. Starten Sie die Installation des System-Updates mit der folgenden Eingabe:

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
     ```

Das automatische Betriebssystem-Update ist nur verfügbar, wenn auf dem Computer Windows 10 1607 (RS1) oder höher ausgeführt wird. Wenn Sie frühere Betriebssystemversionen upgraden möchten, gehen Sie wie folgt vor: zuerst den Datenträger entschlüsseln, dann ein Betriebssystem-Upgrade durchführen und anschließend den Datenträger verschlüsseln.

Wenn Sie die BitLocker-Verschlüsselungstechnologie verwenden, müssen die Festplatten nicht entschlüsselt werden, um Windows 10 zu aktualisieren. Details über BitLocker finden Sie auf der Microsoft-Website.

Behebung von Fehlern beim Upgrade der Verschlüsselungsfunktionalität

Die vollständige Festplattenverschlüsselung wird beim Upgrade einer älteren Version auf Kaspersky Endpoint Security für Windows 14.2 aktualisiert.

Beim Start des Upgrades der Funktionalität zur vollständigen Festplattenverschlüsselung können folgende Fehler auftreten:

- Das Update konnte nicht initialisiert werden.
- Das Gerät ist mit dem Authentifizierungsagenten nicht kompatibel.

Um Fehler zu beheben, die beim Start des Upgrades der Funktionalität zur vollständigen Festplattenverschlüsselung aufgetreten sind, gehen Sie in der neuen Programmversion wie folgt vor:

1. Entschlüsseln Sie die Festplatten.
2. Verschlüsseln Sie die Festplatten erneut.

Beim Upgrade der Funktionalität für die vollständige Festplattenverschlüsselung können folgende Fehler auftreten:

- Das Update konnte nicht abgeschlossen werden.
- Das Upgrade der Verschlüsselungsfunktionalität wurde mit einem Fehler abgeschlossen.

Um Fehler zu beheben, die im Verlauf des Upgrades der Funktionalität zur vollständigen Festplattenverschlüsselung aufgetreten sind,

stellen Sie den Zugriff auf das verschlüsselte Gerät mithilfe des Reparatur-Tools wieder her.

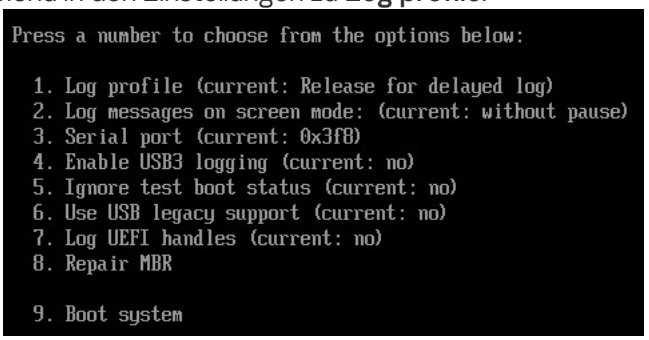
Ablaufverfolgung des Authentifizierungsagenten

Das Programm zeichnet folgende Informationen in einer Protokolldatei auf: Dienstinformationen über die Verwendung des Authentifizierungsagenten und Informationen über die Benutzeraktionen im Authentifizierungsagenten.

So aktivieren Sie die Ablaufverfolgung des Authentifizierungsagenten:

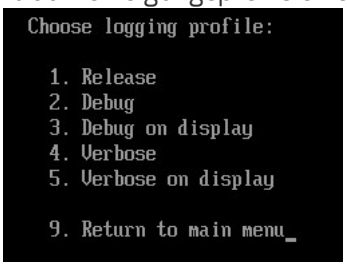
1. Aktivieren Sie die Ablaufverfolgung für Kaspersky Endpoint Security.
2. Starten Sie den Computer neu.
3. Drücken Sie sofort nach dem Start des Computers, dessen Festplatten verschlüsselt sind, die Taste **F3**, um das Fenster mit den Einstellungen des Authentifizierungsagenten zu öffnen.
4. Wählen Sie nach dem Start des FDE-Bootloaders den Bootmanager **KES (FDE <version>)** aus.

5. Gehen Sie im Bootmanager-Menü in den Einstellungen zu **Log profile**.



Bootmanager-Menü

6. Wählen Sie im Konfigurationsfenster des Ablaufverfolgungsprofils eine Ablaufverfolgungsstufe aus:



Ablaufverfolgungsstufen für den Authentifizierungsagenten

- **Release**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei keine Informationen über die Ereignisse des Authentifizierungsagenten.
- **Debug**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten.
- **Debug on display**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten. Außerdem werden die Informationen über den COM-Port übertragen.

  Ist der Computer, dessen Festplatten verschlüsselt sind, über den COM-Port mit einem anderen Computer verbunden, so können die Ereignisse des Authentifizierungsagenten mithilfe des anderen Computers verfolgt werden.
- **Verbose**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei detaillierte Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten.

  Für diese Stufe gilt ein höherer Genauigkeitsgrad als bei Auswahl der Stufe **Debug**. Durch die hohe Aufzeichnungsgenauigkeit kann das Laden des Authentifizierungsagenten und des Betriebssystems verlangsamt werden.
- **Verbose on display**. Bei Auswahl dieser Variante speichert das Programm in der Protokolldatei detaillierte Informationen über die Verwendung des Authentifizierungsagenten und über die Benutzeraktionen im Authentifizierungsagenten. Außerdem werden die Informationen über den COM-Port übertragen.

  Für diese Stufe gilt ein höherer Genauigkeitsgrad als bei Auswahl der Stufe **Debug on display**. Durch die hohe Aufzeichnungsgenauigkeit kann das Laden des Authentifizierungsagenten und des Betriebssystems verlangsamt werden.

Nachdem Sie eine Ablaufverfolgungsstufe ausgewählt haben, erscheint wieder das Bootmanager-Menü.

7. Wählen Sie im Bootmanager-Menü den Punkt **Boot system** aus.

   Der FDE-Bootloader startet den Authentifizierungsagenten.

   Reproduzieren Sie das Problem.

   Eine Protokolldatei des Authentifizierungsagenten wird dann aufgezeichnet, wenn auf dem Computer verschlüsselte Festplatten vorhanden sind oder wenn die vollständige Festplattenverschlüsselung ausgeführt wird.

8. Um die Ablaufverfolgung zu beenden, kehren Sie ins Fenster „Support-Tools“ zurück und deaktivieren Sie die Ablaufverfolgung.

Dadurch werden im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` Ablaufverfolgungsdateien über den Betrieb des Authentifizierungsagenten KES.SRV erstellt. Die Protokolldatei des Authentifizierungsagenten wird im Gegensatz zu anderen Protokolldateien für das Programm nicht an Kaspersky übertragen. Falls erforderlich, können Sie die Protokolldatei des Authentifizierungsagenten selbst zur Analyse an Kaspersky schicken.

Hilfetexte für den Authentifizierungsagenten ändern

Bevor Sie die Hilfetexte für den Authentifizierungsagenten ändern, beachten Sie die Liste der Zeichen, die in der Preboot-Umgebung unterstützt werden (s. unten).

Um die Hilfetexte für den Authentifizierungsagenten zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Allgemeine Verschlüsselungseinstellungen** aus.
4. Klicken Sie im Block **Vorlagen** auf **Hilfe**.
5. Gehen Sie im angezeigten Fenster wie folgt vor:

   - Öffnen Sie die Registerkarte **Authentifizierung**, um den Hilfetext zu ändern, welcher im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem die Anmeldedaten eingegeben werden.
   - Öffnen Sie die Registerkarte **Kennwort ändern**, um den Hilfetext zu ändern, der im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem das Kennwort für ein Benutzerkonto für den Authentifizierungsagenten geändert wird.
   - Öffnen Sie die Registerkarte **Kennwort wiederherstellen**, um den Hilfetext zu ändern, der im Fenster des Authentifizierungsagenten bei dem Schritt angezeigt wird, bei dem das Kennwort für ein Benutzerkonto für den Authentifizierungsagenten wiederhergestellt wird.

6. Ändern Sie die Hilfetexte.

   Um den ursprünglichen Text wiederherzustellen, klicken Sie auf **Standard**.

Der Hilfetext kann maximal 16 Zeilen umfassen. Die maximale Zeilenlänge beträgt 64 Zeichen.

7. Speichern Sie die vorgenommenen Änderungen.

Beschränkungen für die Zeichenunterstützung in Hilfetexten für den Authentifizierungsagenten

In der Preboot-Umgebung werden folgende Unicode-Zeichen unterstützt:

- Basis-Lateinisch (0000 - 007F)
- Lateinisch-1, Ergänzung (0080 - 00FF)
- Lateinisch, erweitert-A (0100 - 017F)
- Lateinisch, erweitert-B (0180 - 024F)
- Spacing Modifier Letters (02B0 - 02FF)
- Kombinierende diakritische Zeichen (0300 - 036F)
- Griechisch und Koptisch (0370 - 03FF)
- Kyrillisch (0400 - 04FF)
- Hebräisch (0590 - 05FF)
- Arabisch (0600 - 06FF)
- Lateinisch, weiterer Zusatz (1E00 - 1EFF)
- Allgemeine Interpunktion (2000 - 206F)
- Währungszeichen (20A0 - 20CF)
- Buchstabenähnliche Symbole (2100 - 214F)
- Geometrische Formen (25A0 - 25FF)
- Arabische Präsentationsformen-B (FE70 - FEFF)

Zeichen, die nicht in dieser Liste angegeben sind, werden in der Preboot-Umgebung nicht unterstützt. Es wird davon abgeraten, solche Zeichen in den Hilfetexten des Authentifizierungsagenten zu verwenden.

Objekte und Daten löschen, die nach dem Testlauf des Authentifizierungsagenten verblieben sind

Wenn bei der Deinstallation des Programms Kaspersky Endpoint Security Objekte und Daten gefunden werden, die nach einem Testlauf des Authentifizierungsagenten auf der Systemfestplatte verblieben sind, so wird die Programmdeinstallation abgebrochen und kann erst wieder gestartet werden, nachdem diese Objekte und Daten gelöscht wurden.

Objekte und Daten verbleiben nach einem Testlauf des Authentifizierungsagenten nur in Ausnahmefällen auf der Systemfestplatte. Dies kann beispielsweise vorkommen, wenn der Computer nach dem Übernehmen der Richtlinie für Kaspersky Security Center, die entsprechende Verschlüsselungseinstellungen enthält, noch nicht neu gestartet wurde oder wenn das Programm nach einem Testlauf des Authentifizierungsagenten nicht gestartet wird.

Es gibt folgende Methoden, um Objekte und Daten zu löschen, die nach einem Testlauf des Authentifizierungsagenten auf der Systemfestplatte verblieben sind:

- mithilfe der Richtlinie für Kaspersky Security Center
- mithilfe des Reparatur-Tools.

Um die Objekte und Daten, die nach einem Testlauf des Authentifizierungsagenten verblieben sind, mithilfe der Richtlinie für Kaspersky Security Center zu löschen, gehen Sie wie folgt vor:

1. Übernehmen Sie für den Computer die Richtlinie für Kaspersky Security Center mit den Einstellungen, die für die Entschlüsselung aller Computerfestplatten gelten.
2. Starten Sie Kaspersky Endpoint Security.

Um die Objekte und Daten, die nach einem Testlauf des Authentifizierungsagenten verblieben sind, mithilfe des Reparatur-Tools zu löschen, gehen Sie wie folgt vor:

1. Führen Sie die Datei mit dem Namen fdert.exe aus, die die ausführbare Datei des Wiederherstellungsprogramms ist. Diese Datei wird von Kaspersky Endpoint Security erstellt.
2. Wählen Sie im Fenster „Reparatur-Tool“ das erforderliche Gerät aus.
3. Klicken Sie auf **Untersuchung**.
4. Wenn Sie nach der Diagnose der Systemfestplatte eine Meldung erhalten, dass Objekte und Daten aus dem Testbetrieb des Authentifizierungsagenten verblieben sind, klicken Sie auf **Objekte und AA-Daten entfernen**.

   Die Schaltfläche **Objekte und AA-Daten entfernen** ist nur verfügbar, wenn Objekte und Daten erkannt werden, die nach dem Testbetrieb des Authentifizierungsagenten verblieben sind.

Um Daten über die Inkompatibilität des Authentifizierungsagenten zu löschen,

geben Sie in der Befehlszeile ein: `avp pbatestreset`.

Verwaltung von BitLocker

BitLocker ist eine integrierte Verschlüsselungstechnologie des Windows-Betriebssystems.
Kaspersky Endpoint Security ermöglicht es, BitLocker mithilfe der Infrastruktur von Kaspersky Next zu kontrollieren und zu verwalten. BitLocker verschlüsselt ein logisches Volume. Wechseldatenträger können mithilfe von BitLocker nicht verschlüsselt werden. Details über BitLocker finden Sie in der Microsoft-Dokumentation.

Wenn der Datenträger verschlüsselt wird, legt BitLocker den Bootloader und andere Hilfsdateien in der system partition ab. Diese Partition ist nicht verschlüsselt. Die Systempartition wird vom Betriebssystem automatisch während der Windows-Installation erstellt. Wenn die Festplatte vor der Windows-Installation vollständig partitioniert ist, kann das Betriebssystem keine Systempartition erstellen. In diesem Fall werden Sie beim Starten der BitLocker-Festplattenverschlüsselung vom Betriebssystem aufgefordert, das Laufwerk neu zu partitionieren und eine Systempartition zu erstellen. Nachdem eine Systempartition erstellt wurde, startet das Betriebssystem die BitLocker-Verschlüsselung.

Der BitLocker-Verschlüsselungsalgorithmus ist nicht von der Version der AES-Bibliothek abhängig, die im Lieferumfang enthalten ist (AES256 oder AES56). Bei der Verschlüsselung wird die integrierte Verschlüsselungsbibliothek des Betriebssystems verwendet.

Zur Verschlüsselung von Geräten, die noch nie verschlüsselt waren, verwendet die Anwendung den BitLocker-Verschlüsselungsalgorithmus mit einer effektiven Schlüssellänge von 256 Bit. Für ein Gerät, das bereits verschlüsselt war, bevor die Anwendung installiert wurde, kann der Verschlüsselungsalgorithmus unterschiedlich sein. Ausführliche Informationen zur Auswahl des Verschlüsselungsalgorithmus finden Sie auf der Website des Technischen Supports von Microsoft. Ab Version 12.9 sendet Kaspersky Endpoint Security den ursprünglichen Wiederherstellungsschlüssel für Geräte, die zuvor mit Drittanbieter-Anwendungen verschlüsselt wurden, an Kaspersky Security Center.

Die Sicherheit beim Speichern von Zugriffsschlüsseln gewährleistet BitLocker mithilfe von Trusted Platform Module. *Trusted Platform Module* (TMP) ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Ein Trusted Platform Module wird normalerweise auf der Hauptplatine des Computers installiert und interagiert mit allen anderen Systemkomponenten über die Hardwareschnittstelle. Die Verwendung des TPM ist die sicherste Art, BitLocker-Zugriffsschlüssel zu speichern, da das TPM eine Überprüfung der Systemintegrität vor dem Systemstart ermöglicht. Auf Computern ohne TPM können Sie Laufwerke verschlüsseln. Dabei wird der Zugriffsschlüssel mit einem Kennwort verschlüsselt. BitLocker verwendet die folgenden Authentifizierungsmethoden:

- TPM.
- TPM und PIN-Code.
- Kennwort.

Nachdem die Systemfestplatte verschlüsselt wurde, von der das Betriebssystem gestartet wird, muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach der Authentifizierung erlaubt BitLocker dem Benutzer die Anmeldung. Die Single-Sign-On-Technologie (SSO) wird von BitLocker nicht unterstützt.

Nach der Laufwerkverschlüsselung erstellt BitLocker einen Wiederherstellungsschlüssel. Kaspersky Endpoint Security sendet den Wiederherstellungsschlüssel an Kaspersky Security Center, damit Sie den Zugriff auf das Laufwerk wiederherstellen können (beispielsweise wenn ein Benutzer sein Kennwort vergessen hat).

Wenn ein Benutzer ein Laufwerk mithilfe von BitLocker verschlüsselt, sendet Kaspersky Endpoint Security den Wiederherstellungsschlüssel und Informationen über die Festplattenverschlüsselung an Kaspersky Security Center.

Wenn Sie Gruppenrichtlinien für Windows verwenden, deaktivieren Sie die BitLocker-Verwaltung in den Richtlinieneinstellungen. Es kann sein, dass die Windows-Richtlinieneinstellungen den Richtlinieneinstellungen von Kaspersky Endpoint Security widersprechen. Bei einer Laufwerksverschlüsselung könnten deshalb Fehler auftreten.

Start der „BitLocker-Laufwerkverschlüsselung"

Es wird empfohlen, vor dem Start der vollständigen Festplattenverschlüsselung sicherzustellen, dass der Computer nicht infiziert ist. Starten Sie dazu eine vollständige Untersuchung oder eine Untersuchung der wichtigen Computerbereiche. Die vollständige Festplattenverschlüsselung auf einem Computer, der von einem Rootkit infiziert ist, kann zur Funktionsuntüchtigkeit des Computers führen.

Damit BitLocker auf Computern mit einem Windows-Betriebssystem für Server ordnungsgemäß funktioniert, kann die Installation der Komponente „BitLocker-Laufwerkverschlüsselung" erforderlich sein. Installieren Sie die Komponente mithilfe der Betriebssystem-Tools (Assistent zum Hinzufügen von Rollen und Komponenten). Details über die Installation der Komponente „BitLocker-Laufwerkverschlüsselung" finden Sie in der Microsoft-Dokumentation.

So führen Sie die BitLocker-Laufwerkverschlüsselung über die Verwaltungskonsole (MMC) aus

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Option **BitLocker-Laufwerkverschlüsselung**.
5. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Alle Festplatten verschlüsseln**.

   Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem die Verschlüsselung ausgeführt wurde.

6. Passen Sie die erweiterten Einstellungen der „BitLocker-Laufwerkverschlüsselung" an (s. folgende Tabelle).
7. Speichern Sie die vorgenommenen Änderungen.

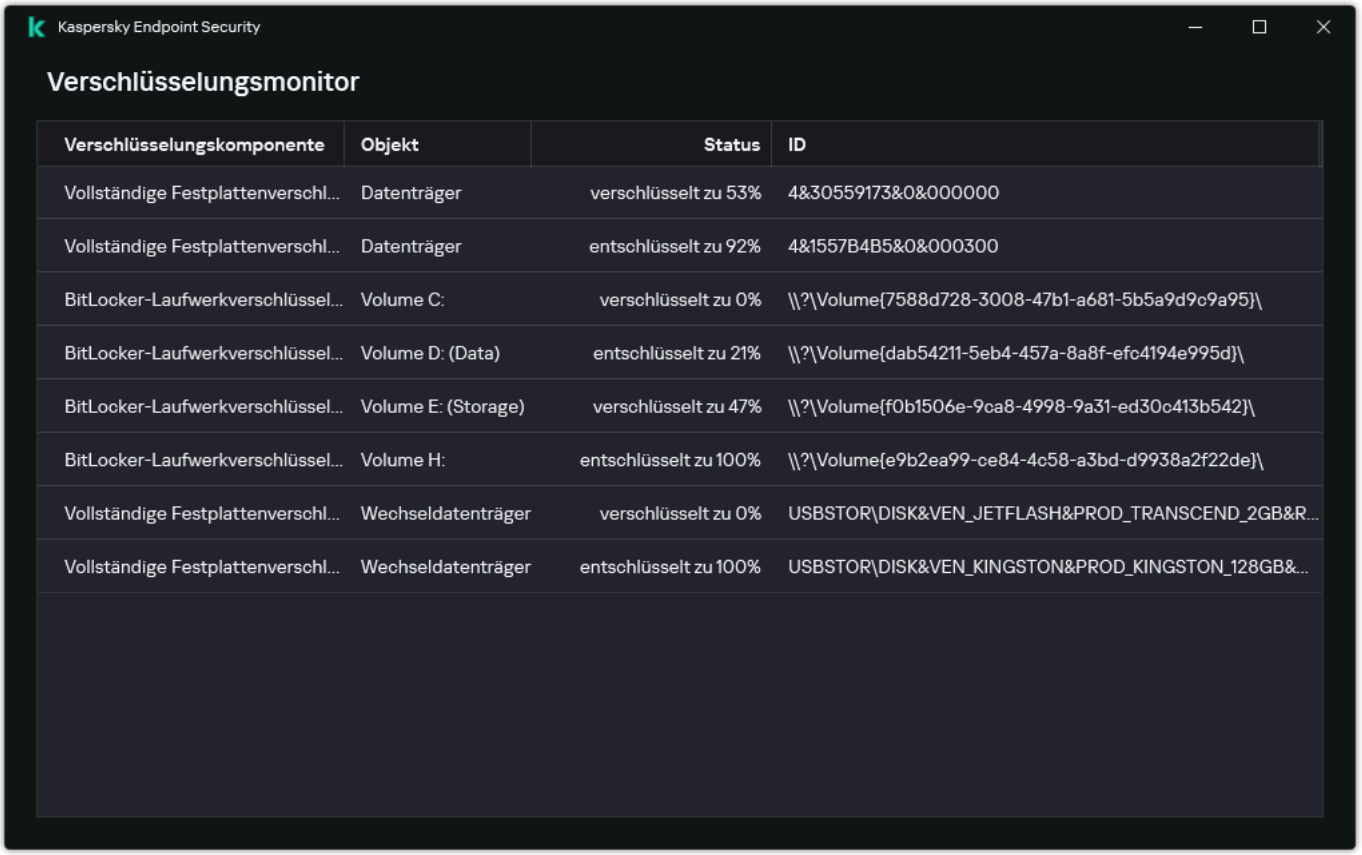
So führen Sie die BitLocker-Laufwerkverschlüsselung über die Web Console aus

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Datenverschlüsselung** → **Vollständige Festplattenverschlüsselung**.
5. Wählen Sie die Technologie **BitLocker-Festplattenverschlüsselung** aus.
6. Wählen Sie im Block **Aktion mit Geräten** die Variante **Alle Festplatten verschlüsseln** aus.

   Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem die Verschlüsselung ausgeführt wurde.

7. Passen Sie die erweiterten Einstellungen der „BitLocker-Laufwerkverschlüsselung“ an (s. folgende Tabelle).
8. Speichern Sie die vorgenommenen Änderungen.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool „Encryption Monitor“ kann über das Programmhauptfenster ausgeführt werden.



Verschlüsselungsmonitor

Nach der Anwendung der Richtlinie zeigt das Programm je nach Authentifizierungseinstellungen die folgenden Abfragen an:

- Nur TPM. Keine Benutzereingabe erforderlich. Der Datenträger wird bei Neustart des Computers verschlüsselt.
- TPM + PIN/Kennwort. Bei Vorhandensein des TPM-Moduls erscheint ein Abfragefenster für den PIN-Code. Wenn kein TPM-Modul vorhanden ist, erscheint ein Abfragefenster für das Kennwort für die Preboot-Authentifizierung.
- Nur Kennwort. Es erscheint ein Abfragefenster für das Kennwort für die Preboot-Authentifizierung.

Ist im Betriebssystem der FIPS-Kompatibilitätsmodus (Federal Information Processing Standard) aktiviert, so erscheint in den Betriebssystemen Windows 8 und in älteren Versionen ein Abfragefenster zur Verbindung eines Massenspeichergerätes für die Speicherung der Wiederherstellungsschlüsseldatei. Sie können auf einem Speichergerät mehrere Dateien mit Wiederherstellungsschlüsseln speichern.

Nachdem Sie ein Kennwort oder einen PIN-Code festgelegt haben, fordert BitLocker Sie auf, den Computer neu zu starten, um die Laufwerkverschlüsselung abzuschließen. Anschließend muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach erfolgreichem BitLocker-Authentifizierungsvorgang ist die Anmeldung am System erforderlich. Nach dem Start des Betriebssystems schließt BitLocker die Laufwerkverschlüsselung ab.

Besteht kein Zugriff auf die Chiffrierschlüssel, so kann der Benutzer beim Administrator des lokalen Unternehmensnetzwerks einen Wiederherstellungsschlüssel anfordern (falls zuvor kein Wiederherstellungsschlüssel auf dem Massenspeichergerät gespeichert wurde oder falls er verloren gegangen ist).

Einstellungen der Komponente „BitLocker-Laufwerkverschlüsselung"

Einstellung	Beschreibung
Verwendung der BitLocker-Authentifizierung aktivieren, die Preboot-Tastatureingaben auf Tablets erfordert	Verwendung einer Authentifizierung, die eine Dateneingabe in einer Preboot-Umgebung selbst dann erfordert, wenn die Plattform keine Option zur Preboot-Eingabe bietet (beispielsweise mit Touchscreen-Tastaturen auf Tablets). Das Touchpad von Tablets ist in der Preboot-Umgebung nicht verfügbar. Um die BitLocker-Authentifizierung auf Tablets auszuführen, muss der Benutzer beispielsweise eine USB-Tastatur anschließen. Ist das Kontrollkästchen aktiviert, so wird die Verwendung der Authentifizierung erlaubt, wenn sie eine Preboot-Tastatureingabe erfordert. Es wird empfohlen, diese Einstellung nur für Geräte zu verwenden, die in einer Preboot-Umgebung alternative Dateneingabemethoden anbieten (z. B. eine USB-Tastatur zusätzlich zu einer Touchscreen-Tastatur). Wenn das Kontrollkästchen deaktiviert ist, ist die BitLocker-Laufwerkverschlüsselung auf Tablets nicht möglich.
Hardwareverschlüsselung verwenden (Windows 8 und höher)	Ist das Kontrollkästchen aktiviert, so verwendet das Programm die Hardwareverschlüsselung. Dadurch wird erlaubt, die Verschlüsselung zu beschleunigen und die Auslastung der Computerressourcen zu reduzieren.

Einstellung	Beschreibung
Nur belegten Speicherplatz verschlüsseln (Windows 8 und höher)	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt. Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Das Kontrollkästchen ist standardmäßig deaktiviert.

Einstellung	Beschreibung
Authentifizierungsmethode	**Nur Kennwort (Windows 8 und höher)** Bei Auswahl dieser Variante fragt Kaspersky Endpoint Security beim Benutzer das Kennwort ab, wenn auf das verschlüsselte Laufwerk zugegriffen wird. Diese Variante für die Aktion kann gewählt werden, wenn das Trusted Platform Module (TPM) nicht verwendet wird. **Trusted Platform Module (TPM)** Bei Auswahl dieser Variante verwendet BitLocker das Trusted Platform Module (TPM). *Trusted Platform Module* (TMP) ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten. Für Computer mit den Betriebssystemen Windows 7 und Windows Server 2008 R2 ist nur die Verschlüsselung unter Verwendung eines TPM-Moduls verfügbar. Wenn kein TPM-Modul installiert ist, ist die BitLocker-Verschlüsselung nicht möglich. Die Verwendung eines Kennworts wird auf diesen Computern nicht unterstützt. Ein Gerät, das mit Trusted Platform Module ausgerüstet ist, kann Chiffrierschlüssel erstellen, die nur seiner Hilfe entschlüsselt werden können. Das Trusted Platform Module verschlüsselt Chiffrierschlüssel mit einem eigenen Storage Root Key. Der Storage Root Key wird im Trusted Platform Module aufbewahrt. Dadurch wird für die Chiffrierschlüssel ein zusätzlicher Schutz vor Angriffsversuchen gewährleistet. Diese Aktion ist standardmäßig ausgewählt. Sie können eine zusätzliche Schutzebene für den Zugriff auf den Chiffrierschlüssel einrichten und den Schlüssel mit einem Kennwort oder einer PIN verschlüsseln: • **PIN für TPM verwenden**. Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer einen PIN-Code verwenden, um auf einen Chiffrierschlüssel zuzugreifen, der im Trusted Platform Module (TPM) aufbewahrt wird. Wenn das Kontrollkästchen deaktiviert ist, ist es dem Benutzer verboten, einen PIN-Code zu verwenden. Um Zugriff auf den Chiffrierschlüssel zu erhalten, verwendet der Benutzer ein Kennwort. • **Trusted Platform Module (TPM) oder Kennwort, falls TPM nicht verfügbar ist**. Wenn diese Option ausgewählt ist, kann der Benutzer mithilfe eines Kennworts Zugriff auf die Chiffrierschlüssel erhalten, falls kein Trusted Platform Module (TPM) verfügbar ist. Wenn das Kontrollkästchen deaktiviert ist und das TPM-Modus nicht verfügbar ist, wird die vollständige Festplattenverschlüsselung nicht gestartet. Die ausgewählte Authentifizierungsmethode muss durch Angabe von Kennwort- oder PIN-Anforderungen konfiguriert werden: • **Mindestlänge der PIN (Zeichen)** (der Standardwert ist 6). • **Mindestlänge des Kennworts (Zeichen)** (der Standardwert ist 8). • **Maximale Anzahl gespeicherter Passwörter/PINs** (der Standardwert ist 5). • **Kennwort/PIN-Gültigkeitsdauer für TPM beschränken (Tage)** (standardmäßig deaktiviert). • **Erweiterte PIN verwenden (Buchstaben und Ziffern)**. Eine *erweiterte PIN* ermöglicht neben der Verwendung numerischer Zeichen auch lateinische Groß- und Kleinbuchstaben, Sonderzeichen und Leerzeichen. Standardmäßig deaktiviert.
Wiederherstellungsschlüssel automatisch neu erstellen (Tage)	Kennwort automatisch aktualisieren, um den Zugriffauf ein BitLocker-geschütztes Laufwerk wiederherzustellen. Wenn das Kontrollkästchen aktiviert ist, geben Sie die Gültigkeitsdauer des Kennworts für den Wiederherstellungsschlüssel an. Dadurch lässt sich eine Wiederverwendung des Kennworts für den Wiederherstellungsschlüssel verhindern.

Entschlüsselung einer Festplatte, die mit BitLocker geschützt ist

Der Benutzer kann das Laufwerk selbstständig mithilfe von Betriebssystem-Tools entschlüsseln (Funktion *BitLocker deaktivieren*). Anschließend schlägt Kaspersky Endpoint Security vor, das Laufwerk erneut zu verschlüsseln. Kaspersky Endpoint Security schlägt so lange vor, das Laufwerk zu verschlüsseln, bis Sie die Entschlüsselung von Laufwerken in der Richtlinie aktivieren.

So entschlüsseln Sie eine durch BitLocker geschützte Festplatte über die Verwaltungskonsole (MMC)

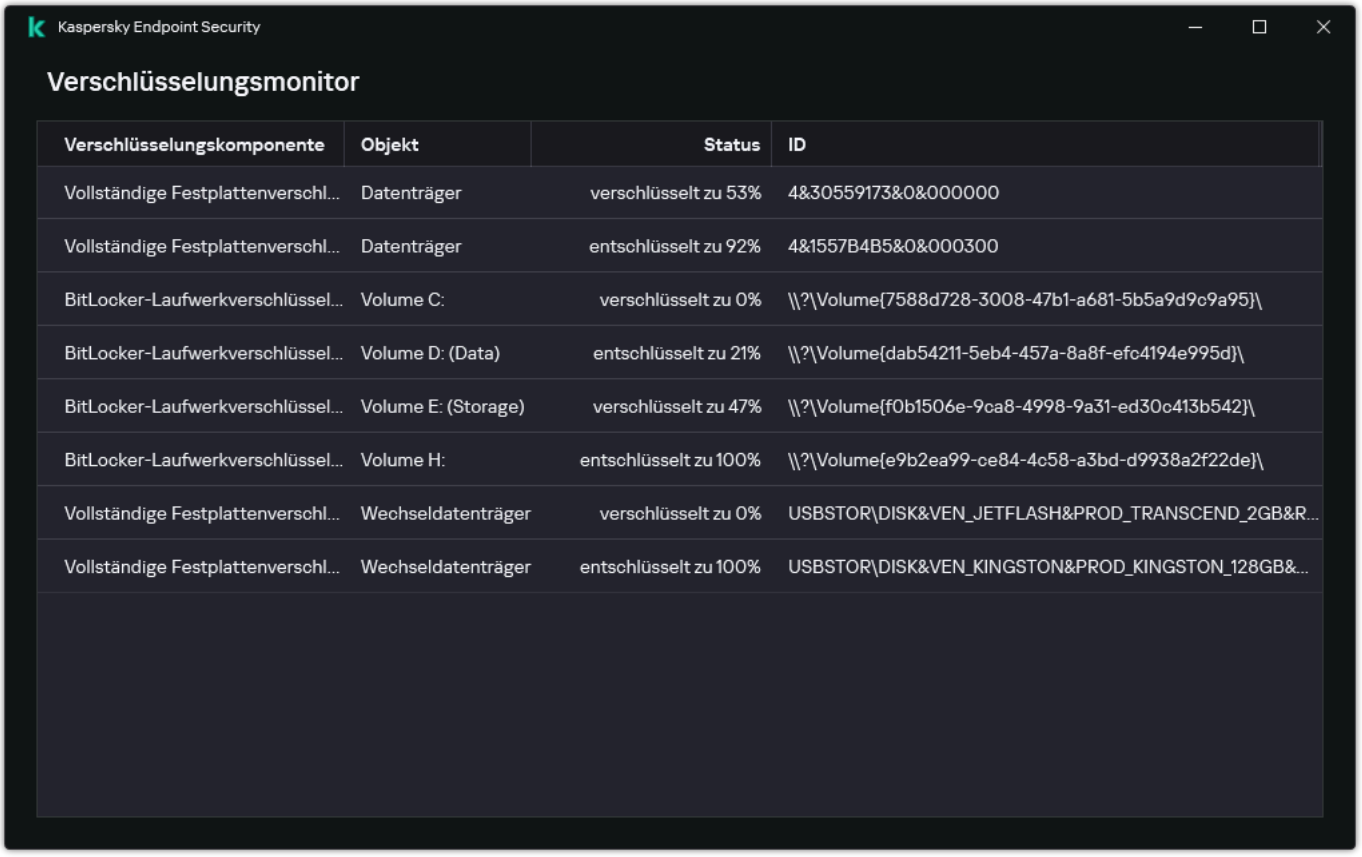
1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Vollständige Festplattenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungstechnologie** die Option **BitLocker-Laufwerkverschlüsselung**.
5. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Alle Festplatten entschlüsseln**.
6. Speichern Sie die vorgenommenen Änderungen.

So entschlüsseln Sie eine mit BitLocker verschlüsselte Festplatte über die Web Console und die Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Datenverschlüsselung → Vollständige Festplattenverschlüsselung**.
5. Wählen Sie die Technologie **BitLocker-Festplattenverschlüsselung** aus.
6. Wählen Sie im Block **Aktion mit Geräten** die Variante **Alle Festplatten entschlüsseln** aus.
7. Speichern Sie die vorgenommenen Änderungen.

Mit dem Tool „Encryption Monitor“ können Sie den Vorgang der Festplattenverschlüsselung und -entschlüsselung auf dem Computer eines Benutzers steuern. Das Tool „Encryption Monitor“ kann über das Programmhauptfenster ausgeführt werden.



Verschlüsselungsmonitor

Wiederherstellen des Zugriffs auf einen Datenträger, der mit BitLocker geschützt ist

Wenn der Benutzer das Kennwort für den Zugriff auf eine Festplatte vergessen hat, die mit BitLocker verschlüsselt ist, muss ein Wiederherstellungsvorgang („Anfrage-Frage“) ausgeführt werden.

Für die Betriebssysteme Windows 8 und für ältere Versionen gilt: Wenn im Betriebssystem der Kompatibilitätsmodus für den Federal Information Processing Standard (FIPS) aktiviert ist, wurde die Wiederherstellungsschlüssel-Datei vor der Verschlüsselung auf dem Wechseldatenträger gespeichert. Um den Zugriff auf den Datenträger wiederherzustellen, verbinden Sie den Datenträger und folgen Sie den Anweisungen auf dem Bildschirm.

Um den Zugriff auf eine Festplatte wiederherzustellen, die mit BitLocker verschlüsselt ist, sind die folgenden Schritte erforderlich:

1. Der Benutzer übermittelt die Wiederherstellungsschlüssel-ID an den Administrator (s. Abb. unten).
2. Der Administrator überprüft die Wiederherstellungsschlüssel-ID in den Computereigenschaften in Kaspersky Security Center. Die ID, die der Benutzer übermittelt hat, muss identisch sein mit der ID, die in den Computereigenschaften angezeigt wird.

3. Wenn die IDs der Wiederherstellungsschlüssel übereinstimmen, teilt der Administrator dem Benutzer den Wiederherstellungsschlüssel mit oder übermittelt eine Wiederherstellungsschlüssel-Datei.

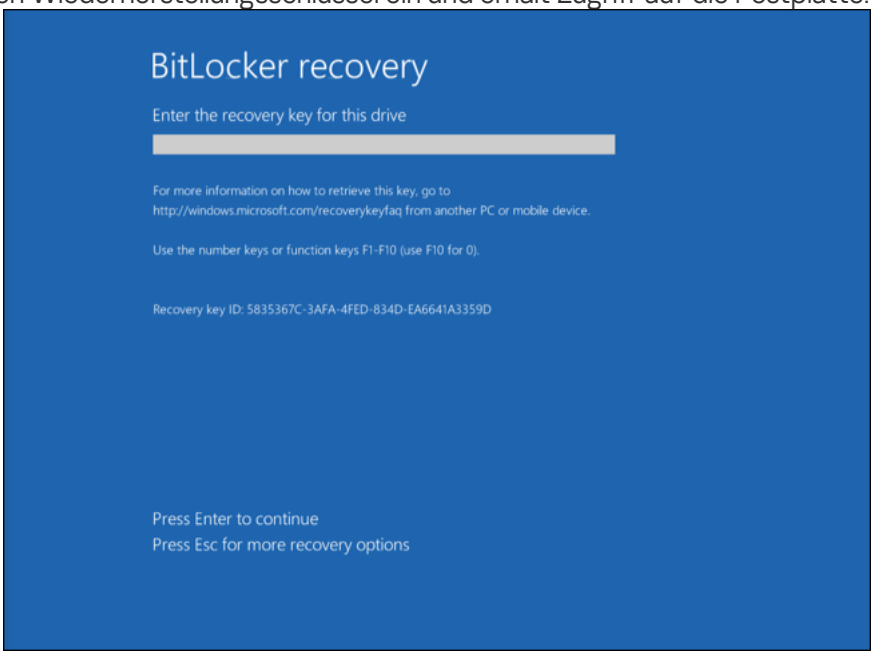
   Eine Wiederherstellungsschlüssel-Datei wird für Computer mit folgenden Betriebssystemen verwendet:

   - Windows 7
   - Windows 8
   - Windows Server 2008
   - Windows Server 2011
   - Windows Server 2012

   Für die übrigen Betriebssysteme wird ein Wiederherstellungsschlüssel benutzt.

   Um zu verhindern, dass das Kennwort für den Wiederherstellungsschlüssel erneut verwendet wird, können Sie in den Richtlinieneinstellungen die automatische Kennwort-Aktualisierung konfigurieren.

4. Der Benutzer gibt den Wiederherstellungsschlüssel ein und erhält Zugriff auf die Festplatte.



Wiederherstellen des Zugriffs auf eine Festplatte, die mit BitLocker verschlüsselt ist

Wiederherstellen des Zugriffs auf ein Systemlaufwerk

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer während der Preboot-Authentifizierung die Taste **Esc** drücken.

In der Verwaltungskonsole (MMC) den Wiederherstellungsschlüssel für ein Systemlaufwerk anzeigen, das mit BitLocker verschlüsselt ist

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte** aus.

3. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der den Zugriff auf verschlüsselte Daten wiederherstellen möchte, und öffnen Sie mit der rechten Maustaste das Kontextmenü.

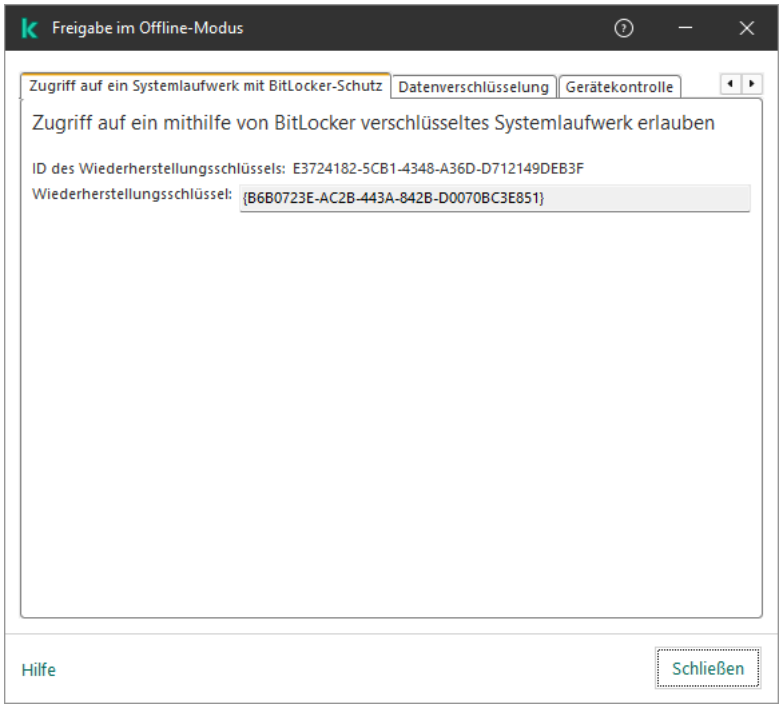
4. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus**.

5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Zugriff auf ein Systemlaufwerk mit BitLocker-Schutz**-Registerkarte aus.

6. Fordern Sie beim Benutzer die ID des Wiederherstellungsschlüssels an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels**.

   Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

Sie erhalten dann einen Wiederherstellungsschlüssel oder eine Wiederherstellungsschlüssel-Datei. Übermitteln Sie den Schlüssel oder die Datei an den Benutzer.



Zugriffswiederherstellung für ein mithilfe von BitLocker verschlüsseltes Laufwerk

So zeigen Sie in der Web Console und der Cloud Console den Wiederherstellungsschlüssel für ein Systemlaufwerk an, das mit BitLocker verschlüsselt ist

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Laufwerkszugriff wiederherstellen möchten.

3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.

4. Wählen Sie im folgenden Fenster den Abschnitt **BitLocker**.

5. Überprüfen Sie die ID des Wiederherstellungsschlüssels. Die ID, die der Benutzer übermittelt hat, muss identisch sein mit der ID, die in den Computereinstellungen angezeigt wird.

   Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

6. Klicken Sie auf **Schlüssel anfordern**.

   Sie erhalten dann einen Wiederherstellungsschlüssel oder eine Wiederherstellungsschlüssel-Datei. Übermitteln Sie den Schlüssel oder die Datei an den Benutzer.

Nachdem das Betriebssystem geladen ist, fordert Kaspersky Endpoint Security den Benutzer auf, das Kennwort oder den PIN-Code zu ändern. Nachdem Sie ein neues Kennwort oder einen neuen PIN-Code festgelegt haben, erstellt BitLocker einen neuen Wiederherstellungsschlüssel und sendet den Schlüssel an Kaspersky Security Center. Infolgedessen werden der Wiederherstellungsschlüssel und die Wiederherstellungsschlüsseldatei aktualisiert. Wenn der Benutzer das Kennwort nicht geändert hat, können Sie beim nächsten Start des Betriebssystems den alten Wiederherstellungsschlüssel verwenden.

Auf Computern mit Windows 7 kann das Kennwort oder der PIN-Code nicht geändert werden. Nachdem der Wiederherstellungsschlüssel eingegeben wurde und das Betriebssystem geladen ist, fordert Kaspersky Endpoint Security den Benutzer nicht auf, das Kennwort oder den PIN-Code zu ändern. Daher ist es nicht möglich, ein neues Passwort oder einen neuen PIN-Code festzulegen. Dieses Problem beruht auf Besonderheiten des Betriebssystems. Um fortzufahren, müssen Sie die Festplatte neu verschlüsseln.

Wiederherstellen des Zugriffs auf ein Nicht-Systemlaufwerk

Um den Wiederherstellungsvorgang zu starten, muss der Benutzer im Zugriffserteilungsfenster für den Datenträger auf den Link **Kennwort vergessen** klicken. Nachdem der Zugriff auf den verschlüsselten Datenträger gewährt wurde, kann der Benutzer in den BitLocker-Einstellungen festlegen, dass der Datenträger bei der Windows-Authentifizierung automatisch entsperrt wird.

In der Verwaltungskonsole (MMC) den Wiederherstellungsschlüssel für ein Nicht-Systemlaufwerk anzeigen, das mit BitLocker verschlüsselt ist

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

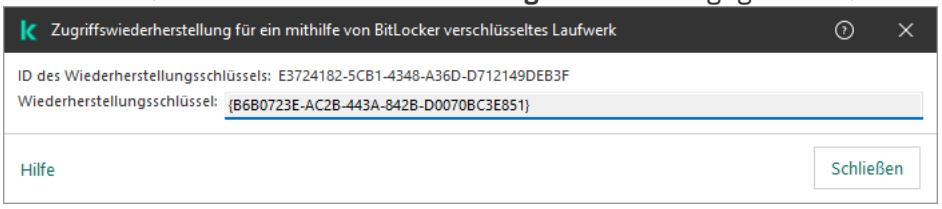
2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Laufwerke** aus.

3. Wählen Sie im Arbeitsbereich das verschlüsselte Gerät aus, für das Sie eine Zugriffsschlüsseldatei erstellen möchten, und wählen Sie dann im Kontextmenü des Gerätes den Punkt **Zugriff auf das Gerät anfordern bei Kaspersky Endpoint Security**.

4. Fordern Sie beim Benutzer die ID des Wiederherstellungsschlüssels an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels**.

   Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf den angegebenen Datenträger wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

5. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.



Zugriffswiederherstellung für ein mithilfe von BitLocker verschlüsseltes Laufwerk

So zeigen Sie in der Web Console und der Cloud Console den Wiederherstellungsschlüssel für ein Nicht-Systemlaufwerk an, das mit BitLocker verschlüsselt ist

1. Klicken Sie im Web Console-Hauptfenster auf **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Laufwerke**.

2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Laufwerkszugriff wiederherstellen möchten.

3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.

   Der Assistent für die Zugriffserteilung auf das Gerät wird gestartet.

4. Folgen Sie den Anweisungen des Assistenten für die Zugriffserteilung auf das Gerät:

   a. Wählen Sie das Plug-in **Kaspersky Endpoint Security für Windows** aus

   b. Überprüfen Sie die ID des Wiederherstellungsschlüssels. Die ID, die der Benutzer übermittelt hat, muss identisch sein mit der ID, die in den Computereinstellungen angezeigt wird.

   > Sind die IDs nicht identisch, so eignet sich dieser Schlüssel nicht, um den Zugriff auf das angegebene Systemlaufwerk wiederherzustellen. Vergewissern Sie sich, ob der Name des gewählten Computers mit dem Namen des Benutzercomputers übereinstimmt.

   c. Klicken Sie auf **Schlüssel anfordern**.

Sie erhalten dann einen Wiederherstellungsschlüssel oder eine Wiederherstellungsschlüssel-Datei. Übermitteln Sie den Schlüssel oder die Datei an den Benutzer.

Anhalten des BitLocker-Schutzes für ein Software-Update

Wenn der BitLocker-Schutz aktiviert ist, sind in den folgenden Fällen einige Besonderheiten zu beachten: beim Aktualisieren des Betriebssystems, beim Installieren von Update-Paketen für das Betriebssystem und beim Aktualisieren anderer Software. Bei der Installation von Updates muss der Computer möglicherweise mehrmals neu gestartet werden. Der Benutzer muss nach jedem Neustart die BitLocker-Authentifizierung durchlaufen. Um sicherzustellen, dass Updates korrekt installiert werden, können Sie die BitLocker-Authentifizierung vorübergehend deaktivieren. In diesem Fall bleibt die Festplatte verschlüsselt und der Benutzer hat nach der Anmeldung am System Zugriff auf die Daten. Die BitLocker-Authentifizierung können Sie mit der Aufgabe *Verwaltung des BitLocker-Schutzes* verwalten. Mit dieser Aufgabe können Sie die Anzahl der Computerneustarts festlegen, für die keine BitLocker-Authentifizierung erforderlich ist. Nachdem die Updates installiert wurden und die Aufgabe *Verwaltung des BitLocker-Schutzes* abgeschlossen wurde, wird die BitLocker-Authentifizierung automatisch aktiviert. Sie können die BitLocker-Authentifizierung jederzeit aktivieren.

So halten Sie den BitLocker-Schutz mithilfe der Verwaltungskonsole (MMC) an

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Verwaltung des BitLocker-Schutzes** aus.

Schritt 2. Verwaltung des BitLocker-Schutzes

Passen Sie die BitLocker-Authentifizierung an. Um den BitLocker-Schutz anzuhalten, wählen Sie **Überspringen der BitLocker-Authentifizierung vorübergehend zulassen** und geben Sie die Anzahl der Neustarts ohne BitLocker-Authentifizierung an (1 bis 15). Geben Sie bei Bedarf an, wann die Aufgabe ablaufen soll (Datum und Uhrzeit). Zum angegebenen Zeitpunkt wird die Aufgabe automatisch deaktiviert, und der Benutzer muss die BitLocker-Authentifizierung durchlaufen, wenn der Computer neu gestartet wird.

Schritt 3. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 4. Aufgabennamen festlegen

Geben Sie den Namen der Aufgabe ein, z. B. *Auf Windows 10 aktualisieren*.

Schritt 5. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

So halten Sie den BitLocker-Schutz mithilfe der „Web Console“ an

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Grundlegende Aufgabeneinstellungen anpassen

Passen Sie die allgemeinen Einstellungen der Aufgabe an:

1. Wählen Sie in der Dropdown-Liste **Anwendung** den Punkt **Kaspersky Endpoint Security für Windows** aus.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Verwaltung des BitLocker-Schutzes**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Auf Windows 10 aktualisieren*.
4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

Schritt 2. Verwaltung des BitLocker-Schutzes

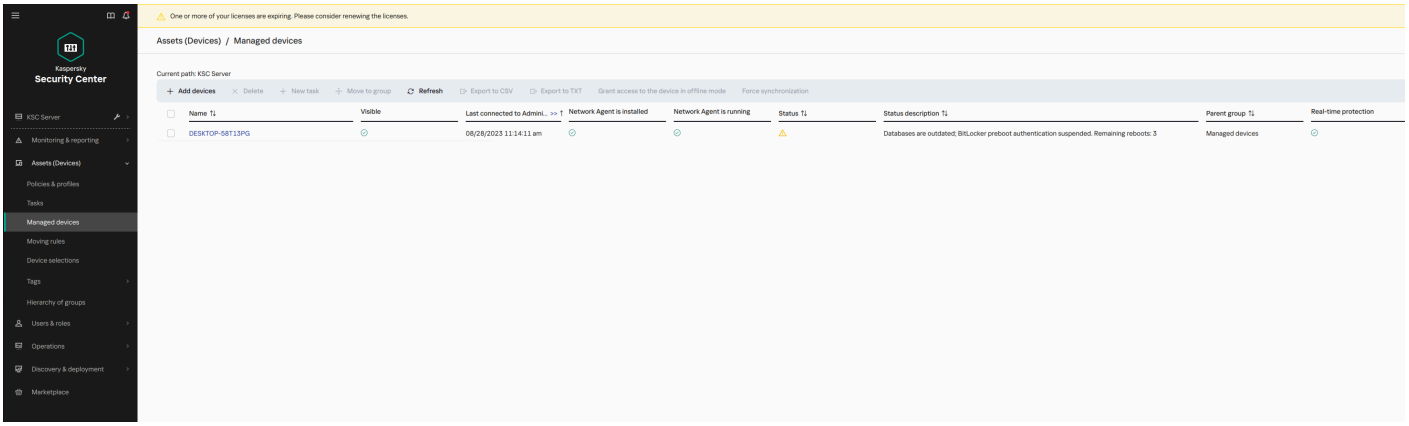
Passen Sie die BitLocker-Authentifizierung an. Um den BitLocker-Schutz anzuhalten, wählen Sie **Überspringen der BitLocker-Authentifizierung vorübergehend zulassen** und geben Sie die Anzahl der Neustarts ohne BitLocker-Authentifizierung an (1 bis 15). Geben Sie bei Bedarf an, wann die Aufgabe ablaufen soll (Datum und Uhrzeit). Zum angegebenen Zeitpunkt wird die Aufgabe automatisch deaktiviert, und der Benutzer muss die BitLocker-Authentifizierung durchlaufen, wenn der Computer neu gestartet wird.

Schritt 3. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Die neue Aufgabe wird in der Aufgabenliste angezeigt.

Aktivieren Sie das Kontrollkästchen neben der Aufgabe und klicken Sie auf **Starten**, um die Aufgabe auszuführen.

Wenn die Aufgabe ausgeführt wird, fordert BitLocker den Benutzer nach dem nächsten Neustart des Computers nicht zur Authentifizierung auf. Kaspersky Endpoint Security generiert nach jedem Neustart des Computers ohne BitLocker-Authentifizierung ein entsprechendes Ereignis und merkt sich die Anzahl der verbleibenden Neustarts. Dann sendet Kaspersky Endpoint Security das Ereignis an Kaspersky Security Center, damit der Administrator den Vorgang verfolgen kann. Die Anzahl der verbleibenden Neustarts können Sie auch im Ordner **Verwaltete Geräte** der Kaspersky Security Center-Konsole in der Beschreibung des Gerätestatus nachsehen.



Die Liste der verwalteten Geräte

Sobald die festgelegte Anzahl von Neustarts erreicht ist oder die Aufgabe abläuft, wird die BitLocker-Authentifizierung automatisch aktiviert. Um Zugriff auf Daten zu erhalten, muss der Benutzer die BitLocker-Authentifizierung durchlaufen.

Auf Computern mit dem Betriebssystem Windows 7 kann BitLocker die Anzahl der Computerneustarts nicht zählen. Darum werden die Neustarts auf Windows 7-Computern von Kaspersky Endpoint Security gezählt. Um die BitLocker-Authentifizierung nach jedem Neustart automatisch zu aktivieren, muss deshalb Kaspersky Endpoint Security gestartet werden.

Um die BitLocker-Authentifizierung vorzeitig zu aktivieren, öffnen Sie die Eigenschaften der Aufgabe *Verwaltung des BitLocker-Schutzes* und aktivieren Sie **Authentifizierung jedes Mal vor dem Start anfragen**.

Dateiverschlüsselung auf lokalen Festplatten des Computers

Die Dateiverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Für die Verschlüsselung von Dateien gelten die folgenden Besonderheiten:

- Kaspersky Endpoint Security verschlüsselt/entschlüsselt die Standardordner nur für die lokalen Benutzerprofile (local user profiles) des Betriebssystems. Kaspersky Endpoint Security verschlüsselt und entschlüsselt die Standardordner nicht für Roaming-Benutzerprofile (roaming user profiles), verbindliche Benutzerprofile (mandatory user profiles), temporäre Benutzerprofile (temporary user profiles) und Ordnerumleitung.

- Für Dateien, deren Veränderung die Funktionsfähigkeit des Betriebssystems und der installierten Programme beeinträchtigen kann, führt Kaspersky Endpoint Security keine Verschlüsselung durch. Zur Liste der Verschlüsselungsausnahmen gehören beispielsweise folgende Dateien und Ordner mit allen untergeordneten Ordnern:

  - %WINDIR%

  - %PROGRAMFILES% und %PROGRAMFILES(X86)%

  - Dateien der Systemregistrierung von Windows

  Die Liste mit Ausnahmen von der Verschlüsselung kann nicht angezeigt oder geändert werden. Dateien und Ordner aus der Liste mit den Verschlüsselungsausnahmen können zur Verschlüsselungsliste hinzugefügt werden; sie werden jedoch bei der Ausführung der Dateiverschlüsselung nicht verschlüsselt.

Dateiverschlüsselung auf lokalen Festplatten des Computers starten

Dateien, die sich im OneDrive-Cloud-Speicher oder in anderen Ordnern mit dem Namen OneDrive befinden, werden von Kaspersky Endpoint Security nicht verschlüsselt. Außerdem blockiert Kaspersky Endpoint Security das Kopieren verschlüsselter Dateien in OneDrive-Ordner, wenn diese Dateien nicht zu einer Entschlüsselungsregel hinzugefügt wurden.

Gehen Sie wie folgt vor, um Dateien auf lokalen Festplatten des Computers zu verschlüsseln:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Verschlüsselung auf Dateiebene** aus.

4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Gemäß den Regeln**.

5. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente:

   a. Wählen Sie das Element **Standardordner**, um die von Kaspersky empfohlenen Dateien aus den Ordnern der lokalen Benutzerprofile zur Verschlüsselungsregel hinzuzufügen.

      - **Dokumente**. Dateien im Standardordner *Dokumente* des Betriebssystems, sowie untergeordnete Ordner.

      - **Favoriten**. Dateien im Standardordner *Favoriten* des Betriebssystems, sowie untergeordnete Ordner.

      - **Desktop**. Dateien im Standardordner *Desktop* des Betriebssystems, sowie untergeordnete Ordner.

- **Temporäre Dateien**. Temporäre Dateien, die mit der Verwendung Programmen zusammenhängen, die auf dem Computer installiert sind. Beispiel: Das Programm Microsoft Office erstellt temporäre Dateien mit Backup-Kopien von Dokumenten.

  Es wird nicht empfohlen, temporäre Dateien zu verschlüsseln, da dies zu Datenverlust führen kann. Beispielsweise erstellt Microsoft Word beim Verarbeiten eines Dokuments temporäre Dateien. Wenn temporäre Dateien verschlüsselt sind, die Originaldatei jedoch nicht, erhält der Benutzer möglicherweise den Fehler *Zugriff abgelehnt* beim Versuch, das Dokument zu speichern. Außerdem kann es vorkommen, dass Microsoft Word die Datei speichert, aber das Dokument beim nächsten Mal nicht mehr geöffnet werden kann, d.h. die Daten gehen verloren.

- **Outlook-Dateien**. Dateien, die mit der Nutzung des Mail-Clients Outlook zusammenhängen: Datendateien (PST), Offlinedatendateien (OST), Offlineadressbuch-Dateien (OAB) und Dateien für Persönliches Adressbuch (PAB).

b. Wählen Sie das Element **Manuell festgelegter Ordner**, um einen Ordner, dessen Pfad manuell angegeben wird, zur Verschlüsselungsregel hinzuzufügen.

Beachten Sie folgende Regeln, wenn Sie einen Ordnerpfad hinzufügen:

- Verwenden Sie eine Umgebungsvariable (z. B. `%FOLDER%\UserFolder\`). Eine Umgebungsvariable kann nur ein Mal und nur am Anfang des Pfads verwendet werden.
- Verwenden Sie keine relativen Pfade.
- Verwenden Sie nicht die Zeichen `*` und `?`.
- Verwenden Sie keine UNC-Pfade.
- Verwenden Sie `;` oder `,` als Trennzeichen.

c. Wählen Sie das Element **Dateien nach Erweiterung** aus, um bestimmte Dateierweiterungen zu der Verschlüsselungsregel hinzuzufügen. Kaspersky Endpoint Security verschlüsselt die Dateien mit den angegebenen Erweiterungen auf allen lokalen Festplatten des Computers.

d. Wählen Sie das Element **Dateien nach Erweiterungsgruppen** aus, um Gruppen für Dateierweiterungen (z. B. die Gruppe *Microsoft-Office-Dokumente*) zu der Verschlüsselungsregel hinzuzufügen. Kaspersky Endpoint Security verschlüsselt die Dateien mit den Erweiterungen, die in den Erweiterungsgruppen aufgezählt sind, auf allen lokalen Festplatten des Computers.

6. Speichern Sie die vorgenommenen Änderungen.

Sofort nachdem die Richtlinie übernommen wurde, verschlüsselt Kaspersky Endpoint Security jene Dateien, die in der Verschlüsselungsregel angegeben sind und nicht in der Entschlüsselungsregel angegeben sind.

Für die Verschlüsselung von Dateien gelten die folgenden Besonderheiten:

- Wenn dieselbe Datei sowohl zu einer Verschlüsselungsregel als auch zu einer Entschlüsselungsregel hinzugefügt wurde, verfährt Kaspersky Endpoint Security wie folgt:
  - Wenn die Quelldatei nicht verschlüsselt ist, verschlüsselt Kaspersky Endpoint Security diese Datei nicht.
  - Wenn die Quelldatei verschlüsselt ist, entschlüsselt Kaspersky Endpoint Security diese Datei.

- Kaspersky Endpoint Security verschlüsselt weiterhin neue Dateien, wenn die Dateien die Kriterien der Verschlüsselungsregel erfüllen. Sie haben beispielsweise die Eigenschaften einer nicht verschlüsselten Datei (Pfad oder Erweiterung) geändert und die Datei erfüllt nun die Kriterien der Verschlüsselungsregel. Kaspersky Endpoint Security verschlüsselt diese Datei.
- Erstellt der Benutzer eine neue Datei, deren Eigenschaften die Kriterien der Verschlüsselungsregel erfüllen, so verschlüsselt Kaspersky Endpoint Security die Datei sofort, wenn die Datei geöffnet wird.
- Kaspersky Endpoint Security wartet mit der Verschlüsselung geöffneter Dateien, bis sie geschlossen werden.
- Wenn Sie eine verschlüsselte Datei in einen anderen Ordner des lokalen Laufwerks verschieben, bleibt die Datei verschlüsselt, unabhängig davon, ob dieser Ordner zur Verschlüsselungsregel gehört.
- Wenn Sie eine Datei entschlüsselt und die Datei in einen anderen Ordner auf einem lokalen Laufwerk kopiert haben, das nicht zur Entschlüsselungsregel gehört, so kann die Dateikopie verschlüsselt werden. Um die Verschlüsselung der Dateikopie zu verhindern, erstellen Sie für den Zielordner eine Entschlüsselungsregel.

Programmzugriffsrechte für verschlüsselte Dateien formulieren

Verschlüsselten Dateien werden von allen Programmen standardmäßig entschlüsselt, wenn damit gearbeitet wird. Wenn Sie bestimmte Programme häufig verwenden (z. B. Browser oder Text-Editoren), können Sie Zugriffsregeln für verschlüsselte Dateien erstellen. Dies verbessert den Schutz der Informationen.

Wir empfehlen, eine Zugriffsregel für verschlüsselte Dateien für die Browser Microsoft Internet Explorer und Microsoft Edge zu erstellen. Aufgrund der Funktionsweise dieser Browser wird eine verschlüsselte Datei automatisch entschlüsselt, wenn Sie diese auf eine Website hochladen (z. B. in einen Cloud-Speicher). Dies kann zu einem Datenleck führen. Verschlüsselte Dateien können mit diesen Browsern nicht hochgeladen werden. Wir empfehlen, die Regel **Zugriff auf verschlüsselte Dateien nur in Form von Ciphertext erlauben** einzurichten. Für andere Browser (z. B. Google Chrome) muss keine Regel erstellt werden.

Gehen Sie wie folgt vor, um Programmzugriffsrechte für verschlüsselte Dateien zu formulieren:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Verschlüsselung auf Dateiebene** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Gemäß den Regeln**.

   Zugriffsregeln gelten nur im Modus **Gemäß den Regeln**. Wenn Sie im Modus **Gemäß den Regeln** Zugriffsregeln übernommen haben und dann in den Modus **Nicht verändern** wechseln, ignoriert Kaspersky Endpoint Security alle Zugriffsregeln. Alle Programme besitzen Zugriff auf alle verschlüsselten Dateien.

5. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Regeln für Programme**.

6. Wenn Sie ausschließlich Programme aus der Liste von Kaspersky Security Center wählen möchten, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme aus der Kaspersky Security Center Liste**.

   a. Geben Sie Filter für die Anzeige der Programmliste in der Tabelle an. Geben Sie dazu die Werte für die Einstellungen **Programm**, **Hersteller** und **Hinzugefügt** sowie für alle Kontrollkästchen im Block **Gruppe** an.

   b. Klicken Sie auf **Aktualisieren**.

   c. In der Tabelle wird eine Programmliste angezeigt, die den angegebenen Filtern entspricht.

   d. Aktivieren Sie in der Spalte **Programm** die Kontrollkästchen der Programme, für die Sie Zugriffsregeln für verschlüsselte Dateien erstellen möchten.

   e. Wählen Sie in der Dropdown-Liste **Regel für Programme** eine Regel, die den Zugriff von Programmen auf verschlüsselte Dateien festlegt.

   f. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Programme** die Aktion, welche Kaspersky Endpoint Security mit den Zugriffsregeln für verschlüsselte Dateien ausführen soll, die bereits für die oben angegebenen Programme vorhanden sind.

   Details zu einer Programmzugriffsregel für verschlüsselte Dateien werden in der Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

7. Um ein Programm manuell zu wählen, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme manuell**.

   a. Geben Sie im Eingabefeld einen Namen oder eine Liste mit Namen von ausführbaren Programmdateien und deren Erweiterungen ein.

   Sie können die Namen von ausführbaren Programmdateien auch aus der Liste für Kaspersky Security Center hinzufügen. Klicken Sie dazu auf **Aus der Liste für Kaspersky Security Center hinzufügen**.

   b. Geben Sie erforderlichenfalls im Feld **Beschreibung** eine Beschreibung der Programmliste ein.

   c. Wählen Sie in der Dropdown-Liste **Regel für Programme** eine Regel, die den Zugriff von Programmen auf verschlüsselte Dateien festlegt.

   Details zu einer Programmzugriffsregel für verschlüsselte Dateien werden in der Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

8. Speichern Sie die vorgenommenen Änderungen.

Verschlüsselung von Dateien, die von bestimmten Programmen erstellt und geändert werden

Sie können eine Regel erstellen, nach der Kaspersky Endpoint Security alle Dateien verschlüsseln soll, welche von in der Regel angegebenen Programmen erstellt oder geändert werden.

Dateien, die von den angegebenen Programmen erstellt oder geändert worden sind, bevor die Verschlüsselungsregel übernommen wurde, werden nicht verschlüsselt.

Um die Verschlüsselung von Dateien anzupassen, die von bestimmten Programmen erstellt und geändert werden, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Verschlüsselung auf Dateiebene** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Gemäß den Regeln**.

   Verschlüsselungsregeln gelten nur im Modus **Gemäß den Regeln**. Wenn Sie im Modus **Gemäß den Regeln** Verschlüsselungsregeln übernommen haben und dann in den Modus **Nicht verändern** wechseln, ignoriert Kaspersky Endpoint Security alle Verschlüsselungsregeln. Dateien, die zuvor verschlüsselt worden sind, bleiben weiterhin verschlüsselt.

5. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Regeln für Programme**.
6. Wenn Sie ausschließlich Programme aus der Liste von Kaspersky Security Center wählen möchten, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme aus der Kaspersky Security Center Liste**.

   a. Geben Sie Filter für die Anzeige der Programmliste in der Tabelle an. Geben Sie dazu die Werte für die Einstellungen **Programm**, **Hersteller** und **Hinzugefügt** sowie für alle Kontrollkästchen im Block **Gruppe** an.

   b. Klicken Sie auf **Aktualisieren**.

      In der Tabelle wird eine Programmliste angezeigt, die den angegebenen Filtern entspricht.

   c. Aktivieren Sie in der Spalte **Programm** die Kontrollkästchen jener Programme, deren erstellte Dateien Sie verschlüsseln möchten.

   d. Wählen Sie in der Dropdown-Liste **Regel für Programme** die Option **Alle neu erstellten Dateien verschlüsseln**.

   e. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Programme** die Aktion, welche Kaspersky Endpoint Security mit den Verschlüsselungsregeln für Dateien ausführen soll, die bereits für die oben angegebenen Programme erstellt worden sind.

   Informationen über die Verschlüsselungsregel für Dateien, die von den ausgewählten Anwendungen erstellt oder geändert wurden, werden in der Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

7. Um ein Programm manuell zu wählen, klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste das Element **Programme manuell**.

   a. Geben Sie im Eingabefeld einen Namen oder eine Liste mit Namen von ausführbaren Programmdateien und deren Erweiterungen ein.

      Sie können die Namen von ausführbaren Programmdateien auch aus der Liste für Kaspersky Security Center hinzufügen. Klicken Sie dazu auf **Aus der Liste für Kaspersky Security Center hinzufügen**.

   b. Geben Sie erforderlichenfalls im Feld **Beschreibung** eine Beschreibung der Programmliste ein.

   c. Wählen Sie in der Dropdown-Liste **Regel für Programme** die Option **Alle neu erstellten Dateien verschlüsseln**.

Informationen über die Verschlüsselungsregel für Dateien, die von den ausgewählten Anwendungen erstellt oder geändert wurden, werden in der Tabelle auf der Registerkarte **Regeln für Programme** angezeigt.

8. Speichern Sie die vorgenommenen Änderungen.

Entschlüsselungsregel erstellen

Um eine Entschlüsselungsregel zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Verschlüsselung auf Dateiebene** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Gemäß den Regeln**.
5. Klicken Sie auf der Registerkarte **Entschlüsselung** auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente:
   a. Wählen Sie das Element **Standardordner**, um die von Kaspersky empfohlenen Dateien aus den Ordnern der lokalen Benutzerprofile zur Entschlüsselungsregel hinzuzufügen.
   b. Wählen Sie das Element **Manuell festgelegter Ordner**, um den Ordner, dessen Pfad manuell angegeben wird, zur Entschlüsselungsregel hinzuzufügen.
   c. Wählen Sie das Element **Dateien nach Erweiterung** aus, um bestimmte Dateierweiterungen zu der Entschlüsselungsregel hinzuzufügen. Dateien mit den angegebenen Erweiterungen werden auf allen lokalen Festplatten des Computers nicht von Kaspersky Endpoint Security verschlüsselt.
   d. Wählen Sie das Element **Dateien nach Erweiterungsgruppen** aus, um Gruppen für Dateierweiterungen (z. B. die Gruppe *Microsoft-Office-Dokumente*) zu der Entschlüsselungsregel hinzuzufügen. Dateien mit den Erweiterungen, die in den Erweiterungsgruppen aufgezählt sind, werden von Kaspersky Endpoint Security auf allen lokalen Festplatten des Computers nicht verschlüsselt.
6. Speichern Sie die vorgenommenen Änderungen.

Wurde eine Datei sowohl zur Verschlüsselungsregel als auch zur Entschlüsselungsregel hinzugefügt, so geht Kaspersky Endpoint Security wie folgt vor: Wenn die Datei nicht verschlüsselt ist, wird sie nicht verschlüsselt, und wenn die Datei verschlüsselt ist, wird sie entschlüsselt.

Dateientschlüsselung auf lokalen Festplatten des Computers

Gehen Sie wie folgt vor, um Dateien auf lokalen Datenträgern des Computers zu entschlüsseln:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Verschlüsselung auf Dateiebene** aus.
4. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Verschlüsselung**.
5. Schließen Sie aus der Verschlüsselungsliste alle Dateien und Ordner aus, die Sie entschlüsseln möchten. Wählen Sie dazu in der Liste diese Dateien aus und wählen Sie im Kontextmenü der Schaltfläche **Löschen** den Punkt **Regel löschen und Dateien entschlüsseln**.

   Die aus der Verschlüsselungsliste gelöschten Dateien und Ordner werden automatisch zur Entschlüsselungsliste hinzugefügt.
6. Erstellen Sie eine Dateiliste für Entschlüsselung
7. Speichern Sie die vorgenommenen Änderungen.

Unmittelbar nach der Übernahme der Richtlinie entschlüsselt Kaspersky Endpoint Security die verschlüsselten Dateien, die der Entschlüsselungsliste hinzugefügt wurden.

Kaspersky Endpoint Security entschlüsselt verschlüsselte Dateien, wenn ihre Parameter (Dateipfad / Dateiname / Dateierweiterung) geändert wurden und nach der Änderung den Parametern der Objekte entsprechen, die in die Entschlüsselungsliste aufgenommen sind.

Kaspersky Endpoint Security wartet mit der Entschlüsselung geöffneter Dateien, bis sie geschlossen werden.

Verschlüsselte Archive erstellen

Für den Schutz von Daten, die von Benutzern innerhalb des Unternehmensnetzwerks mit Dateien übertragen werden, können Sie verschlüsselte Archive verwenden. Verschlüsselte Archive eignen sich zur Übertragung großer Dateien mithilfe von Wechseldatenträgern, da E-Mail-Clients eine Größenbeschränkung für Dateien haben.

Vor dem Erstellen eines verschlüsselten Archivs fragt Kaspersky Endpoint Security den Benutzer nach einem Kennwort. Um einen zuverlässigen Datenschutz zu gewährleisten, können Sie die Überprüfung der Kennwortstärke aktivieren und Komplexitätskriterien festlegen. In diesem Fall ist die Verwendung kurzer und einfacher Kennwörter untersagt (wie beispielsweise `1234`).

Aktivieren der Kennwortstärkeprüfung beim Erstellen verschlüsselter Archive in der Verwaltungskonsole (MMC)

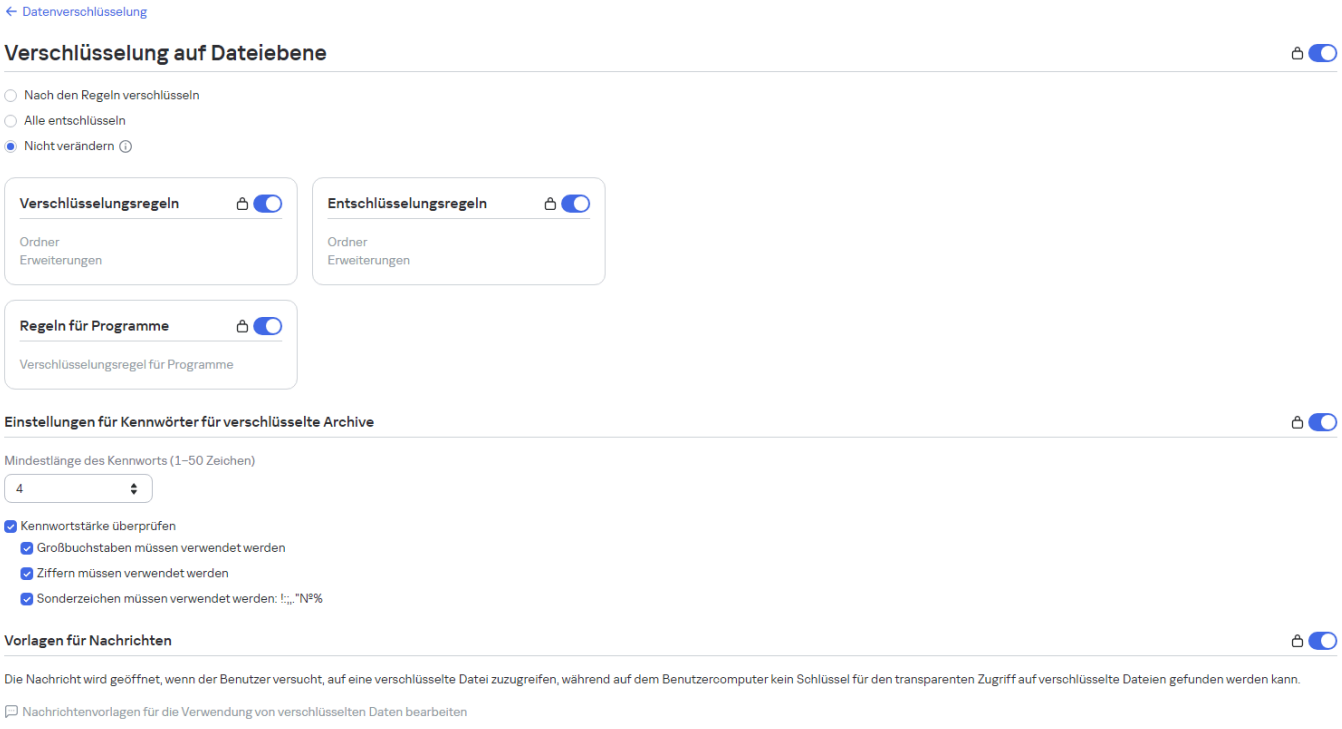
1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Allgemeine Verschlüsselungseinstellungen** aus.
4. Klicken Sie im Block **Einstellungen für Kennwörter** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Verschlüsselte Archive**-Registerkarte aus.
6. Passen Sie die Einstellungen für die Kennwortstärke an, die beim Erstellen verschlüsselter Archive gelten sollen.

So aktivieren Sie die Kennwortstärkeprüfung beim Erstellen verschlüsselter Archive in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Datenverschlüsselung → Verschlüsselung auf Dateiebene**.
5. Konfigurieren Sie im Block **Einstellungen für Kennwörter für verschlüsselte Pakete** die Kriterien für die Kennwortstärke, die beim Erstellen verschlüsselter Archive gelten sollen.



Einstellungen der Dateiverschlüsselung

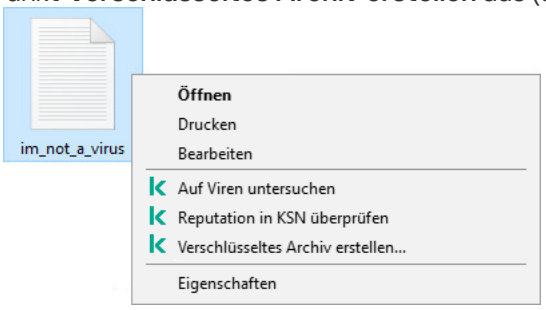
Verschlüsselte Archive können Sie auf Computern erstellen, auf denen das Programm Kaspersky Endpoint Security mit der Funktion zur Datenverschlüsselung installiert ist.

Wenn zu einem verschlüsselten Archiv eine Datei hinzugefügt wird, deren Inhalt sich im Cloud-Speicher OneDrive befindet, lädt Kaspersky Endpoint Security den Inhalt der entsprechenden Datei herunter und führt die Verschlüsselung aus.

Gehen Sie folgendermaßen vor, um ein verschlüsseltes Archiv zu erstellen:

1. Verwenden Sie einen beliebigen Dateimanager, um die Dateien und Ordner zu markieren, die Sie zu einem verschlüsselten Archiv hinzufügen möchten. Öffnen Sie durch Rechtsklick das Kontextmenü.

2. Wählen Sie im Kontextmenü den Punkt **Verschlüsseltes Archiv erstellen** aus (s. Abb. unten).



Verschlüsseltes Archiv erstellen

3. Legen Sie im folgenden Fenster ein Kennwort fest und bestätigen Sie es.

   Das Kennwort muss den Komplexitätskriterien entsprechen, die in der Richtlinie angegeben sind.

4. Klicken Sie auf **Erstellen**.

   Der Vorgang zur Erstellung eines verschlüsselten Archivs wird gestartet. Während der Erstellung eines verschlüsselten Archivs nimmt Kaspersky Endpoint Security keine Dateikomprimierung vor. Nach Abschluss des Vorgangs wird am angegebenen Speicherort auf dem Datenträger ein selbstentpackendes Archiv erstellt, das verschlüsselt und durch ein Kennwort geschützt ist (ausführbare Datei mit der Erweiterung exe) – .

Um Zugriff auf die Dateien in einem verschlüsselten Archiv zu erhalten, muss der Assistent zum Extrahieren des Archivs gestartet werden. Der Assistent wird durch Doppelklick und Kennworteingabe gestartet. Wenn Sie das Kennwort vergessen haben, kann der Zugriff auf die Dateien in einem verschlüsselten Archiv nicht wiederhergestellt werden. Sie können ein neues verschlüsseltes Archiv erstellen.

Wiederherstellen des Zugriffs auf verschlüsselte Dateien

Bei der Dateiverschlüsselung erhält Kaspersky Endpoint Security einen Chiffrierschlüssel, der für den direkten Zugriff auf die verschlüsselten Dateien erforderlich ist. Mithilfe eines Chiffrierschlüssels kann ein Benutzer direkten Zugriff auf verschlüsselte Dateien erhalten. Voraussetzung dafür ist, dass der Benutzer bei einem beliebigen Windows-Benutzerkonto angemeldet ist, das zum Zeitpunkt der Dateiverschlüsselung aktiv war. Damit Benutzer, die bei Windows-Benutzerkonten angemeldet sind, welche zum Zeitpunkt der Dateiverschlüsselung inaktiv waren, auf verschlüsselte Dateien zugreifen können, ist eine Verbindung mit Kaspersky Security Center erforderlich.

Verschlüsselte Dateien können in folgenden Fällen nicht verfügbar sein:

- Auf dem Benutzercomputer sind Chiffrierschlüssel vorhanden, es besteht aber keine Verbindung zu Kaspersky Security Center. Diese Verbindung ist für die Arbeit mit Chiffrierschlüsseln erforderlich. In diesem Fall muss der Benutzer den Zugriff auf die verschlüsselten Dateien beim Administrator des lokalen Unternehmensnetzwerks anfordern.

Wenn keine Verbindung zu Kaspersky Security Center besteht, ist es erforderlich:

- für den Zugriff auf verschlüsselte Dateien, die auf Computerfestplatten gespeichert sind, einen Zugriffsschlüssel anzufordern
- für den Zugriff auf verschlüsselte Dateien, die auf Wechseldatenträgern gespeichert sind, für jeden Wechseldatenträger einen separaten Zugriffsschlüssel für die verschlüsselten Dateien anzufordern.

- Die Verschlüsselungskomponenten wurden vom Benutzercomputer entfernt. In diesem Fall kann der Benutzer verschlüsselte Dateien auf lokalen Datenträgern und auf Wechseldatenträgern zwar öffnen, der Inhalt der Dateien wird aber in verschlüsselter Form angezeigt.

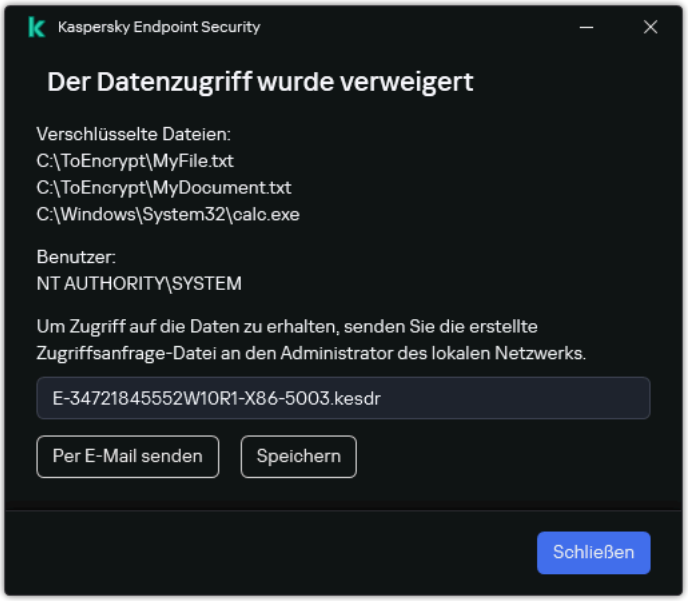
  Der Benutzer kann unter folgenden Bedingungen mit verschlüsselten Dateien arbeiten:

  - Die Dateien befinden sich in verschlüsselten Archiven, die auf einem Computer erstellt wurden, auf dem das Programm Kaspersky Endpoint Security installiert ist.
  - Die Dateien sind auf Wechseldatenträgern gespeichert, für welche die Arbeit im portablen Modus zugelassen ist.

Um Zugriff auf die verschlüsselten Dateien zu erhalten, muss der Benutzer den Wiederherstellungsvorgang („Anfrage-Frage“) starten.

Der Zugriff auf die verschlüsselten Dateien wird mit den folgenden Schritten wiederhergestellt:

1. Der Benutzer sendet eine Zugriffsanfrage-Datei an den Administrator (s. Abb. unten).
2. Der Administrator fügt die Zugriffsanfrage-Datei in Kaspersky Security Center hinzu, erstellt eine Zugriffsschlüsseldatei und sendet diese Datei an den Benutzer.
3. Der Benutzer fügt die Zugriffsschlüsseldatei in Kaspersky Endpoint Security hinzu und erhält Zugriff auf die Dateien.



Wiederherstellen des Zugriffs auf verschlüsselte Dateien

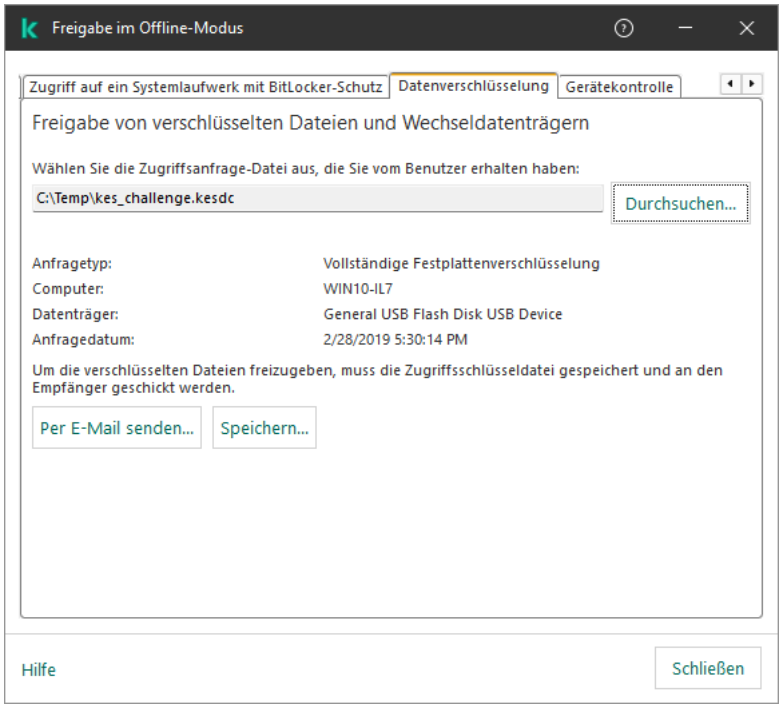
Um den Wiederherstellungsvorgang zu starten, muss der Benutzer auf eine Datei zugreifen. Dann erstellt Kaspersky Endpoint Security eine Zugriffsanfrage-Datei (Datei mit der Erweiterung kesdc), die beispielsweise per E-Mail an den Administrator übermittelt werden muss.

Kaspersky Endpoint Security erstellt eine Zugriffsanfrage-Datei, die für alle verschlüsselten Dateien gilt, die auf dem Computerlaufwerk (lokales Laufwerk oder Wechseldatenträger) gespeichert sind.

In der Verwaltungskonsole (MMC) eine Zugriffsschlüsseldatei für verschlüsselte Daten anfordern

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Geräte** aus.
3. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der den Zugriff auf verschlüsselte Daten wiederherstellen möchte, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
4. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Datenverschlüsselung**-Registerkarte aus.
6. Klicken Sie auf der Registerkarte **Datenverschlüsselung** auf **Durchsuchen**.
7. Geben Sie im Auswahlfenster der Zugriffsanfrage-Datei den Pfad der Datei an, die Sie vom Benutzer erhalten haben.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.



Zugriff im Offline-Modus gewähren

In der „Web Console“ eine Zugriffsschlüsseldatei für verschlüsselte Daten anfordern

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Datenzugriff wiederherstellen möchten.
3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.
4. Wählen Sie den Punkt **Datenverschlüsselung**.
5. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung kesdc).

   Die „Web Console“ zeigt Informationen über die Anfrage an. Unter anderem den Namen des Computers, auf dem der Benutzer Zugriff auf eine Datei anfordert.
6. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung kesdr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Nachdem der Benutzer die Zugriffsschlüsseldatei für die verschlüsselten Daten erhalten hat, muss er die Datei durch Doppelklick starten. Dann gewährt Kaspersky Endpoint Security den Zugriff auf alle verschlüsselten Dateien, die auf dem Laufwerk gespeichert sind. Um Zugriff auf verschlüsselte Dateien zu erhalten, die sich auf anderen Datenträgern befinden, müssen separate Zugriffsschlüssel für diese Datenträger angefordert werden.

Zugriff auf verschlüsselte Daten beim Ausfall des Betriebssystems wiederherstellen

Wenn das Betriebssystem ausfällt, ist die Wiederherstellung des Datenzugriffs nur für die Dateiverschlüsselung (FLE) verfügbar. Bei der vollständigen Festplattenverschlüsselung (FDE) ist es nicht möglich, den Datenzugriff wiederherzustellen.

Um bei einem Ausfall des Betriebssystems den Zugriff auf verschlüsselte Daten wiederherzustellen, gehen Sie wie folgt vor:

1. Installieren Sie das Betriebssystem neu, ohne die Festplatte zu formatieren.
2. Installieren Sie Kaspersky Endpoint Security.
3. Stellen Sie eine Verbindung zwischen dem Computer und dem Administrationsserver für Kaspersky Security Center her, von dem der Computer während der Datenverschlüsselung verwaltet wurde.

Der Zugriff auf verschlüsselte Daten wird zu den gleichen Bedingungen gewährt, wie sie vor dem Ausfall des Betriebssystems galten.

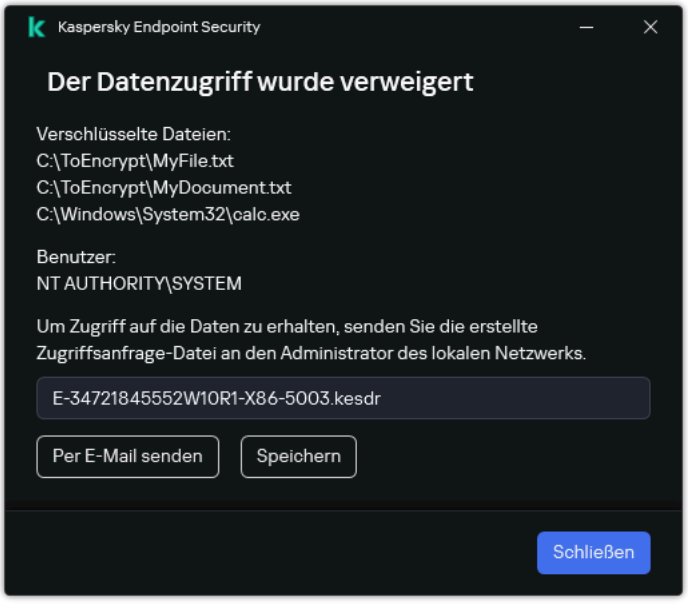
Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anpassen

Gehen Sie wie folgt vor, um Meldungsvorlagen für den Zugriff auf verschlüsselte Dateien anzupassen:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Allgemeine Verschlüsselungseinstellungen** aus.
4. Klicken Sie im Block **Vorlagen** auf **Vorlagen**.
5. Gehen Sie im angezeigten Fenster wie folgt vor:
   - Um die Vorlage für eine vom Benutzer gesendete Nachricht zu ändern, wählen Sie die Registerkarte **Nachricht vom Benutzer**. Das folgende Fenster wird geöffnet, wenn der Benutzer auf eine verschlüsselte Datei zugreifen möchte, während auf dem Computer kein Zugriffsschlüssel für die verschlüsselten Dateien vorhanden ist. Durch Klick auf **Per E-Mail senden** wird automatisch eine Nachricht an den Benutzer erstellt. Diese Nachricht wird zusammen mit der Anforderungsdatei für den Zugriff auf verschlüsselte Dateien an den Administrator des lokalen Unternehmensnetzwerks gesendet.
   - Um die Vorlage für eine vom Administrator gesendete Nachricht zu ändern, wählen Sie die Registerkarte **Nachricht vom Administrator**. Der Benutzer erhält diese Nachricht, nachdem der Zugriff auf verschlüsselte Dateien gewährt wurde.
6. Ändern Sie die Meldungsvorlagen.

   Um dem Vorlagentext eine Variable hinzuzufügen, zeigen Sie mit dem Mauszeiger auf die entsprechende Position, klicken Sie auf **Variable** und wählen Sie die gewünschte Variable in der Liste aus.

   Den Standardvorlagentext können Sie mithilfe der Schaltfläche **Standard** wiederherstellen.
7. Speichern Sie die vorgenommenen Änderungen.



Wechseldatenträger verschlüsseln

Die Verschlüsselung von Wechseldatenträgern wird auf Arm-basierten Computern wird nicht unterstützt.

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Kaspersky Endpoint Security unterstützt die Dateiverschlüsselung in FAT32- und NTFS-Dateisystemen. Wenn mit dem Computer ein Wechseldatenträger mit einem nicht unterstützten Dateisystem verbunden ist, wird die Verschlüsselung dieses Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger den Zugriffsstatus „Nur Lesen“ fest.

Um die Daten auf Wechseldatenträgern zu schützen, können Sie folgende Verschlüsselungsmethoden verwenden:

- Full Disk Encryption (FDE).

  Verschlüsselung des gesamten Wechseldatenträgers, einschließlich des Dateisystems.

  Es ist nicht möglich, außerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen. Außerdem ist es nicht möglich, innerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen, wenn der Computer nicht mit Kaspersky Security Center („Gast-Computer“) verbunden ist.

- File Level Encryption (FLE).

  Nur Dateien auf dem Wechseldatenträger verschlüsseln. Dabei wird das Dateisystem nicht verändert.

  Die Verschlüsselung von Dateien auf Wechseldatenträgern ermöglicht es, auch außerhalb des Unternehmensnetzwerks auf die Daten zuzugreifen. Dazu dient der *portable Modus*.

Bei der Verschlüsselung erstellt Kaspersky Endpoint Security einen Master-Schlüssel. Kaspersky Endpoint Security speichert den Master-Schlüssel in den folgenden Speichern:

- Kaspersky Security Center.
- Benutzercomputer.

  Der Master-Schlüssel wird mit einem Geheimschlüssel des Benutzers verschlüsselt.

- Wechseldatenträger.

  Der Master-Schlüssel wird mit einem offenen Schlüssel von Kaspersky Security Center verschlüsselt.

Nach der Verschlüsselung sind die Daten auf dem Wechseldatenträger innerhalb des Unternehmensnetzwerks verfügbar, als würde ein gewöhnlicher unverschlüsselter Wechseldatenträger verwendet.

Zugriffserteilung auf verschlüsselte Daten

Wenn eine Wechseldatenträger mit verschlüsselten Daten verbunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

1. Es wird überprüft, ob in der lokalen Datenverwaltung auf dem Benutzercomputer ein Master-Schlüssel vorhanden ist.

   Wenn ein Master-Schlüssel gefunden wird, erhält der Benutzer Zugriff auf die Daten des Wechseldatenträgers.

   Wenn kein Master-Schlüssel gefunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

   a. Es wird eine Anfrage an Kaspersky Security Center gesendet.

      Daraufhin sendet Kaspersky Security Center eine Antwort mit einem Master-Schlüssel.

   b. Kaspersky Endpoint Security speichert den Master-Schlüssel in der lokalen Datenverwaltung auf dem Benutzercomputer, um ihn künftig für den verschlüsselten Wechseldatenträger zu verwenden.

2. Die Daten werden entschlüsselt.

Besonderheiten bei der Verschlüsselung von Wechseldatenträgern

Für die Verschlüsselung von Wechseldatenträgern gelten die folgenden Besonderheiten:

- Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Gruppe von verwalteten Computern erstellt. Deshalb ist das Ergebnis, das durch das Übernehmen der Richtlinie für Kaspersky Security Center mit angepasster Verschlüsselung/Entschlüsselung von Wechseldatenträgern erreicht wird, davon abhängig, mit welchen Computern ein Wechseldatenträger verbunden ist.

- Für Dateien mit dem Zugriffsstatus „nur Lesen“, die auf Wechseldatenträgern gespeichert sind, führt Kaspersky Endpoint Security keine Dateiverschlüsselung/-entschlüsselung durch.

- Als Wechseldatenträger werden folgende Gerätetypen unterstützt:

  - Datenträger, die über eine USB-Schnittstelle verbunden werden

  - Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

  - SSD-Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

Verschlüsselung von Wechseldatenträgern starten

Sie können einen Wechseldatenträger mithilfe einer Richtlinie entschlüsseln. Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Administrationsgruppe erstellt. Deshalb hängt das Ergebnis der Datenentschlüsselung auf Wechseldatenträgern davon ab, mit welchem Computer der Wechseldatenträger verbunden ist.

Kaspersky Endpoint Security unterstützt die Dateiverschlüsselung in FAT32- und NTFS-Dateisystemen. Wenn mit dem Computer ein Wechseldatenträger mit einem nicht unterstützten Dateisystem verbunden ist, wird die Verschlüsselung dieses Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger den Zugriffsstatus „Nur Lesen“ fest.

Bevor Sie Dateien auf einem Wechseldatenträger verschlüsseln, müssen Sie sicherstellen, dass der Datenträger formatiert ist und keine versteckten Partitionen enthält (z. B. eine EFI-Systempartition). Wenn der Datenträger unformatierte oder verborgene Partitionen enthält, schlägt die Dateiverschlüsselung möglicherweise fehl und ein Fehler wird angezeigt.

Um Wechseldatenträger zu verschlüsseln, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Verschlüsselung von Wechseldatenträgern** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Aktion aus, die Kaspersky Endpoint Security standardmäßig mit Wechseldatenträgern ausführen soll:

   - **Gesamten Wechseldatenträger verschlüsseln** (FDE). Kaspersky Endpoint Security verschlüsselt den Inhalt eines Wechseldatenträgers sektorweise. Dabei werden nicht nur die Dateien verschlüsselt, die auf dem Wechseldatenträger gespeichert sind, sondern auch die Dateisysteme, einschließlich Dateinamen und Ordnerstrukturen, auf dem Wechseldatenträger.
   - **Alle Dateien verschlüsseln** (FLE). Kaspersky Endpoint Security verschlüsselt alle Dateien, die auf Wechseldatenträgern gespeichert sind. Nicht verschlüsselt werden die Dateisysteme von Wechseldatenträgern sowie Dateinamen und Ordnerstrukturen.
   - **Nur neue Dateien verschlüsseln** (FLE). Kaspersky Endpoint Security verschlüsselt nur jene Dateien, die zu Wechseldatenträgern hinzugefügt wurden, oder die bereits auf Wechseldatenträgern gespeichert waren und verändert wurden, nachdem die Richtlinie für Kaspersky Security Center zum letzten Mal übernommen wurde.

   Ein bereits verschlüsselter Wechseldatenträger wird durch Kaspersky Endpoint Security nicht erneut verschlüsselt.

5. Wenn Sie den portablen Modus verwenden möchten, um Wechseldatenträger zu verschlüsseln, aktivieren Sie das Kontrollkästchen **Portabler Modus**.

   Der *portable Modus* ist ein Verschlüsselungsmodus für Dateien (FLE) auf Wechseldatenträgern. Der Modus ermöglicht einen Datenzugriff auch außerhalb des Unternehmensnetzwerks. Der portable Modus ermöglicht es außerdem, auf Computern, auf denen das Programm Kaspersky Endpoint Security nicht installiert ist, mit verschlüsselten Dateien zu arbeiten.

6. Wenn Sie einen neuen Wechseldatenträger verschlüsseln möchten, sollten Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln** aktivieren. Ist das Kontrollkästchen deaktiviert, so verschlüsselt Kaspersky Endpoint Security alle Dateien, einschließlich Reste gelöschter oder veränderter Dateien.

7. Um die Verschlüsselung für bestimmte Wechseldatenträger anzupassen, können Sie Verschlüsselungsregeln angeben.

8. Um die vollständige Festplattenverschlüsselung für Wechseldatenträger im Offline-Modus zu verwenden, aktivieren Sie das Kontrollkästchen **Verschlüsselung von Wechseldatenträgern im Offline-Modus erlauben**.

   Offline-Verschlüsselungsmodus – Verschlüsselungsmodus für Wechseldatenträger (FDE), wenn keine Verbindung zu Kaspersky Security Center besteht. Bei der Verschlüsselung speichert Kaspersky Endpoint Security den Master-Schlüssel nur auf dem Benutzercomputer. Kaspersky Endpoint Security sendet den Master-Schlüssel bei der nächsten Synchronisierung an Kaspersky Security Center.

   > Ist der Computer beschädigt, auf dem der Master-Schlüssel liegt, und die Daten wurden nicht an Kaspersky Security Center gesendet, so ist kein Zugriff auf den Wechseldatenträger möglich.

   Wenn das Kontrollkästchen **Verschlüsselung von Wechseldatenträgern im Offline-Modus erlauben** deaktiviert ist und keine Verbindung zu Kaspersky Security Center besteht, können Wechseldatenträger nicht verschlüsselt werden.

9. Speichern Sie die vorgenommenen Änderungen.

Wenn eine Richtlinie übernommen wurde und der Benutzer einen Wechseldatenträger anschließt oder bereits ein Wechseldatenträger verbunden ist, fragt Kaspersky Endpoint Security nach einer Bestätigung für den Verschlüsselungsvorgang (siehe folgende Abb.).

Das Programm bietet die folgenden Aktionen zur Auswahl:

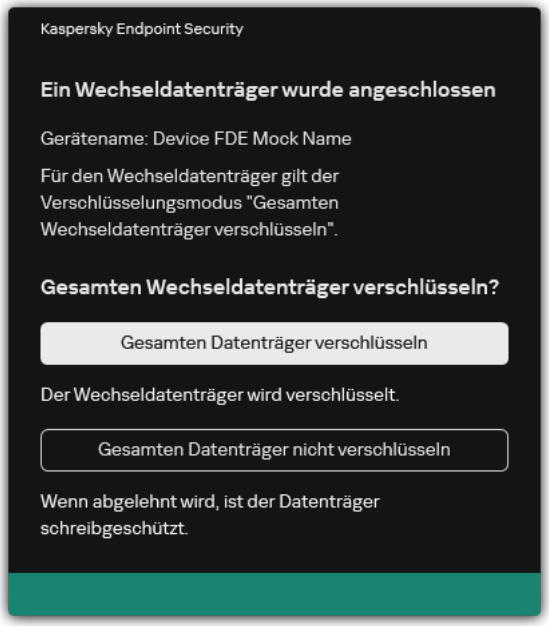
- Wenn der Benutzer die Verschlüsselungsanfrage bestätigt, verschlüsselt Kaspersky Endpoint Security die Daten.

- Wenn der Benutzer die Verschlüsselungsanfrage ablehnt, verändert Kaspersky Endpoint Security die Daten nicht und legt für diesen Wechseldatenträger das Zugriffsrecht „nur Lesen“ fest.

- Wenn der Benutzer die Verschlüsselungsanfrage nicht beantwortet, verändert Kaspersky Endpoint Security die Daten nicht und legt für diesen Wechseldatenträger das Zugriffsrecht „nur Lesen“ fest. Wenn die Richtlinie zum nächsten Mal angewendet wird oder wenn dieser Wechseldatenträger zum nächsten Mal verbunden wird, fragt das Programm erneut nach einer Bestätigung.

Initiiert der Benutzer während der Datenverschlüsselung das sichere Entfernen des Wechseldatenträgers, so bricht Kaspersky Endpoint Security die Datenverschlüsselung ab und ermöglicht so, den Wechseldatenträger vor dem Abschluss des Verschlüsselungsvorgangs sicher zu entfernen. Die Datenverschlüsselung wird vorgeschlagen, wenn der Wechseldatenträger zum nächsten Mal mit dem Computer verbunden wird.

Wenn die Verschlüsselung des Wechseldatenträgers fehlgeschlagen ist, überprüfen Sie den Bericht **Datenverschlüsselung** auf der Benutzeroberfläche von Kaspersky Endpoint Security. Möglicherweise ist der Zugriff auf die Dateien durch ein anderes Programm gesperrt. Versuchen Sie in diesem Fall, den Wechseldatenträger vom Computer zu trennen und erneut zu verbinden.



Anfrage zur Verschlüsselung eines Wechseldatenträgers

Verschlüsselungsregel für Wechseldatenträger hinzufügen

Um eine Verschlüsselungsregel für Wechseldatenträger hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung** → **Verschlüsselung von Wechseldatenträgern** aus.
4. Klicken Sie auf **Hinzufügen** und wählen Sie in der Dropdown-Liste eines der folgenden Elemente aus:
   - Um Verschlüsselungsregeln für Wechseldatenträger hinzuzufügen, die auf der Liste der vertrauenswürdigen Geräte für die Komponente „Gerätekontrolle“ stehen, wählen Sie das Element **Aus der Liste für vertrauenswürdige Geräte dieser Richtlinie**.
   - Um Verschlüsselungsregeln für Wechseldatenträger hinzuzufügen, die auf der Liste für Kaspersky Security Center stehen, wählen Sie das Element **Aus der Liste für Kaspersky Security Center** aus.
5. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus für die ausgewählten Geräte** die Aktion aus, die Kaspersky Endpoint Security mit auf Wechseldatenträgern gespeicherten Dateien ausführen soll.

6. Aktivieren Sie das Kontrollkästchen **Portabler Modus**, wenn Kaspersky Endpoint Security die Wechseldatenträger vor der Verschlüsselung so vorbereiten soll, dass die darauf verschlüsselten Dateien im portablen Modus verfügbar sind.

   Im portablen Modus können verschlüsselte Dateien auf Wechseldatenträgern auch dann verwendet werden, wenn der Wechseldatenträger mit einem Computer verbunden ist, auf dem die Verschlüsselungsfunktion nicht verfügbar ist.

7. Aktivieren Sie das Kontrollkästchen **Nur belegten Speicherplatz verschlüsseln**, damit Kaspersky Endpoint Security nur jene Laufwerkssektoren verschlüsselt, die mit Dateien belegt sind.

   Verwenden Sie die Verschlüsselung auf einem Datenträger, der bereits benutzt wurde, so sollte der gesamte Datenträger verschlüsselt werden. Dies garantiert den Schutz aller Daten, selbst gelöschter Daten, aus denen noch Informationen entnommen werden könnten. Die Funktion **Nur belegten Speicherplatz verschlüsseln** wird für neue Datenträger empfohlen, die bisher noch nicht benutzt wurden.

   Wenn ein Gerät zuvor mit der Funktion **Nur belegten Speicherplatz verschlüsseln** verschlüsselt wurde, werden Sektoren, die nicht mit Dateien belegt sind, auch dann weiterhin nicht verschlüsselt, nachdem eine Richtlinie im Modus **Gesamten Wechseldatenträger verschlüsseln** übernommen wurde.

8. Wählen Sie in der Dropdown-Liste **Aktion für bereits ausgewählte Geräte** die Aktion aus, die Kaspersky Endpoint Security mit Verschlüsselungsregeln ausführen soll, die bereits für Wechseldatenträger festgelegt wurden.

   - Wenn Sie eine zuvor erstellte Verschlüsselungsregel für einen Wechseldatenträger nicht ändern möchten, wählen Sie das Element **Überspringen**.
   - Wenn Sie eine zuvor erstellte Verschlüsselungsregel für einen Wechseldatenträger durch eine neue Regel ersetzen möchten, wählen Sie das Element **Aktualisieren**.

9. Speichern Sie die vorgenommenen Änderungen.

Die hinzugefügten Verschlüsselungsregeln für Wechseldatenträger werden auf Wechseldatenträger angewendet, die mit einem beliebigen Computer des Unternehmens verbunden sind.

Exportieren und Importieren einer Liste von Verschlüsselungsregeln für Wechseldatenträger

Sie können die Liste der Regeln der Wechseldatenträger-Verschlüsselung in eine XML-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Wechseldatenträgern desselben Typs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup für die Liste der Regeln anzulegen oder die Regeln auf einen anderen Server zu migrieren.

Exportieren und Importieren einer Liste von Regeln für die Verschlüsselung von Wechseldatenträgern in die Verwaltungskonsole (MMC)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Datenverschlüsselung → Verschlüsselung von Wechseldatenträgern**.

5. Klicken Sie im Block **Verschlüsselungsregeln für ausgewählte Geräte** auf den Link **<N> Regeln**.

   Dies öffnet eine Liste von Verschlüsselungsregeln für Wechseldatenträger.

6. So exportieren Sie die Liste der Verschlüsselungsregeln für Wechseldatenträger:

   a. Wählen Sie die Regeln, die Sie exportieren möchten.

   b. Klicken Sie auf **Exportieren**.

   c. Bestätigen Sie, dass Sie nur die ausgewählten Regeln exportieren möchten, oder exportieren Sie die gesamte Liste.

   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in eine XML-Datei im Standard-Download-Ordner.

7. So importieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Klicken Sie auf den Link **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

8. Speichern Sie die vorgenommenen Änderungen.

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.

2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Verschlüsselung von Wechseldatenträgern** aus.

4. So exportieren Sie die Liste der Verschlüsselungsregeln für Wechseldatenträger:

   a. Wählen Sie die Regeln, die Sie exportieren möchten. Um mehrere Ports auszuwählen, verwenden Sie die Tasten **STRG** oder **SHIFT**.

      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Endpoint Security alle Regeln.

   b. Klicken Sie auf den Link **Exportieren**.

   c. Geben Sie im folgenden Fenster den Namen der XLM-Datei an, in die Sie die Liste der Regeln exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die Liste der Regeln in die XLM-Datei.

5. So importieren Sie eine Liste von Verschlüsselungsregeln für Wechseldatenträger:

   a. Klicken Sie auf den Link **Importieren**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

   b. Öffnen Sie die Datei.

      Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Endpoint Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

6. Speichern Sie die vorgenommenen Änderungen.

Portabler Modus für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern

Der *portable Modus* ist ein Verschlüsselungsmodus für Dateien (FLE) auf Wechseldatenträgern. Der Modus ermöglicht einen Datenzugriff auch außerhalb des Unternehmensnetzwerks. Der portable Modus ermöglicht es außerdem, auf Computern, auf denen das Programm Kaspersky Endpoint Security nicht installiert ist, mit verschlüsselten Dateien zu arbeiten.

Der portable Modus bietet sich in folgenden Fällen an:

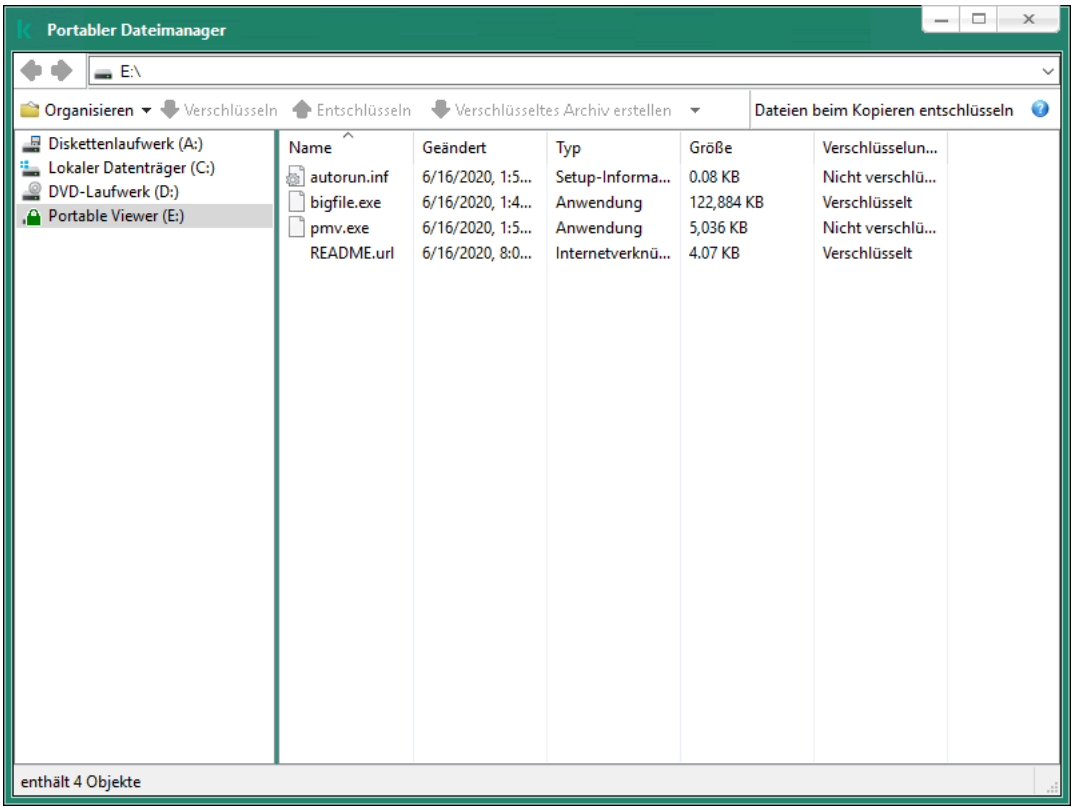
- Es besteht keine Verbindung zwischen dem Computer und dem Kaspersky Security Center Administrationsserver.
- Durch eine Änderung des Kaspersky Security Center Administrationsservers hat sich die Infrastruktur geändert.
- Das Programm Kaspersky Endpoint Security ist nicht auf dem Computer installiert.

Portabler Dateimanager

Für den portablen Modus installiert Kaspersky Endpoint Security auf dem Wechseldatenträger ein spezielles Verschlüsselungsmodul: den *portablen Dateimanager*. Der portable Dateimanager bietet eine Benutzeroberfläche für die Arbeit mit verschlüsselten Daten, wenn das Programm Kaspersky Endpoint Security nicht auf dem Computer installiert ist (s. Abb. unten). Wenn das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, können Sie einen gewöhnlichen Dateimanager (z. B. Explorer) verwenden, um mit verschlüsselten Wechseldatenträgern zu arbeiten.

Der portable Dateimanager speichert einen Schlüssel für die Verschlüsselung von Dateien auf dem Wechseldatenträger. Der Schlüssel ist mit einem Benutzerkennwort verschlüsselt. Der Benutzer legt das Kennwort fest, bevor die Dateien auf dem Wechseldatenträger verschlüsselt werden.

Der portable Dateimanager startet automatisch, wenn ein Wechseldatenträger mit einem Computer verbunden wird, auf dem das Programm Kaspersky Endpoint Security installiert ist. Wenn auf dem Computer der Autostart von Programmen deaktiviert ist, müssen Sie den portablen Dateimanager manuell starten. Führen Sie dazu die Datei pmv.exe aus, die auf dem Wechseldatenträger gespeichert ist.



Portabler Dateimanager

Unterstützung des portablen Modus für die Arbeit mit verschlüsselten Dateien

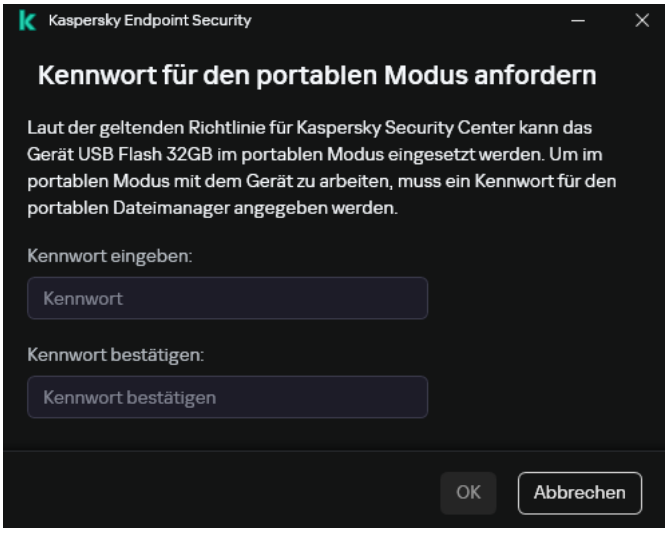
In der Verwaltungskonsole (MMC) die Unterstützung des portablen Modus für die Arbeit mit verschlüsselten Dateien auf Wechseldatenträgern aktivieren

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Verschlüsselung von Wechseldatenträgern** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus für die ausgewählten Geräte** die Variante **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln**.

   Der portable Modus ist nur für die Dateiverschlüsselung (FLE) verfügbar. Die Unterstützung des portablen Modus für die vollständige Festplattenverschlüsselung (FDE) kann nicht aktiviert werden.

5. Aktivieren Sie das Kontrollkästchen **Portabler Modus**.
6. Bei Bedarf können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.
7. Speichern Sie die vorgenommenen Änderungen.
8. Nachdem Sie die Richtlinie angewendet haben, verbinden Sie den Wechseldatenträger mit dem Computer.
9. Bestätigen Sie den Vorgang zur Verschlüsselung des Wechseldatenträgers.

Ein Fenster zum Erstellen eines Kennworts für den portablen Dateimanager wird geöffnet.



Kennwortanforderung für den portablen Modus

10. Legen Sie ein Kennwort fest, das den Anforderungen entspricht, und bestätigen Sie das Kennwort.
11. Speichern Sie die vorgenommenen Änderungen.

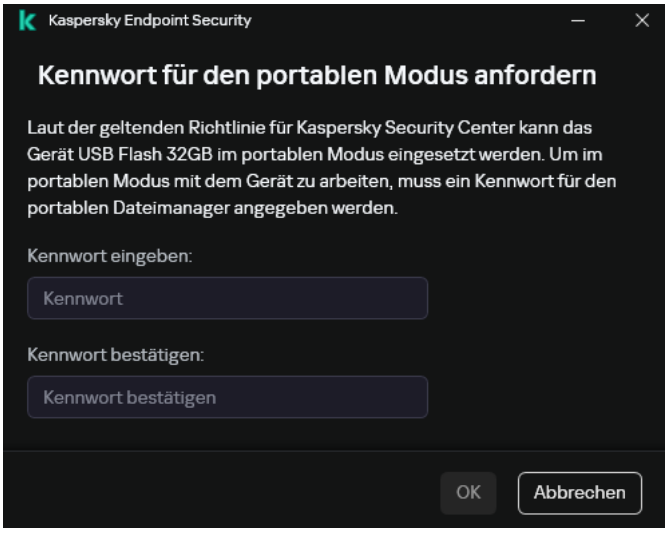
In der „Web Console“ die Unterstützung des portablen Modus für die Arbeit mit verschlüsselten Dateien auf Wechseldatenträgern aktivieren

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Datenverschlüsselung** → **Verschlüsselung von Wechseldatenträgern**.
5. Wählen Sie im Block **Standardaktion** den Punkt **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** aus.

   Der portable Modus ist nur für die Dateiverschlüsselung (FLE) verfügbar. Die Unterstützung des portablen Modus für die vollständige Festplattenverschlüsselung (FDE) kann nicht aktiviert werden.
6. Aktivieren Sie das Kontrollkästchen **Portabler Modus**.
7. Bei Bedarf können Sie Verschlüsselungsregeln für bestimmte Wechseldatenträger erstellen.
8. Speichern Sie die vorgenommenen Änderungen.
9. Nachdem Sie die Richtlinie angewendet haben, verbinden Sie den Wechseldatenträger mit dem Computer.
10. Bestätigen Sie den Vorgang zur Verschlüsselung des Wechseldatenträgers.

Ein Fenster zum Erstellen eines Kennworts für den portablen Dateimanager wird geöffnet.



Kennwortanforderung für den portablen Modus

11. Legen Sie ein Kennwort fest, das den Anforderungen entspricht, und bestätigen Sie das Kennwort.

12. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Endpoint Security verschlüsselt die Dateien auf dem Wechseldatenträger. Auf dem Wechseldatenträger wird auch der portable Dateimanager für die Verwendung verschlüsselter Dateien hinzugefügt. Wenn auf dem Wechseldatenträger bereits verschlüsselte Dateien vorhanden sind, verschlüsselt Kaspersky Endpoint Security diese erneut mithilfe eines eigenen Schlüssels. Dadurch kann der Benutzer im portablen Modus auf alle Dateien des Wechseldatenträgers zugreifen.

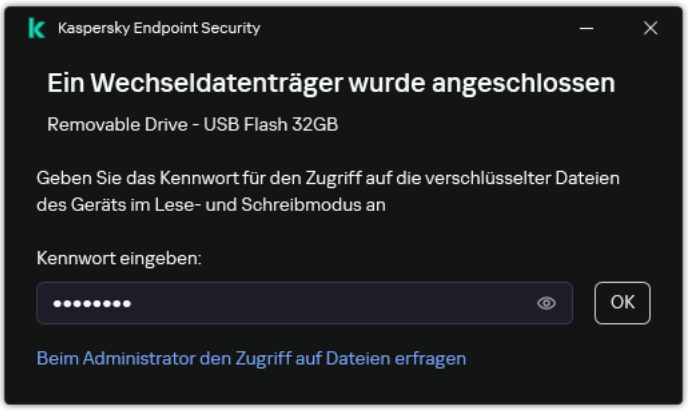
Zugriff auf verschlüsselte Dateien auf einem Wechseldatenträger anfordern

Nachdem Dateien auf einem Wechseldatenträger mit Unterstützung des portablen Modus verschlüsselt wurden, gibt es folgende Methoden für den Zugriff auf Dateien:

- Wenn das Programm Kaspersky Endpoint Security nicht auf dem Computer installiert ist, werden Sie vom portablen Dateimanager zur Kennworteingabe aufgefordert. Das Kennwort muss jedes Mal eingegeben werden, wenn der Computer neu gestartet oder ein Wechseldatenträger erneut verbunden wird.

- Wenn sich der Computer außerhalb des Unternehmensnetzwerks befindet und das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, werden Sie vom Programm aufgefordert, das Kennwort einzugeben oder beim Administrator den Zugriff auf die Dateien anzufordern. Nachdem der Zugriff auf die Dateien des Wechseldatenträgers gewährt wurde, speichert Kaspersky Endpoint Security einen Geheimschlüssel im Schlüsselspeicher des Computers. Dadurch ist der Dateizugriff künftig ohne Kennworteingabe oder Anfrage an den Administrator möglich (siehe folgende Abbildung).

- Wenn sich der Computer innerhalb des Unternehmensnetzwerks befindet und das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, erhalten Sie ohne Kennworteingabe Zugriff auf das Gerät. Kaspersky Endpoint Security erhält einen Geheimschlüssel von dem Kaspersky Security Center Administrationsserver, mit dem der Computer verbunden ist.



Zugriff auf verschlüsselte Dateien auf einem Wechseldatenträger anfordern

Wiederherstellen des Kennworts für den portablen Modus

Wenn Sie das Kennwort für den portablen Modus vergessen haben, müssen Sie den Wechseldatenträger innerhalb des Unternehmensnetzwerks mit einem Computer verbinden, auf dem das Programm Kaspersky Endpoint Security installiert ist. Sie erhalten Zugriff auf die Dateien, da der Geheimschlüssel im Schlüsselspeicher des Computers oder auf dem Administrationsserver gespeichert ist. Entschlüsseln Sie die Dateien und verschlüsseln Sie sie dann mit einem neuen Kennwort.

Besonderheiten des portablen Modus, wenn ein Wechseldatenträger mit einem Computer aus einem anderen Netzwerk verbunden wird

Wenn sich der Computer außerhalb des Unternehmensnetzwerks befindet und das Programm Kaspersky Endpoint Security auf dem Computer installiert ist, können Sie wie folgt ohne Kennworteingabe Zugriff auf die Dateien erhalten:

- **Zugriff mit Kennwort**

  Nach der Kennworteingabe können Sie die Dateien auf dem Wechseldatenträger anzeigen, ändern und speichern (*transparenter Zugriff*). Kaspersky Endpoint Security kann für einen Wechseldatenträger das Zugriffsrecht „nur Lesen“ festlegen, wenn in den Richtlinieneinstellungen für die Verschlüsselung von Wechseldatenträgern folgende Einstellungen festgelegt sind:

  - Die Unterstützung des portablen Modus ist deaktiviert.
  - Der Modus **Alle Dateien verschlüsseln** oder **Nur neue Dateien verschlüsseln** ist ausgewählt.

  In den übrigen Fällen erhalten Sie Vollzugriff auf den Wechseldatenträger („Schreiben und Lesen“). Sie können Dateien hinzufügen und löschen.

  Sie können die Rechte für den Zugriff auf einen Wechseldatenträger auch dann ändern, wenn der Wechseldatenträger mit dem Computer verbunden ist. Wenn sich die Rechte für den Zugriff auf einen Wechseldatenträger geändert haben, blockiert Kaspersky Endpoint Security den Zugriff auf die Dateien und fragt das Kennwort erneut ab.

Nach der Kennworteingabe können Richtlinieneinstellungen für die Verschlüsselung eines Wechseldatenträgers nicht angewendet werden. Deshalb ist es nicht möglich, die Dateien auf dem Wechseldatenträger zu entschlüsseln oder erneut zu verschlüsseln.

- **Anfrage für den Zugriff auf Dateien an den Administrator**

  Wenn Sie das Kennwort für den portablen Modus vergessen haben, fordern Sie beim Administrator den Zugriff auf die Dateien an. Für den Zugriff auf Dateien muss der Benutzer eine Zugriffsanfrage-Datei an den Administrator senden (Datei mit der Erweiterung .kesdc). Der Benutzer kann die Zugriffsanfrage-Datei beispielsweise per E-Mail senden. Der Administrator sendet eine Datei für den Zugriff auf die verschlüsselten Daten (Datei mit der Erweiterung kesdr).

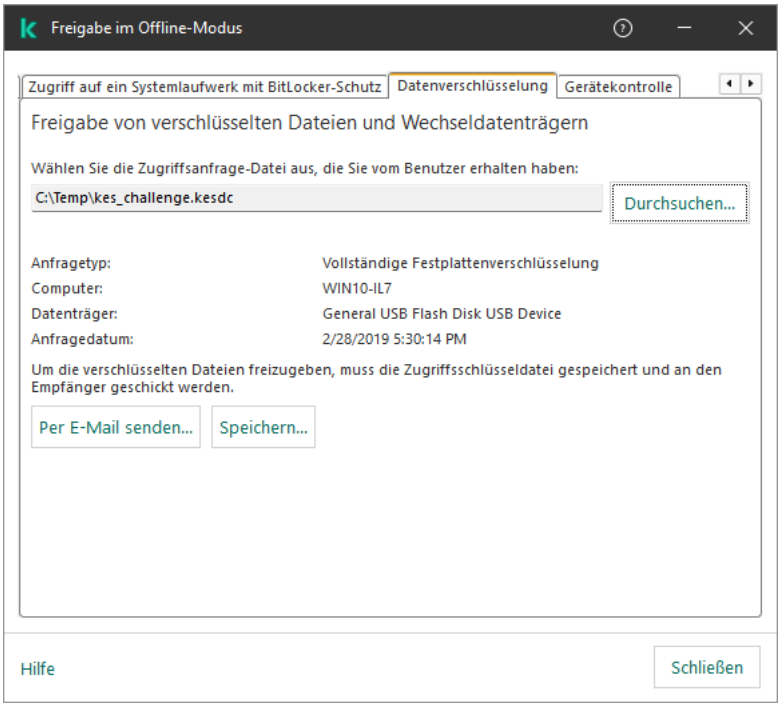
  Nachdem Sie den Vorgang zur Kennwortwiederherstellung („Anfrage-Frage“) durchlaufen haben, erhalten Sie transparenten Zugriff auf die Dateien auf dem Wechseldatenträger und Vollzugriff auf den Wechseldatenträger (Recht „Schreiben und Lesen“).

  Sie können die Richtlinie für die Verschlüsselung von Wechseldatenträgern anwenden und beispielsweise Dateien entschlüsseln. Nachdem das Kennwort wiederhergestellt wurde oder wenn die Richtlinie aktualisiert wird, fordert Kaspersky Endpoint Security Sie auf, die Änderungen zu bestätigen.

  In der Verwaltungskonsole (MMC) eine Zugriffsdatei für verschlüsselte Daten anfordern

  1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
  2. Wählen Sie in der Konsolenstruktur den Punkt **Geräte** aus.
  3. Markieren Sie auf der Registerkarte **Geräte** den Computer des Benutzers, der den Zugriff auf verschlüsselte Daten wiederherstellen möchte, und öffnen Sie mit der rechten Maustaste das Kontextmenü.
  4. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus**.
  5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die **Datenverschlüsselung**-Registerkarte aus.
  6. Klicken Sie auf der Registerkarte **Datenverschlüsselung** auf **Durchsuchen**.
  7. Geben Sie im Auswahlfenster der Zugriffsanfrage-Datei den Pfad der Datei an, die Sie vom Benutzer erhalten haben.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.



Zugriff im Offline-Modus gewähren

In der „Web Console“ eine Zugriffsdatei für verschlüsselte Daten anfordern

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, für den Sie den Datenzugriff wiederherstellen möchten.
3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.
4. Wählen Sie den Punkt **Datenverschlüsselung**.
5. Klicken Sie auf **Datei wählen** und wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung kesdc).

   Die „Web Console“ zeigt Informationen über die Anfrage an. Unter anderem den Namen des Computers, auf dem der Benutzer Zugriff auf eine Datei anfordert.
6. Klicken Sie auf **Schlüssel speichern** und wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung kesdr).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Wechseldatenträger entschlüsseln

Sie können einen Wechseldatenträger mithilfe einer Richtlinie entschlüsseln. Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Administrationsgruppe erstellt. Deshalb hängt das Ergebnis der Datenentschlüsselung auf Wechseldatenträgern davon ab, mit welchem Computer der Wechseldatenträger verbunden ist.

Um Wechseldatenträger zu entschlüsseln, gehen Sie wie folgt vor:

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Datenverschlüsselung → Verschlüsselung von Wechseldatenträgern** aus.
4. Um alle verschlüsselten Dateien zu entschlüsseln, die auf Wechseldatenträgern gespeichert sind, wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Aktion **Gesamten Wechseldatenträger entschlüsseln**.
5. Um die Daten zu entschlüsseln, die auf bestimmten Wechseldatenträgern gespeichert sind, ändern Sie die Verschlüsselungsregeln für die entsprechenden Wechseldatenträger. Gehen Sie dazu folgendermaßen vor:
   a. Wählen Sie in der Liste der Wechseldatenträger, für die Verschlüsselungsregeln vorliegen, den Eintrag des entsprechenden Wechseldatenträgers.
   b. Klicken Sie auf **Regel angeben**, um die Verschlüsselungsregel für diesen Wechseldatenträger zu bearbeiten.
   c. Wählen Sie im Kontextmenü der Schaltfläche **Regel angeben** den Punkt **Gesamten Wechseldatenträger entschlüsseln** aus.
6. Speichern Sie die vorgenommenen Änderungen.

Wenn der Benutzer den Wechseldatenträger verbindet oder er bereits verbunden ist, entschlüsselt Kaspersky Endpoint Security den Wechseldatenträger. Das Programm warnt den Benutzer, dass die Entschlüsselung einige Zeit in Anspruch nehmen kann. Initiiert der Benutzer während der Datenentschlüsselung das sichere Entfernen des Wechseldatenträgers, so bricht Kaspersky Endpoint Security die Datenentschlüsselung ab und ermöglicht so, den Wechseldatenträger vor dem Abschluss des Entschlüsselungsvorgangs sicher zu entfernen. Die Datenentschlüsselung wird fortgesetzt, nachdem der Wechseldatenträger zum nächsten Mal mit dem Computer verbunden wird.

Wenn die Entschlüsselung des Wechseldatenträgers fehlgeschlagen ist, überprüfen Sie den Bericht **Datenverschlüsselung** auf der Benutzeroberfläche von Kaspersky Endpoint Security. Möglicherweise ist der Zugriff auf die Dateien durch ein anderes Programm gesperrt. Versuchen Sie in diesem Fall, den Wechseldatenträger vom Computer zu trennen und erneut zu verbinden.

Informationen zur Datenverschlüsselung anzeigen

Während der Verschlüsselung und Entschlüsselung von Daten erhält Kaspersky Security Center von Kaspersky Endpoint Security Informationen zum Status der Übernahme von Verschlüsselungseinstellungen auf den Client-Computern.

Verschlüsselungsstatus anzeigen

Der Status bietet Ihnen Informationen über die Datenverschlüsselung. Für den Verschlüsselungsstatus gibt es in Kaspersky Endpoint Security die folgenden Varianten:

- **Entspricht nicht der Richtlinie; vom Benutzer abgebrochen**. Der Benutzer hat die Datenverschlüsselung abgebrochen.
- **Entspricht nicht der Richtlinie wegen eines Fehlers**. Fehler bei der Datenverschlüsselung, z. B. keine Lizenz vorhanden.
- **Die Richtlinie wird übernommen; ein Neustart ist erforderlich**. Auf dem Computer wird eine Datenverschlüsselung ausgeführt. Starten Sie den Computer neu, um die Datenverschlüsselung abzuschließen.
- **Es wurde keine Verschlüsselungsrichtlinie festgelegt**. Die Datenverschlüsselung ist in den Richtlinieneinstellungen deaktiviert.
- **Nicht unterstützt**. Auf dem Computer sind keine Datenverschlüsselungskomponenten installiert.
- **Die Richtlinie wird übernommen**. Auf dem Computer wird die Verschlüsselung und/oder Entschlüsselung von Daten ausgeführt.

Gehen Sie wie folgt vor, um die Verschlüsselungsstatus für die Daten des Computers anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte** aus.
3. Verschieben Sie auf der Registerkarte **Geräte** im Arbeitsbereich die Bildlaufleiste ganz nach rechts. Wenn die Spalte **Verschlüsselungsstatus** nicht angezeigt wird, fügen Sie diese Spalte in den Einstellungen der Kaspersky Security Center-Konsole hinzu.

   In der Spalte **Verschlüsselungsstatus** werden die Statusvarianten für die Datenverschlüsselung auf den Computern der ausgewählten Administrationsgruppe angezeigt. Dieser Status beruht auf Informationen über die Verschlüsselung von Dateien auf den lokalen Computerlaufwerken und über die vollständige Festplattenverschlüsselung.
4. Hat die Datenverschlüsselung für den Computer den Status **Bei der Übernahme der Richtlinie**, können Sie die Fortschrittsanzeige für die Verschlüsselung überwachen:
   a. Doppelklicken Sie auf die Eigenschaften des Computers mit dem Status **Bei der Übernahme der Richtlinie**.
   b. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Programme** aus.
   c. Wählen Sie in der Liste der auf dem Computer installierten Kaspersky-Apps den Punkt **Kaspersky Endpoint Security für Windows** aus.
   d. Klicken Sie auf **Statistik**.
   e. Unter **Verschlüsselung von Geräten** sehen Sie den aktuellen Fortschritt der Datenverschlüsselung mit Prozentangabe.

Verschlüsselungsstatistik in den Informationsbereichen von Kaspersky Security Center anzeigen

Gehen Sie wie folgt vor, um die Statusmeldungen zur Dateiverschlüsselung in den Informationsbereichen von Kaspersky Security Center anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Ordner **Administrationsserver** aus.
3. Wählen Sie im Arbeitsbereich, der sich rechts von der Verwaltungskonsole befindet, die Registerkarte **Statistik**.
4. Erstellen Sie eine neue Seite mit Informationsbereichen mit einer Statistik für die Datenverschlüsselung. Gehen Sie dazu folgendermaßen vor:
   a. Klicken Sie auf der Registerkarte **Statistik** auf **Ansicht konfigurieren**.
   b. Klicken Sie im folgenden Fenster auf **Hinzufügen**.
   c. Dadurch wird ein Fenster geöffnet; geben Sie in diesem Fenster im Abschnitt **Allgemein** den Namen der Seite ein.
   d. Klicken Sie im Abschnitt **Informationsbereiche** auf **Hinzufügen**.
   e. Wählen Sie im folgenden Fenster in der Gruppe **Schutzstatus** den Eintrag **Verschlüsselung von Geräten** aus.
   f. Klicken Sie auf **OK**.
   g. Ändern Sie erforderlichenfalls die Einstellungen des Detailbereichs. Verwenden Sie dazu die Abschnitte **Ansicht** und **Geräte**.
   h. Klicken Sie auf **OK**.
   i. Wiederholen Sie die Punkte d) bis h) dieser Anleitung. Wählen Sie dabei im Abschnitt **Schutzstatus** den Punkt **Wechseldatenträger verschlüsseln** aus.

      Die hinzugefügten Informationsbereiche erscheinen in der Liste **Informationsbereiche**.
   j. Klicken Sie auf **OK**.

      Der Name der Seite mit Informationsbereichen, die bei den vorhergehenden Schritten erstellt wurde, erscheint in der Liste **Seiten**.
   k. Klicken Sie auf **Schließen**.
5. Öffnen Sie auf der Registerkarte **Statistik** die Seite, die bei den vorhergehenden Schritten der Anleitung erstellt wurde.

Es werden Informationsbereiche angezeigt, in denen Sie den Verschlüsselungsstatus von Computern und Wechseldatenträgern einsehen können.

Fehler anzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten

Um Fehler anzuzeigen, die bei der Dateiverschlüsselung auf lokalen Computerlaufwerken auftreten, gehen Sie wie folgt vor:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Verwaltete Geräte** aus.
3. Markieren Sie in der Liste auf der Registerkarte **Geräte** den Computer und öffnen Sie durch Rechtsklick das Kontextmenü.
4. Wählen Sie im Kontextmenü des Computers den Punkt **Eigenschaften** aus. Wählen Sie im folgenden Fenster den Abschnitt **Schutz**.
5. Wechseln Sie mit dem Link **Fehler der Datenverschlüsselung anzeigen** ins Fenster **Fehler bei Datenverschlüsselung**.

In diesem Fenster werden Informationen über Fehler bei der Dateiverschlüsselung auf lokalen Laufwerken angezeigt. Wenn ein Fehler korrigiert wurde, löscht Kaspersky Security Center im Fenster **Fehler bei Datenverschlüsselung** die Informationen dazu.

Bericht über die Datenverschlüsselung anzeigen

Mit Kaspersky Security Center können Sie Bereiche zur Datenverschlüsselung erstellen:

- **Bericht über den Verschlüsselungsstatus verwalteter Geräte**. Der Bericht enthält Informationen darüber, ob der Verschlüsselungsstatus des Computers der Verschlüsselungsrichtlinie entspricht.
- **Bericht über den Verschlüsselungsstatus der Massenspeichergeräte**. Der Bericht enthält Informationen zum Verschlüsselungsstatus von externen Geräten und Massenspeichergeräten.
- **Bericht über Zugriffsrechte auf verschlüsselte Laufwerke**. Der Bericht enthält Informationen zum Status von Benutzerkonten, die Zugriff auf verschlüsselte Laufwerke haben.
- **Bericht über Fehler bei der Dateiverschlüsselung**. Der Bericht enthält Informationen zu Fehlern, die im Verlauf von Aufgaben zur Datenverschlüsselung bzw. Datenentschlüsselung auf Computern aufgetreten sind.
- **Bericht über blockierte Zugriffe auf verschlüsselte Dateien**. Der Bericht enthält Informationen über Apps, die am Zugriff auf verschlüsselte Dateien gehindert werden.

Gehen Sie folgendermaßen vor, um einen Bericht über die Datenverschlüsselung anzuzeigen:

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Knoten **Administrationsserver** die Registerkarte **Berichte** aus.

3. Klicken Sie auf **Neue Berichtsvorlage**.

   Der „Assistent für das Erstellen einer Berichtsvorlage“ wird gestartet.

4. Befolgen Sie die Anweisungen des Assistenten zur Erstellung einer Berichtsvorlage. Wählen Sie im Fenster **Typ der Berichtsvorlage auswählen** im Abschnitt **Andere** einen der Datenverschlüsselungsberichte aus.

   Nachdem der Assistent zum Erstellen einer Berichtsvorlage abgeschlossen wurde, erscheint die neue Berichtsvorlage in der Tabelle auf der Registerkarte **Berichte**.

5. Wählen Sie die Berichtsvorlage, die Sie bei den vorherigen Schritten der Anleitung erstellt haben.

6. Wählen Sie im Kontextmenü der Vorlage den Punkt **Bericht anzeigen** aus.

Der Vorgang zur Berichterstellung wird gestartet. Der Bericht wird in einem neuen Fenster angezeigt.

Mit verschlüsselten Geräten arbeiten, wenn kein Zugriff besteht

Freigabe von verschlüsselten Geräten

In folgenden Fällen kann es erforderlich sein, dass der Benutzer den Zugriff auf verschlüsselte Geräte anfordert:

- Die Festplatte wurde auf einem anderen Computer verschlüsselt.
- Auf dem Computer ist kein Chiffrierschlüssel für das Gerät vorhanden (z. B. beim ersten Zugriff auf einen verschlüsselten Wechseldatenträger auf diesem Computer) und es besteht keine Verbindung zu Kaspersky Security Center.

  Nachdem der Benutzer den Zugriffsschlüssel für ein verschlüsseltes Gerät übernommen hat, speichert Kaspersky Endpoint Security den Chiffrierschlüssel auf diesem Benutzercomputer und gibt künftig den Zugriff auf dieses Gerät frei, auch wenn keine Verbindung zu Kaspersky Security Center besteht.

Die Freigabe von verschlüsselten Geräten kann wie folgt erfolgen:

1. Der Benutzer erstellt über die Benutzeroberfläche von Kaspersky Endpoint Security eine Zugriffsanfrage-Datei mit der Erweiterung kesdc und übermittelt die Datei an den Administrator des lokalen Unternehmensnetzwerks.

2. Der Administrator erstellt in der Verwaltungskonsole von Kaspersky Security Center eine Zugriffsschlüsseldatei mit der Erweiterung kesdr und übermittelt die Datei an den Benutzer.

3. Der Benutzer wendet den Zugriffsschlüssel an.

Daten auf verschlüsselten Geräten wiederherstellen

Für die Arbeit mit verschlüsselten Geräten kann der Benutzer das Reparatur-Tool für verschlüsselte Geräte verwenden (im Folgenden „Reparatur-Tool“ genannt). Dies kann in folgenden Fällen erforderlich sein:

- Der Freigabevorgang mithilfe eines Zugriffsschlüssels ist fehlgeschlagen.
- Auf dem Computer mit dem verschlüsselten Gerät sind die Verschlüsselungskomponenten nicht installiert.

Die Daten, die erforderlich sind, um den Zugriff auf verschlüsselte Geräte mithilfe des Reparatur-Tools wiederherzustellen, befinden sich für einen bestimmten Zeitraum in unverschlüsselter Form im Arbeitsspeicher des Benutzercomputers. Um das Risiko eines unbefugten Zugriffs auf diese Daten zu reduzieren, wird empfohlen, den Wiederherstellungsvorgang nur auf vertrauenswürdigen Computern auszuführen.

Die Datenwiederherstellung auf verschlüsselten Geräten wird wie folgt ausgeführt:

1. Der Benutzer erstellt mithilfe des Reparatur-Tools eine Zugriffsanfrage-Datei mit der Erweiterung fdertc und übermittelt die Datei an den Administrator des lokalen Unternehmensnetzwerks.
2. Der Administrator erstellt in der Verwaltungskonsole für Kaspersky Security Center eine Zugriffsschlüsseldatei mit der Erweiterung fdertr und übermittelt die Datei an den Benutzer.
3. Der Benutzer wendet den Zugriffsschlüssel an.

Für die Wiederherstellung von Daten auf verschlüsselten Systemfestplatten kann der Benutzer im Reparatur-Tool auch die Anmeldedaten für den Authentifizierungsagenten angeben. Sind die Metadaten des Authentifizierungsagenten-Benutzerkontos beschädigt, so muss der Benutzer die Wiederherstellung mithilfe einer Zugriffsanfrage-Datei ausführen.

Bevor Daten auf verschlüsselten Geräten wiederhergestellt werden, sollte entweder der betreffende Computer aus der Verschlüsselungsrichtlinie für Kaspersky Security Center entnommen werden oder die Verschlüsselung in den Einstellungen der Richtlinie für Kaspersky Security Center deaktiviert werden. Dadurch wird verhindert, dass das Gerät erneut verschlüsselt wird.

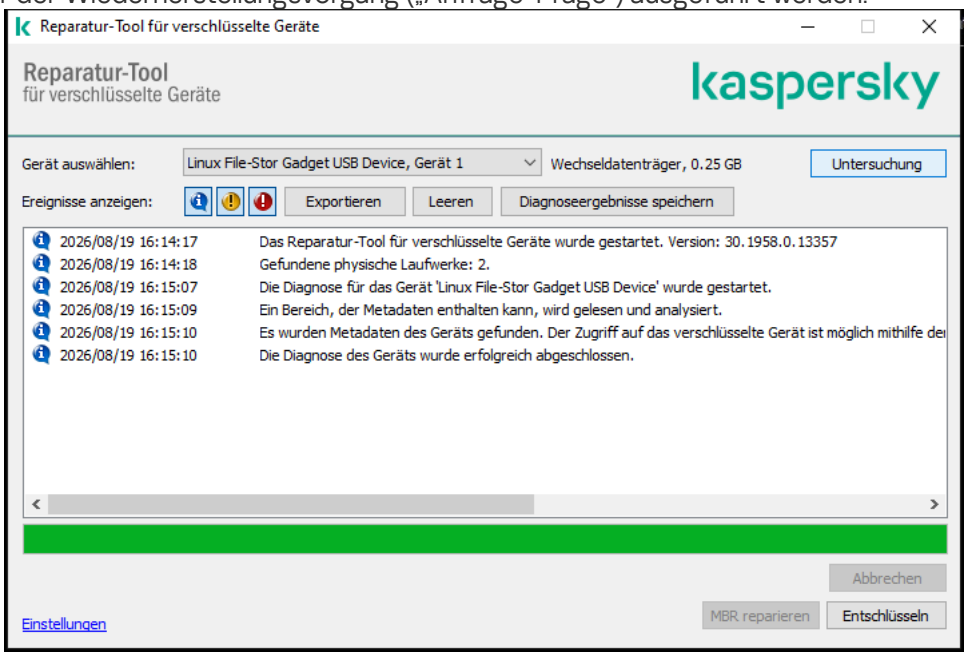
Datenwiederherstellung mithilfe des Reparatur-Tools FDERT

Bei einer Fehlfunktion der Festplatte kann das Dateisystem beschädigt werden. Dann sind die Daten, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt sind, nicht verfügbar. Sie können die Daten entschlüsseln und die Daten auf einen neuen Datenträger kopieren.

Um die Daten, die mit der Technologie Kaspersky-Festplattenverschlüsselung geschützt sind, auf einem Datenträger wiederherzustellen, sind die folgenden Schritte erforderlich:

1. Erstellen eines autonomen Reparatur-Tools (s. Abb. unten).
2. Verbinden des Datenträgers mit einem Computer, auf dem die Verschlüsselungskomponenten von Kaspersky Endpoint Security nicht vorhanden sind.
3. Starten des Reparatur-Tools und der Festplatten-Analyse.

4. Zugriff auf die Daten auf dem Datenträger. Dazu müssen die Anmeldedaten des Authentifizierungsagenten eingegeben oder der Wiederherstellungsvorgang („Anfrage-Frage“) ausgeführt werden.



FDERT-Reparatur-Tool

Erstellen eines autonomen Reparatur-Tools

Gehen Sie folgendermaßen vor, um eine ausführbare Datei des Wiederherstellungstools zu erstellen:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Klicken Sie im angezeigten Fenster auf **Verschlüsseltes Gerät wiederherstellen**.

   Das Reparatur-Tool für verschlüsselte Geräte wird gestartet.
3. Klicken Sie im Fenster des Wiederherstellungstools auf **Autonomes Reparatur-Tool erstellen**.
4. Speichern Sie das autonome Reparatur-Tool auf dem Computer.

Dadurch wird die ausführbare Datei des Wiederherstellungstools fdert.exe im angegebenen Ordner gespeichert. Kopieren Sie das Reparatur-Tool auf einen Computer, auf dem die Verschlüsselungskomponenten von Kaspersky Endpoint Security nicht vorhanden sind. Dadurch wird verhindert, dass der Datenträger erneut verschlüsselt wird.

Die Daten, die erforderlich sind, um den Zugriff auf verschlüsselte Geräte mithilfe des Reparatur-Tools wiederherzustellen, befinden sich für einen bestimmten Zeitraum in unverschlüsselter Form im Arbeitsspeicher des Benutzercomputers. Um das Risiko eines unbefugten Zugriffs auf diese Daten zu reduzieren, wird empfohlen, den Wiederherstellungsvorgang nur auf vertrauenswürdigen Computern auszuführen.

Datenwiederherstellung auf einer Festplatte

Um den Zugriff auf ein verschlüsseltes Gerät mithilfe des Reparatur-Tools wiederherzustellen, gehen Sie wie folgt vor:

1. Führen Sie die Datei mit dem Namen fdert.exe aus, die die ausführbare Datei des Wiederherstellungsprogramms ist. Diese Datei wird von Kaspersky Endpoint Security erstellt.

2. Wählen Sie im Fenster „Wiederherstellungs-Assistent“ das verschlüsselte Gerät aus, auf das Sie den Zugriff wiederherstellen möchten.

3. Klicken Sie auf die Schaltfläche **Untersuchung**, damit das Tool feststellen kann, welche Aktion mit dem verschlüsselten Gerät ausgeführt werden soll: entsperren oder entschlüsseln.

   Ist die Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf dem Computer verfügbar, so bietet das Reparatur-Tool an, das Gerät zu entsperren. Beim Entsperren wird das Gerät nicht entschlüsselt, es wird aber der direkte Zugriff freigegeben. Ist die Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf dem Computer nicht verfügbar, so bietet das Reparatur-Tool an, das Gerät zu entschlüsseln.

4. Um die Diagnose-Informationen zu importieren, klicken Sie auf **Diagnoseergebnisse speichern**.

   Das Tool speichert ein Archiv mit den Dateien der Diagnose-Informationen.

5. Klicken Sie auf **MBR reparieren**, wenn bei der Diagnose einer verschlüsselten Systemfestplatte Probleme gemeldet wurden, die mit dem Master Boot Record (MBR) des Geräts zusammenhängen.

   Eine Reparatur des Master Boot Records des Geräts kann den Empfang von Informationen beschleunigen, die für das Entsperren und die Entschlüsselung des Geräts benötigt werden.

6. Klicken Sie abhängig von den Ergebnissen der Diagnose auf **Entsperren** oder **Entschlüsseln**.

7. Wenn Sie die Daten mithilfe des Authentifizierungsagenten-Benutzerkontos wiederherstellen möchten, wählen Sie die Variante **Einstellungen des Benutzerkontos für den Authentifizierungsagenten verwenden** aus und geben Sie die Anmeldedaten des Authentifizierungsagenten ein.

   Diese Methode ist nur bei der Wiederherstellung von Daten auf einer Systemfestplatte möglich. Wurde die Systemfestplatte beschädigt und die Daten über das Authentifizierungsagenten-Benutzerkonto sind verloren gegangen, so muss für die Wiederherstellung von Daten auf einem verschlüsselten Gerät beim Administrator des lokalen Unternehmensnetzwerks ein Zugriffsschlüssel angefordert werden.

8. Wenn Sie den Wiederherstellungsvorgang starten möchten, gehen Sie wie folgt vor:

   a. Wählen Sie die Option **Zugriffsschlüssel für das Gerät manuell angeben** aus.

   b. Klicken Sie auf **Zugriffsschlüssel anfordern** und speichern Sie die Zugriffsanfrage-Datei auf dem Computer (Datei mit der Erweiterung fdertc).

   c. Senden Sie die Zugriffsanfrage-Datei an den Administrator des lokalen Unternehmensnetzwerks.

   Schließen Sie das Fenster **Zugriffsschlüssel für das Gerät anfordern** nicht, bevor Sie den Zugriffsschlüssel erhalten haben. Wenn dieses Fenster erneut geöffnet wird, kann der zuvor vom Administrator erstellte Zugriffsschlüssel nicht mehr verwendet werden.

d. Speichern Sie die erhaltene Zugriffsdatei (Datei mit der Erweiterung fdertr), die der Administrator des lokalen Unternehmensnetzwerks erstellt und an Sie übermittelt hat (s. Anleitung unten).

e. Laden Sie die Zugriffsdatei im Fenster **Zugriffsschlüssel für das Gerät anfordern**.

9. Wenn Sie die Entschlüsselung des Gerätes ausführen, müssen weitere Entschlüsselungseinstellungen angepasst werden:

   - Geben Sie einen Bereich für die Entschlüsselung an:

     - Wenn Sie das gesamte Gerät entschlüsseln möchten, wählen Sie die Variante **Ganzes Gerät entschlüsseln**.

     - Wenn Sie einen Teil der Daten auf dem Gerät entschlüsseln möchten, wählen Sie die Variante **Bestimmte Bereiche des Geräts entschlüsseln** und geben Sie die Grenzen des Entschlüsselungsbereichs an.

   - Legen Sie fest, wo die entschlüsselten Daten gespeichert werden sollen:

     - Damit die Daten auf dem ursprünglichen Gerät durch die entschlüsselten Daten überschrieben werden, deaktivieren Sie das Kontrollkästchen **Entschlüsselung in eine Laufwerkabbildsdatei**.

     - Damit die entschlüsselten Daten getrennt von den verschlüsselten Quelldaten gespeichert werden, aktivieren Sie das Kontrollkästchen **Entschlüsselung in eine Laufwerkabbildsdatei** und geben Sie mithilfe der Schaltfläche **Durchsuchen** einen Pfad an, unter dem die Datei im VHD-Format gespeichert werden soll.

10. Klicken Sie auf **OK**.

Der Vorgang zum Entsperren und zur Entschlüsselung des Geräts wird gestartet.

In der Verwaltungskonsole (MMC) eine Zugriffsdatei für verschlüsselte Daten erstellen

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Laufwerke** aus.

3. Wählen Sie im Arbeitsbereich das verschlüsselte Gerät aus, für das Sie eine Zugriffsschlüsseldatei erstellen möchten, und wählen Sie dann im Kontextmenü des Gerätes den Punkt **Zugriff auf das Gerät anfordern bei Kaspersky Endpoint Security**.

   Wenn unklar ist, für welchen Computer die Zugriffsanfrage-Datei erstellt wurde, wählen Sie in der Verwaltungskonsolenstruktur den Ordner **Erweitert → Verschlüsselung und Datenschutz** aus und klicken Sie im Arbeitsbereich auf **Chiffrierschlüssel für das Gerät anfordern bei Kaspersky Endpoint Security**.

4. Wählen Sie im folgenden Fenster den erforderlichen Verschlüsselungsalgorithmus aus: AES256 oder AES56.

   Der Datenverschlüsselungsalgorithmus ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Starke Verschlüsselung (AES256)* oder *Leichte Verschlüsselung (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.

5. Klicken Sie auf **Durchsuchen**. Geben Sie im angezeigten Fenster den Pfad der Anfragedatei mit der Erweiterung fdertc an, die Sie vom Benutzer erhalten haben.

6. Klicken Sie auf **Entsperren**.

Informationen über die Benutzeranfrage werden angezeigt. Kaspersky Security Center erstellt eine Zugriffsschlüsseldatei. Senden Sie die erstellte Zugriffsschlüsseldatei für die verschlüsselten Daten per E-Mail an den Benutzer. Oder speichern Sie die Zugriffsdatei und übermitteln Sie die Datei auf andere Weise.

In der „Web Console“ eine Zugriffsdatei für verschlüsselte Daten erstellen

1. Klicken Sie im Web Console-Hauptfenster auf **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Laufwerke**.

2. Aktivieren Sie das Kontrollkästchen mit dem Namen des Computers, auf dem Sie die Daten wiederherstellen möchten.

3. Klicken Sie auf **Zugriff auf das Gerät im autonomen Modus gewähren**.

   Der Assistent für die Zugriffserteilung auf das Gerät wird gestartet.

4. Folgen Sie den Anweisungen des Assistenten für die Zugriffserteilung auf das Gerät:

   a. Wählen Sie das Plug-in für Kaspersky Endpoint Security für Windows aus.

   b. Wählen Sie den erforderlichen Verschlüsselungsalgorithmus aus: AES256 oder AES56.

      Der Datenverschlüsselungsalgorithmus ist von der AES-Verschlüsselungsbibliothek abhängig, die zum Programmpaket gehört: *Starke Verschlüsselung (AES256)* oder *Leichte Verschlüsselung (AES56)*. Die AES-Verschlüsselungsbibliothek wird zusammen mit dem Programm installiert.

   c. Wählen Sie die Zugriffsanfrage-Datei aus, die Sie vom Benutzer erhalten haben (Datei mit der Erweiterung FDERTC).

   d. Wählen Sie aus, in welchem Ordner die Zugriffsschlüsseldatei für die verschlüsselten Daten gespeichert werden soll (Datei mit der Erweiterung FDERTC).

Sie erhalten dann einen Zugriffsschlüssel für die verschlüsselten Daten. Übermitteln Sie den Schlüssel an den Benutzer.

Notfall-CD erstellen

Die Notfall-CD kann eingesetzt werden, wenn ein Zugriff auf die verschlüsselte Systemfestplatte nicht möglich ist und sich das Betriebssystem nicht hochfahren lässt.

Sie können mithilfe der Notfall-CD ein Abbild des Windows-Betriebssystems laden und mithilfe des im Abbild enthaltenen Wiederherstellungstools den Zugriff auf die verschlüsselte Systemfestplatte wiederherstellen.

Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:

1. Erstellen Sie eine ausführbare Datei für das Reparatur-Tool für verschlüsselte Geräte.

2. Erstellen Sie ein benutzerdefiniertes Windows PE-Abbild. Wenn Sie das benutzerdefinierte Windows PE-Abbild erstellen, fügen Sie dem Abbild die Datei des Reparatur-Tools für verschlüsselte Geräte hinzu.

3. Speichern Sie das benutzerdefinierte Windows PE-Abbild auf einem bootfähigen Medium, beispielsweise auf einer CD oder einem Wechseldatenträger.

   Eine Anleitung zum Erstellen eines benutzerdefinierten Windows PE-Abbilds finden Sie in der Microsoft-Hilfe (beispielsweise bei Microsoft TechNet).

„Detection and Response“-Lösungen

Kaspersky Detection and Response-Lösungen sind Sicherheitssysteme zur Erkennung komplexer Bedrohungen und Angriffsindikatoren auf verschiedenen Ebenen einer Unternehmensinfrastruktur. Detection and Response-Lösungen liefern Informationen über die erkannte Bedrohung und ermöglichen die Verwaltung von Maßnahmen zur Bedrohungsabwehr.

Die Detection and Response-Lösung umfasst folgende Funktionen:

- Empfang von Informationen über den Betrieb eines Computers, Servers oder anderer Geräte (Telemetrie).
- Automatische Analyse dieser Informationen, um Bedrohungen zu erkennen.
- Generieren von Alarmdetails als Element der Bedrohungsentwicklungskette für die Analyse und Auswahl von Aktionen zur Bedrohungsabwehr.
- Durchführen von Aktionen zur Bedrohungsabwehr (z. B. Netzwerkisolation des Computers).

Kaspersky Endpoint Security unterstützt die „Detection and Response“-Lösungen, die einen integrierten Agenten verwenden. Der integrierte Agent sendet Telemetriedaten an die Server unserer Lösungen und führt Aktionen zur Bedrohungsabwehr aus. Der integrierte Agent unterstützt:

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)
- Kaspersky Anti Targeted Attack Platform:
  - Endpoint Detection and Response (EDR) Version 7.1 oder älter
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

Sie können Kaspersky Endpoint Security in verschiedenen Konfigurationen mit der Detection and Response-Lösung verwenden, z. B. als [EDR Optimum+MDR].

Lizenzverwaltung für MDR und EDR Optimum

Kaspersky Endpoint Security unterstützt die Funktionalitäten der Lösungen Kaspersky Managed Detection and Response (MDR) und Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). Sie können Kaspersky Endpoint Security mit diesen Lösungen in verschiedenen Konfigurationen verwenden und ein maßgeschneidertes Schutzsystem zusammenstellen, das Ihre speziellen Anforderungen erfüllt. Dafür müssen Sie für jede der Lösungen eine Lizenz erwerben. Die Lizenz kann das Recht zur Nutzung einer einzelnen Lösung (z. B. nur Add-on für MDR) oder mehrerer Lösungen (Add-on für [EDR Optimum+MDR]) einschließen.

MDR und EDR Optimum unterstützen die folgenden Methoden der Lizenzierung:

- Die Funktionalität von MDR oder EDR Optimum wird durch die Lizenz für Kaspersky Endpoint Security für Windows abgedeckt.

  Die Funktionalität steht nach der Aktivierung von Kaspersky Endpoint Security für Windows sofort zur Verfügung. Es genügt, einen Schlüssel hinzufügen.

- Separate Lizenzen für MDR oder EDR Optimum (MDR Add-on, EDR Optimum Add-on, [EDR Optimum+MDR] Add-on).

  Die Funktionalität wird verfügbar, sobald ein separater Schlüssel für das entsprechende Add-on von MDR, EDR Optimum oder [EDR Optimum+MDR] hinzugefügt wurde. Dadurch werden zwei Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security und ein Schlüssel für MDR oder EDR Optimum. Der Schlüssel für Kaspersky Endpoint Security muss zuerst hinzugefügt werden.

In Kaspersky Endpoint Security kann nur ein *aktiver Schlüssel* zur Lizenzierung von MDR und EDR Optimum hinzugefügt werden. Wenn Sie daher vorhaben, beide Lösungen zu aktivieren, müssen Sie einen Schlüssel für das [EDR Optimum+MDR] Add-on hinzufügen, anstelle eines separaten Schlüssels für jede der Lösungen. Zusätzlich können Sie einen *Reserveschlüssel* hinzufügen.

Wenn Sie bei der Bereitstellung von MDR eine BLOB-Datei verwendet haben, benötigen Sie keinen separaten Schlüssel, um MDR zu aktivieren. Die Lizenzinformationen sind bereits in der BLOB-Datei enthalten.

Erstmalige Lizenzierung der Lösungen

Im Rahmen der erstmaligen Bereitstellung von MDR und EDR Optimum werden diese Lösungen auf dieselbe Weise aktiviert, wie die Anwendung „Kaspersky Endpoint Security“. Einen Schlüssel können Sie mittels der Aufgabe *Schlüssel hinzufügen* oder der Funktion zur automatischen Schlüsselverteilung hinzufügen. Der Lizenzschlüssel wird der Anwendung entweder als zweiter aktiver Schlüssel oder, bei Aktivierung des entsprechenden Kontrollkästchens, als Reserveschlüssel hinzugefügt.

Von einer Lizenz zu einer anderen wechseln

Wenn in Ihrem Unternehmen bereits eine dieser Lösungen bereitgestellt wurde und der entsprechende Schlüssel zur Anwendung hinzugefügt wurde, sind bei der Lizenzierung der neuen Konfiguration einige Besonderheiten zu beachten. Beim Wechsel zu einer anderen Lizenz fügt die Anwendung den neuen Schlüssel der Anwendung nicht hinzu, sondern ersetzt den aktuellen Schlüssel durch den neuen Schlüssel. Der Grund dafür ist die Beschränkung, aufgrund derer die Anwendung nur einen Schlüssel hinzufügen kann, um MDR und EDR Optimum zu aktivieren.

So kann in Ihrem Unternehmen etwa [EDR Optimum+MDR] bereitgestellt sein und Sie haben nun vor, zur Konfiguration mit dem MDR-Add-on zu wechseln. Um zur neuen Konfiguration zu wechseln, müssen Sie den Schlüssel für das [EDR Optimum+MDR] Add-on durch den Schlüssel des MDR-Add-ons ersetzen.

Eine separate Lizenz ist für EDR Optimum und MDR (Add-on von [EDR Optimum+MDR]) nicht mehr verfügbar. Wenn Sie beide Lösungen verwenden möchten, müssen Sie MDR mittels einer BLOB-Datei und EDR Optimum mittels eines Lizenzschlüssels aktivieren.

Bei Verwendung der Funktion zur automatischen Schlüsselverteilung lehnt die Anwendung Lizenzschlüssel ab, von denen die gleiche Anzahl an Lösungen abgedeckt werden. Das heißt, dass Sie im Falle eines hinzugefügten Schlüssels für das Add-on von EDR Optimum, diesen Schlüssel nicht durch einen Schlüssel für das Add-on von MDR ersetzen können. Sie können jedoch den Schüssel für das Add-on von EDR Optimum durch einen Schlüssel für das Add-on von [EDR Optimum+MDR]. Gleichermaßen lehnt die Anwendung einen Schlüssel auch dann ab, wenn Sie versuchen, einen Schlüssel für das Add-on von MDR durch einen Schlüssel für das Add-on von EDR zu ersetzen. Zum Ersetzen eines Schlüssels können Sie die Aufgabe *Schlüssel hinzufügen* ausführen. Mit der Aufgabe *Schlüssel hinzufügen* können Lizenzschlüssel durch eine beliebige Anzahl von Lösungen zu ersetzt werden.

Wenn Sie einen Reserveschlüssel für das [EDR Optimum+MDR] Add-on hinzugefügt haben und einen aktiven Schlüssel für das EDR Optimum-Add-on oder das MDR-Add-on hinzuzufügen möchten, müssen Sie den Reserveschlüssel zunächst durch einen Schlüssel für das EDR Optimum-Add-on oder das MDR-Add-on ersetzen. Alternativ dazu können Sie den Reserveschlüssel auch löschen und anschließend den aktiven Schlüssel ersetzen.

Kompatibilität mit Drittanbieter-EDR-Lösungen

Sie können Kaspersky Endpoint Security zum Schutz von Workstations und Servern zusammen mit EDR-Lösungen von Drittanbietern verwenden. Zur Vermeidung von Fehlalarmen wird empfohlen, die ausführbaren Dateien von Kaspersky Endpoint Security und des Administrationsagenten zur vertrauenswürdigen Zone der Drittanbieter-EDR-Lösung hinzuzufügen.

Vertrauenswürdige Zone für die Kompatibilität mit Drittanbieter-EDR-Lösungen

	Kaspersky Endpoint Security für Windows	Administrationsagent von Kaspersky Security Center
Arbeitsordner	`C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0`	`C:\Program Files (x86)\Kaspersky Lab\NetworkAgent`

Ausführbare Dateien	`avp.exe`
	`avp.com`
	`avpsus.exe`
	`avpui.exe`
	`dump_writer_agent.exe`
	`kescli.exe`
	`kesdr.exe`
	`kldw.exe`
	`klpsm.exe`
	`kvdb_upgrader.exe`
	`modify_watcher.exe`
	`pmv.exe`
	`remediation.exe`
	`service_stub.exe`
		`AVPDTAgt.exe`
		`fix_gflags.exe`
		`getsysteminfo.exe`
		`integrity_checker.exe`
		`klcpuld.exe`
		`klcsldcl.exe`
		`klcsngtgui.exe`
		`klcspxy.exe`
		`kldumper.exe`
		`klmover.exe`
		`klnagchk.exe`
		`klnagent.exe`
		`klnagntf.exe`
		`klnagwds.exe`
		`klosprep.exe`
		`klrbtagt.exe`
		`klscflag.exe`
		`klscmodchk.exe`
		`klshwmsg.exe`
		`klwd.exe`
		`ksnproxy.exe`
		`Patch.exe`
		`tslauncher.exe`
		`Up2Date.exe`
		`vapm.exe`

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent gewährleistet die Interaktion zwischen dem Programm und anderen Kaspersky-Lösungen für die Erkennung komplexer Bedrohungen (z. B. Kaspersky Sandbox). Die Kaspersky-Lösungen, die Kaspersky Endpoint Agent unterstützen, sind von der Version von Kaspersky Endpoint Agent abhängig.

Um Kaspersky Endpoint Agent als Teil anderer Kaspersky-Lösungen zu verwenden, müssen Sie diese Lösungen mit einem entsprechenden Lizenzschlüssel aktivieren.

Umfassende Informationen zu Kaspersky Endpoint Agent, der Teil der von Ihnen verwendeten Softwarelösung ist, sowie umfassende Informationen zur Standalone-Lösung finden Sie in der Hilfe zum jeweiligen Produkt:

- Hilfe zu Kaspersky Anti Targeted Attack Platform
- Hilfe zu Kaspersky Sandbox
- Hilfe zu Kaspersky Endpoint Detection and Response Optimum
- Hilfe zu Kaspersky Managed Detection and Response

Der Lieferumfang von Kaspersky Endpoint Security für die Versionen 11.2.0 – 11.8.0 enthält Kaspersky Endpoint Agent. Sie können Kaspersky Endpoint Agent auswählen, wenn Sie Kaspersky Endpoint Security für Windows installieren. Dadurch werden zwei Apps auf Ihrem Computer installiert: KEA und KES. In Kaspersky Endpoint Security 11.9.0 ist das Verteilungspaket für Kaspersky Endpoint Agent nicht mehr Teil des Verteilungskits für Kaspersky Endpoint Security.

Entsprechung von KEA-Versionen (als Teil von KES) und KES-Versionen

Kaspersky Endpoint Security für Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

Kaspersky stellt Detection and Response komplett von Kaspersky Endpoint Agent auf die Verwendung mit dem integrierten Kaspersky Endpoint Security-Agenten um. Kaspersky fügt nach und nach die Unterstützung für diese Lösungen hinzu und lässt Kaspersky Endpoint Agent auslaufen (siehe Tabelle unten). Ab Version 12.1 unterstützt die App alle Detection and Response-Lösungen. Außerdem ist die App ab Version 12.1 nicht mehr mit Kaspersky Endpoint Agent kompatibel und die gleichzeitige Installation beider Apps auf demselben Computer ist nicht mehr möglich.

Version von Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (Komponente Endpoint Detection and Response)	Kaspersky Anti Targeted Attack Platform (Komponente Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	Kaspersky Endpoint Agent
12.6	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**	**Integrierter Agent**

Migration der Konfiguration [KES+KEA] zur Konfiguration [KES+built-in agent]

Kaspersky Endpoint Security verfügt über integrierte Agenten für die Verwendung mit Detection and Response-Lösungen. Das separate Programm „Kaspersky Endpoint Agent“ ist nicht mehr erforderlich, um diese Lösungen zu nutzen. Wenn Sie Kaspersky Endpoint Security auf Computern bereitstellen, auf denen Kaspersky Endpoint Agent installiert ist, funktionieren die Detection and Response-Lösungen weiterhin mit Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt.

Der Lieferumfang von Kaspersky Endpoint Security für die Versionen 11.2.0 – 11.8.0 enthält Kaspersky Endpoint Agent. Sie können Kaspersky Endpoint Agent auswählen, wenn Sie Kaspersky Endpoint Security für Windows installieren. Dadurch werden zwei Apps auf Ihrem Computer installiert: KEA und KES. In Kaspersky Endpoint Security 11.9.0 ist das Verteilungspaket für Kaspersky Endpoint Agent nicht mehr Teil des Verteilungskits für Kaspersky Endpoint Security.

Die Migration der Konfiguration [KES+KEA] zu [KES+built-in agent] umfasst die folgenden Schritte:

1. **Upgrade von Kaspersky Security Center**

   Upgraden Sie alle Komponenten von Kaspersky Security Center auf Version 13.2 oder höher, einschließlich des Administrationsagenten auf den Benutzercomputern und in Web Console.

2. **Upgrade des Web-Plug-ins für Kaspersky Endpoint Security**

Upgraden Sie in Kaspersky Security Center Web Console das Web-Plug-in für Kaspersky Endpoint Security auf Version 11.7.0 oder höher. Die Komponenten „EDR Optimum“ und „Kaspersky Sandbox“ müssen via Web Console verwaltet werden.

Zur Verwendung von Kaspersky Anti Targeted Attack Platform (EDR) benötigen Sie ein Web-Plug-in für Kaspersky Endpoint Security Version 12.1 oder höher.

Zur Verwendung von Kaspersky Anti Targeted Attack Platform (NDR) benötigen Sie ein Web-Plug-in für Kaspersky Endpoint Security Version 12.7 oder höher.

3. **Migration der Richtlinie und der Aufgaben**

   Verwenden Sie den Migrations-Assistenten für die Richtlinien und Aufgaben von Kaspersky Endpoint Agent, um die Einstellungen von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für Windows zu migrieren.

   Dadurch wird eine neue Richtlinie für Kaspersky Endpoint Security erstellt. Die neue Richtlinie hat den Status *Inaktiv*. Um die Richtlinie anzuwenden, öffnen Sie die Richtlinieneigenschaften, akzeptieren Sie die Bedingungen der Erklärung zu Kaspersky Security Network und setzen Sie den Status auf *Aktiv*.

4. **Lizenzverwaltung**

   Wenn Sie eine gewöhnliche Lizenz für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security zur Aktivierung von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Agent verwenden, wird die Funktionalität „EDR Optimum“ nach dem Upgrade des Programms auf Version 11.7.0 automatisch aktiviert. Sie müssen keine zusätzlichen Aktionen ausführen.

   Wenn Sie eine eigenständige Lizenz für das Kaspersky Endpoint Detection and Response Optimum-Add-on zur Aktivierung der EDR Optimum-Funktionalität verwenden, müssen Sie sicherstellen, dass der Schlüssel für das EDR Optimum-Add-on zur Kaspersky Security Center-Datenverwaltung hinzugefügt wird und dass die Funktionalität zur automatischen Verteilung von Lizenzschlüsseln aktiviert ist. Nach dem Upgrade des Programms auf Version 11.7.0 wird die Funktionalität „EDR Optimum“ automatisch aktiviert.

   Wenn Sie Kaspersky Endpoint Agent mit einer Lizenz für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security aktivieren und eine andere Lizenz zur Aktivierung von Kaspersky Endpoint Security für Windows verwenden, müssen Sie den Schlüssel für Kaspersky Endpoint Security für Windows mit dem gewöhnlichen Schlüssel für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security ersetzen. Sie können den Schlüssel mithilfe der Aufgabe *Schlüssel hinzufügen* ersetzen.

   Die Funktionalität „Kaspersky Sandbox“ muss nicht aktiviert werden. Kaspersky Sandbox ist sofort nach dem Upgrade und der Aktivierung von Kaspersky Endpoint Security für Windows verfügbar.

   Zum Aktivieren von Kaspersky Endpoint Security als Teil der Kaspersky Anti Targeted Attack Platform-Lösung kann nur die Lizenz von Kaspersky Anti Targeted Attack Platform verwendet werden. Nach dem Upgrade der App auf Version 12.1 wird die Funktionalität EDR (KATA) automatisch aktiviert. Sie müssen keine zusätzlichen Aktionen ausführen.

5. **Upgrade von Kaspersky Endpoint Security**

   Es wird empfohlen, für das Upgrade des Programms und die Migration der Funktionalitäten „EDR Optimum“ und „Kaspersky Sandbox“ eine Aufgabe zur Remote-Installation zu verwenden.

Um ein Upgrade des Programms mithilfe einer Aufgabe zur Remote-Installation vorzunehmen, bearbeiten Sie die folgenden Einstellungen:

- Wählen Sie die Komponenten für Detection and Response-Lösungen in den Einstellungen des Installationspakets aus.
- Schließen Sie die Komponente Kaspersky Endpoint Agent in den Einstellungen des Installationspakets aus (für Kaspersky Endpoint Security für Windows Versionen 11.2.0 – 11.8.0).
- Wenn der Kennwortschutz aktiviert ist, um den Zugriff auf Kaspersky Endpoint Agent einzuschränken, geben Sie das Deinstallationskennwort für die Anwendung in den Einstellungen der Aufgabe *Remote-Installation einer Anwendung* ein. Ab Kaspersky Security Center Linux 15.1 können Sie das Deinstallationskennwort eingeben.

Sie können das Programm auch mit den folgenden Methoden upgraden:

- Über den Kaspersky-Update-Dienst (Seamless Update – SMU).
- Lokal mithilfe des Installationsassistenten für das Programm.

Kaspersky Endpoint Security unterstützt die automatische Komponentenauswahl, wenn ein Programm-Upgrade auf einem Computer ausgeführt wird, auf dem das Programm „Kaspersky Endpoint Agent“ installiert ist. Die automatische Komponentenauswahl ist abhängig von den Berechtigungen des Benutzerkontos, unter dem das Programm upgegradet wird.

Wenn Sie Kaspersky Endpoint Security mithilfe der EXE- oder MSI-Datei unter dem Systemkonto (SYSTEM) upgraden, erhält Kaspersky Endpoint Security Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. Ist auf dem Computer beispielsweise Kaspersky Endpoint Agent installiert und die Lösung „EDR Optimum“ aktiviert, so konfiguriert das Kaspersky Endpoint Security-Installationsprogramm automatisch die Komponentenauswahl und wählt die Komponente „EDR Optimum“ aus. Dadurch wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent. Gewöhnlich wird das MSI-Installationsprogramm unter dem Systemkonto (SYSTEM) ausgeführt, wenn das Upgrade über den Kaspersky-Update-Dienst (SMU) erfolgt oder wenn ein Installationspaket über Kaspersky Security Center bereitgestellt wird.

Wenn Sie Kaspersky Endpoint Security mithilfe einer MSI-Datei unter einem Benutzerkonto ohne Administratorrechte upgraden, hat Kaspersky Endpoint Security keinen Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. In diesem Fall wählt Kaspersky Endpoint Security die Komponenten automatisch auf Basis der Kaspersky Endpoint Agent-Konfiguration aus. Anschließend wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

6 Neustart des Computers

Starten Sie Ihren Computer neu, um das Upgrade des Programms mit dem integrierten Agenten abzuschließen. Beim Programm-Upgrade wird Kaspersky Endpoint Agent vom Installationsprogramm entfernt, bevor der Computer neu gestartet wird. Nach dem Neustart des Computers fügt das Installationsprogramm den integrierten Agenten hinzu. Kaspersky Endpoint Security führt also die Funktionen von EDR und „Kaspersky Sandbox“ nicht aus, bis der Computer neu gestartet wurde.

7 Status von Kaspersky Endpoint Detection and Response Optimum und Kaspersky Sandbox überprüfen

Falls der Computer nach dem Upgrade in der Kaspersky Security Center-Konsole den Status *Kritisch* hat:

- Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
- Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*.
- Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

- Stellen Sie mithilfe der Option *Bericht über den Status der Programmkomponenten* sicher, dass die EDR Optimum-Funktionalität aktiviert ist. Wird für eine Komponente der Status *Nicht durch Lizenz abgedeckt* angezeigt wird, stellen Sie sicher, dass die Funktionalität zur automatischen Verteilung von Lizenzschlüsseln in EDR Optimum aktiviert ist.

Migration von Richtlinien und Aufgaben für Kaspersky Endpoint Agent

Kaspersky Endpoint Security für Windows enthält einen Assistenten für die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security. Sie können Richtlinien- und Aufgabeneinstellungen für die folgenden Lösungen migrieren:

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

Ein Assistent für die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security funktioniert nur in Web Console und Cloud Console. In der Verwaltungskonsole (MMC) können Sie die Einstellungen für die Lösung Kaspersky Anti Targeted Attack Platform (EDR) nur mit dem standardmäßigen Assistenten für die Migration von Richtlinien und Aufgaben von Kaspersky Security Center migrieren.

Es wird empfohlen, zunächst auf einem einzelnen Computer mit der Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security zu beginnen, dann auf einer Gruppe von Computern, und schließlich auf allen Computern der Organisation.

Um Richtlinien- und Aufgabeneinstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security zu migrieren,

wählen Sie im Web Console-Hauptfenster den Punkt **Vorgänge** → **Migration von Kaspersky Endpoint Agent** aus.

Dadurch wird der Migrations-Assistent für Richtlinien und Aufgaben ausgeführt. Folgen Sie den Anweisungen.

Schritt 1. Migration der Richtlinien

Der Migrationsassistent erstellt eine neue Richtlinie, die die Einstellungen der Richtlinien von Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammenführt. Wählen Sie in der Richtlinienliste jene Richtlinien von Kaspersky Endpoint Agent aus, deren Einstellungen Sie mit der Richtlinie von Kaspersky Endpoint Security zusammenführen möchten. Klicken Sie auf eine Richtlinie von Kaspersky Endpoint Agent, um die Richtlinie von Kaspersky Endpoint Security auszuwählen, mit der Sie die Einstellungen zusammenführen möchten. Stellen Sie sicher, dass Sie die korrekten Richtlinien ausgewählt haben, und gehen Sie weiter zum nächsten Schritt

Schritt 2. Aufgabenmigration

Der Migrations-Assistent erstellt neue Aufgaben für Kaspersky Endpoint Security. Wählen Sie in der Aufgabenliste die Aufgaben von Kaspersky Endpoint Agent, die Sie für die Kaspersky Endpoint Security-Richtlinie erstellen möchten. Der Assistent unterstützt Aufgaben für Kaspersky Endpoint Detection and Response und Kaspersky Sandbox. Weiter zum nächsten Schritt

Schritt 3. Assistent abschließen

Schließen Sie den Assistenten ab. Als Ergebnis geht der Assistent wie folgt vor:

- Er erstellt eine neue Richtlinie für Kaspersky Endpoint Security.

  Die Richtlinie führt Einstellungen Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammen. Die Richtlinie heißt *<Kaspersky Endpoint Security-Richtlinienname> & <Kaspersky Endpoint Agent-Richtlinienname>*. Die neue Richtlinie hat den Status *Inaktiv*. Um fortzufahren, ändern Sie den Status der Richtlinien von Kaspersky Endpoint Agent und Kaspersky Endpoint Security in *Inaktiv* und aktivieren Sie die neue zusammengeführte Richtlinie.

  > Stellen Sie nach der Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für Windows sicher, dass in der neuen Richtlinie die Funktion der Datenübertragung zum Administrationsserver (Daten zu Quarantänedateien und Daten zur Entwicklungskette der Bedrohung) eingerichtet ist. Es erfolgt keine Migration der Werte der Datenübertragungseinstellungen von den Richtlinien von Kaspersky Endpoint Agent.

  Wenn Sie die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für die Lösung Kaspersky Anti Targeted Attack Platform (EDR) ausführen, können beim Verbinden des Computers mit Central Node-Servern Fehler auftreten. Der Grund ist, dass der Migrations-Assistent in Web Console die folgenden Richtlinieneinstellungen überspringt und diese nicht migriert:

  - Verbot von Einstellungsänderungen **Verbindung mit KATA-Servern** („Schloss“).

    Die Einstellungen können standardmäßig geändert werden (das „Schloss“ ist geöffnet). Die Einstellungen werden daher nicht auf dem Computer übernommen. Sie müssen Einstellungsänderungen verbieten und das „Schloss“ verriegeln.

- Krypto-Container.

  Wenn Sie die Zwei-Wege-Authentifizierung zur Verbindung mit Central Node-Servern verwenden, müssen Sie den Krypto-Container erneut hinzufügen. Der Migrations-Assistent migriert das TLS-Zertifikat des Servers korrekt.

Der Migrations-Assistent für Richtlinien und Aufgaben in der Verwaltungskonsole (MMC) migriert alle Einstellungen für die Lösung Kaspersky Anti Targeted Attack Platform (EDR).

- Er erstellt Aufgaben für Kaspersky Endpoint Security.

  Neue Aufgaben sind Kopien der Aufgaben von Kaspersky Endpoint Agent für Kaspersky Endpoint Detection and Response und Kaspersky Sandbox. Gleichzeitig lässt der Assistent die Aufgaben von Kaspersky Endpoint Agent unverändert.

So migrieren Sie in der Verwaltungskonsole (MMC) die Richtlinien- und Aufgabeneinstellungen von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security (nur für KATA (EDR))

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus und öffnen Sie durch Rechtsklick das Kontextmenü.

2. Wählen Sie die Option **Alle Aufgaben → Assistent für das Massenkonvertieren von Richtlinien und Aufgaben** aus.

Der „Assistent für das Massenkonvertieren von Richtlinien und Aufgaben“ wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Auswahl des Programms, für das Sie Richtlinien und Aufgaben konvertieren müssen

Bei diesem Schritt müssen Sie Kaspersky Endpoint Security für Windows auswählen. Weiter zum nächsten Schritt

Schritt 2. Konvertieren von Richtlinien

Der Migrations-Assistent erstellt eine neue Kaspersky Endpoint Security-Richtlinie, in die die Richtlinieneinstellungen von Kaspersky Endpoint Agent migriert werden. Wählen Sie in der Richtlinienliste jene Kaspersky Endpoint Agent-Richtlinien aus, deren Einstellungen Sie in die Kaspersky Endpoint Security-Richtlinie übertragen möchten. Weiter zum nächsten Schritt

Der Migrations-Assistent beginnt mit der Richtlinienkonvertierung. Während der Richtlinienkonvertierung fordert der Migrations-Assistent Sie auf, die Erklärung zu Kaspersky Security Network zu akzeptieren. Die neuen Richtlinien erhalten den Namen *<Name der Richtlinie> (konvertiert)*.

Schritt 3. Konvertieren von Aufgaben

Überspringen Sie diesen Schritt. Der Assistent unterstützt nur Aufgaben für Kaspersky Endpoint Detection and Response Optimum und Kaspersky Sandbox. Die Verwaltung dieser Komponenten ist nur in der Web Console verfügbar. Weiter zum nächsten Schritt

Schritt 4. Assistent abschließen

Schließen Sie den Assistenten ab. Beim Ausführen des Assistenten wird eine neue Kaspersky Endpoint Security-Richtlinie erstellt.

Endpoint Detection and Response Agent (EDR Agent)

Ab Kaspersky Endpoint Security 12.3 für Windows enthält das Programm eine Konfiguration für Endpoint Detection and Response Agent (EDR Agent). Die App *Endpoint Detection and Response Agent* wird in der IT-Infrastruktur des Unternehmens auf einzelnen Workstations und Servern installiert und unterstützt die folgenden Detection and Response-Lösungen von Kaspersky:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (ab Version 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (ab Version 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (ab Version 12.11)

EDR Agent unterstützt die Integration in die Lösung Kaspersky Endpoint Detection and Response Expert (cloud) nicht.

EDR Agent überwacht auf diesen Computern kontinuierlich alle ausgeführten Prozesse, offenen Netzwerkverbindungen und geänderten Dateien. Die Schutz- und Kontrollkomponenten der App sind für EDR Agent nicht verfügbar.

EDR Agent ist mit Drittanbieter-EPP-Anwendungen kompatibel. Dadurch können Sie neben Detection and Response-Lösungen von Kaspersky auch Infrastruktur-Sicherheitstools von Drittanbietern nutzen.

Um EDR Agent bereitzustellen, muss der Administrationsagent auf dem Computer installiert sein und der Computer muss in der Kaspersky Security Center-Konsole hinzugefügt werden. Damit EDR Agent mit Kaspersky Security Center interagieren kann, müssen Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows installieren. Die Einstellungen von EDR Agent können Sie über eine Gruppenrichtlinie angeben. Um EDR Agent zu integrieren, müssen Sie die Integration in den entsprechenden Richtlinienabschnitten konfigurieren.

Damit Kaspersky Detection and Response unterstützt wird, müssen in der Infrastruktur die folgenden Kaspersky-Anwendungen installiert sein:

	• Administrationsagent • EDR Agent
Endpoint	
	Verwaltungs-Plug-in für Kaspersky Endpoint Security für Windows
Kaspersky Security Center	

Detection and Response-Lösungen: MDR, KATA (EDR), KATA (NDR), KUMA, EDR Expert (on-premises)	

EDR Agent installieren

Kaspersky Endpoint Security wird in der Konfiguration für Endpoint Detection and Response Agent (EDR Agent) für die Kaspersky Detection and Response-Lösungen auf die gleiche Weise installiert.

Um EDR Agent auf dem Computer zu installieren, gibt es folgende Möglichkeiten:

- per Fernzugriff mithilfe von Kaspersky Security Center.
- Lokal mithilfe des Installationsassistenten.
- Lokal in der Befehlszeile (nur für KATA (EDR) und EDR Expert (on-premises)).

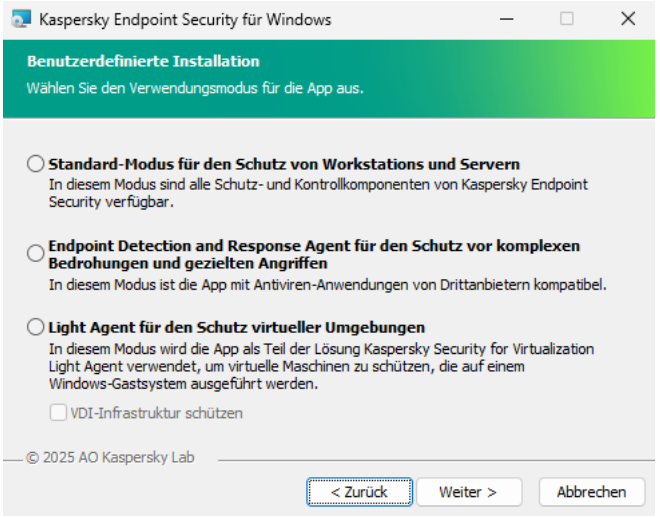
Um EDR Agent zu installieren, müssen Sie in den Einstellungen des Installationspakets oder im Setup-Assistenten die passende Konfiguration auswählen.

So installieren Sie EDR Agent mithilfe des Setup-Assistenten

1. Kopieren Sie den Ordner Lieferumfang auf den Benutzercomputer.
2. Führen Sie setup_kes.exe aus.

   Der Setup-Assistent wird gestartet.

Konfiguration von Kaspersky Endpoint Security



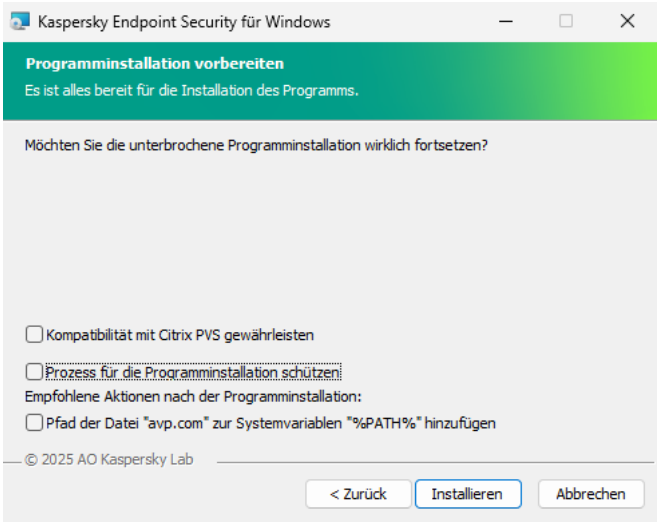
Programmkonfiguration auswählen

Wählen Sie die Konfiguration **Endpoint Detection and Response Agent** aus. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.

Komponenten von Kaspersky Endpoint Security

Wählen Sie die Komponenten aus, die Sie installieren möchten. Nach der Programminstallation können Sie die Auswahl der Komponenten ändern. Dazu müssen Sie den Installationsassistenten erneut starten und den Vorgang zur Änderung der Komponentenauswahl auswählen.

Erweiterte Einstellungen



Erweiterte Installationseinstellungen für das Programm

Prozess für die Programminstallation schützen. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).

Kompatibilität mit Citrix PVS gewährleisten. Sie können die Unterstützung von Citrix Provisioning Services für die Installation von Kaspersky Endpoint Security auf einer virtuellen Maschine aktivieren.

Pfad der Datei "avp.com" zur Systemvariablen "%PATH%" hinzufügen. Sie können den Installationspfad zur Variablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen.

So installieren Sie EDR Agent über die Befehlszeile (nur für KATA (EDR) und EDR Expert (on-premises))

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.

3. Führen Sie den folgenden Befehl aus:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
```

oder

```
msiexec /i <Name des Distributionspakets> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

Dadurch wird die EDR Agent-Anwendung für die Integration mit Kaspersky Anti Targeted Attack Platform (EDR) oder Kaspersky Endpoint Detection and Response Expert (on-premises) auf dem Computer installiert. Mit dem Befehl `status` können Sie überprüfen, ob das Programm installiert ist und welche Programmeinstellungen festgelegt sind.

So installieren Sie EDR Agent über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.
3. Öffnen Sie die Eigenschaften des Installationspakets.

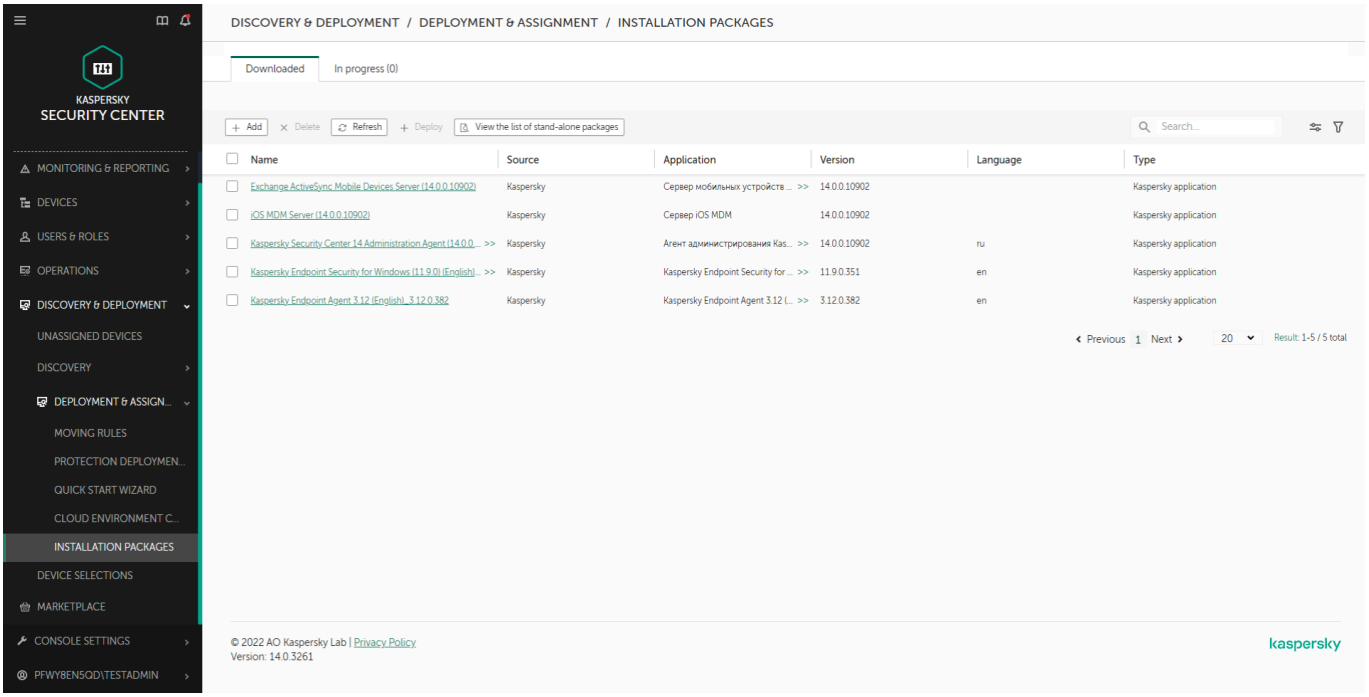
   Erstellen Sie bei Bedarf ein neues Installationspaket.
4. Wechseln Sie zum Abschnitt **Schutzkomponenten**.
5. Wählen Sie die Konfiguration **Endpoint Detection and Response Agent für den Schutz vor komplexen Bedrohungen und gezielten Angriffen** aus. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.
6. Wählen Sie die Komponenten aus, die Sie installieren möchten.

   Nach der Programminstallation können Sie die Auswahl der Komponenten ändern.
7. Speichern Sie die vorgenommenen Änderungen.
8. Erstellen Sie eine Remote-Installationsaufgabe. Wählen Sie in den Aufgabeneigenschaften das von Ihnen erstellte Installationspaket aus.

So installieren Sie EDR Agent über die Web Console

1. Klicken Sie im Web Console-Hauptfenster auf **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**.

Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.



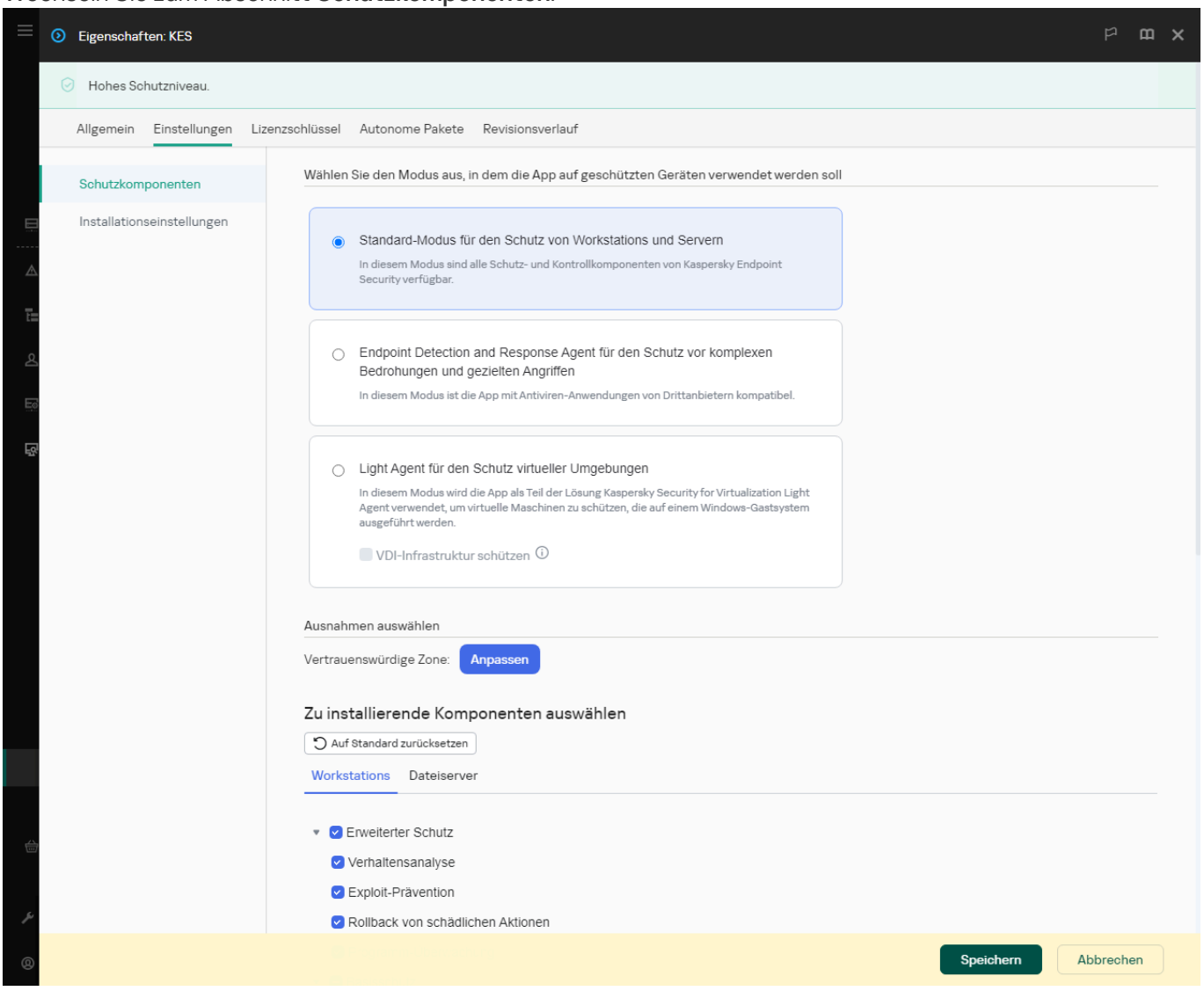
Liste der Installationspakete

2. Öffnen Sie die Eigenschaften des Installationspakets.

   Erstellen Sie bei Bedarf ein neues Installationspaket.

3. Wählen Sie die Registerkarte **Einstellungen** aus.

4. Wechseln Sie zum Abschnitt **Schutzkomponenten**.



Im Installationspaket enthaltene Komponenten

5. Wählen Sie die Konfiguration **Endpoint Detection and Response Agent** aus. In dieser Konfiguration können Sie nur die Komponenten installieren, die die Detection and Response-Lösungen unterstützen: MDR, EDR (KATA), NDR (KATA), EDR Expert (on-premises) und KUMA. Diese Konfiguration ist erforderlich, wenn in Ihrem Unternehmen neben einer Kaspersky Detection and Response-Lösung auch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.

6. Wählen Sie die Komponenten aus, die Sie installieren möchten.

   Nach der Programminstallation können Sie die Auswahl der Komponenten ändern.

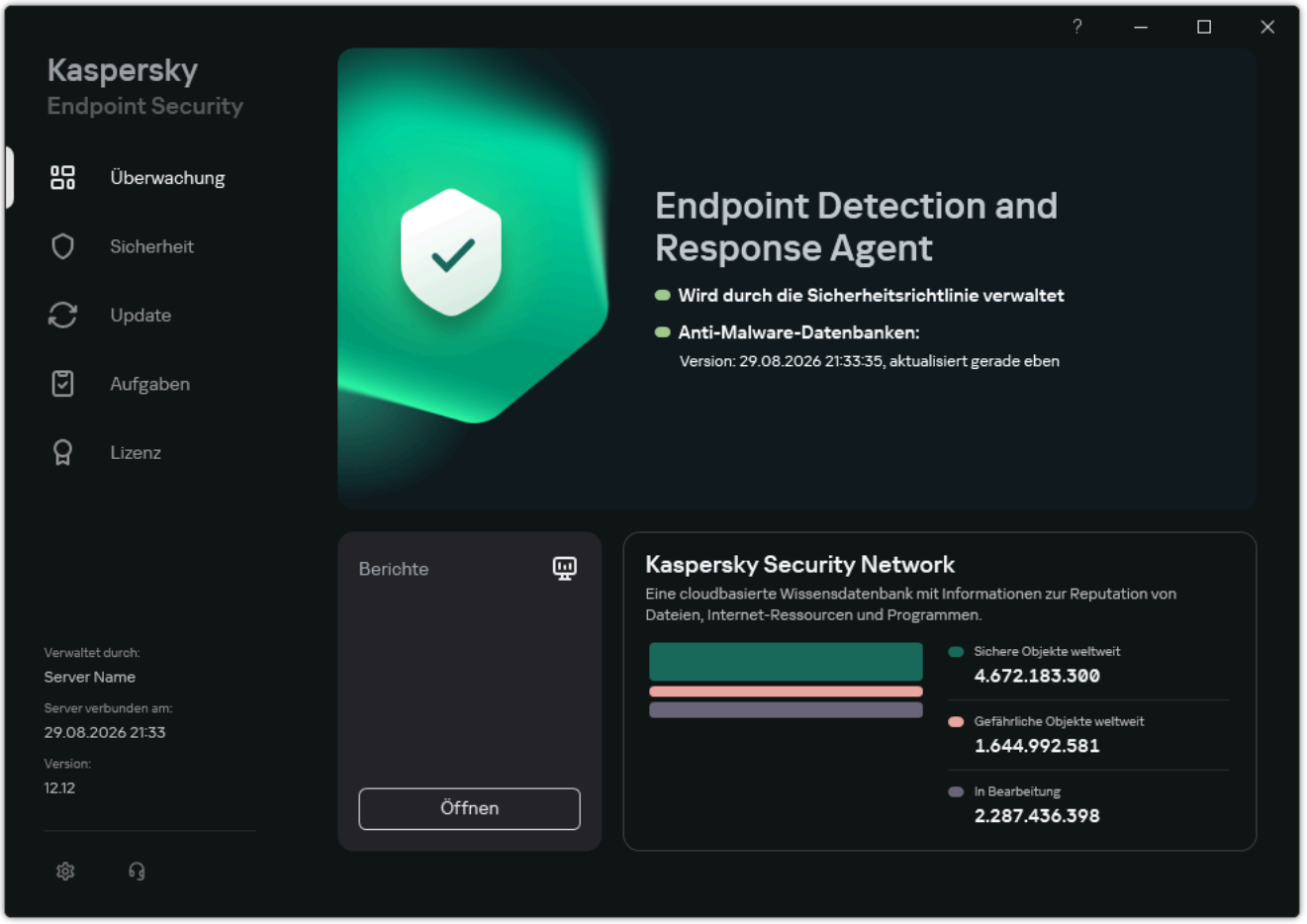
7. Speichern Sie die vorgenommenen Änderungen.

8. Erstellen Sie eine Remote-Installationsaufgabe. Wählen Sie in den Aufgabeneigenschaften das von Ihnen erstellte Installationspaket aus.

Dadurch wird EDR Agent auf dem Benutzercomputer installiert. Sie können die Benutzeroberfläche des Programms verwenden, und im Infobereich wird ein Symbol für das Programm angezeigt .

In Kaspersky Security Center hat der Computer, auf dem das Programm in der EDR Agent-Konfiguration installiert ist, den Status *Kritisch* – . Der Computer hat diesen Status, da die Komponente „Schutz vor bedrohlichen Dateien“ fehlt. Sie müssen nichts unternehmen.

Sollte die Installation von EDR Agent auf einem Computer mit einer Drittanbieter-EPP-Anwendung fehlschlagen, weil das Installationsprogramm auf dem Computer inkompatible Software gefunden hat, können Sie die Überprüfung auf inkompatible Software überspringen.



Hauptfenster von EDR Agent

Jetzt müssen Sie die Integration in die Lösung Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) oder Kaspersky Anti Targeted Attack (NDR) konfigurieren. Sie können auch erweiterte Programmeinstellungen angeben und beispielsweise eine vertrauenswürdige Zone erstellen oder die Benutzeroberfläche des Programms ausblenden. Einstellungen in den folgenden Abschnitten sind verfügbar:

- Kaspersky Security Network
- Programmeinstellungen
- Netzwerkeinstellungen
- Ausnahmen
- Berichte

- Benutzeroberfläche
- Einstellungen verwalten

Integration von EDR Agent in MDR

EDR Agent wird auf Workstations und Servern in der IT-Infrastruktur des Unternehmens installiert. EDR Agent verarbeitet Daten und sendet sie über Kaspersky Security Network-Streams an Kaspersky Managed Detection and Response.

Damit Kaspersky Managed Detection and Response gemeinsam mit dem Administrationsserver über Kaspersky Security Center Web Console funktioniert, müssen Sie eine neue sichere Verbindung (*Hintergrundverbindung*) herstellen. Kaspersky Managed Detection and Response fordert Sie auf, eine Hintergrundverbindung herzustellen, wenn Sie die Lösung bereitstellen. Stellen Sie sicher, dass die Hintergrundverbindung hergestellt wurde.

Erstellung einer Hintergrundverbindung in Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Einstellungen** → **Integration** aus.
2. Wechseln Sie zum Abschnitt **Integration**.
3. Aktivieren Sie den Schalter **Background-Verbindung für die Integration Aktiviert**.
4. Speichern Sie die vorgenommenen Änderungen.

Zur Integration von Kaspersky Managed Detection and Response sind folgende Schritte erforderlich:

1. **Installation der Komponente Managed Detection and Response**

   Sie können die Komponente MDR während der Installation oder beim Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   > Um die Komponente Managed Detection and Response ohne Neustart des Computers mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern* zu installieren, müssen Sie in den Aufgabeneinstellungen die Option **Auf inkompatible Dritthersteller-Programme überprüfen** deaktivieren.

2. **Kaspersky Private Security Network konfigurieren**

   > Überspringen Sie diesen Schritt, wenn Sie „Kaspersky Security Center Cloud Console" verwenden. Kaspersky Security Center Cloud Console konfiguriert Kaspersky Private Security Network automatisch, wenn das MDR-Plug-in installiert wird.

   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.

   Laden Sie in den Eigenschaften des Administrationsservers die Konfigurationsdatei von Kaspersky Security Network hoch. Die Konfigurationsdatei von Kaspersky Security Network 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 über die Konfiguration von Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center. Die Konfigurationsdatei von Kaspersky Security Network kann auch über die Befehlszeile auf den Computer hochgeladen werden (siehe Anleitung unten).

So konfigurieren Sie Kaspersky Private Security Network über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

   ```
   avp.com KSN /private <file name>
   ```

   wobei `<file name>` der Name der Konfigurationsdatei ist, welche die Einstellungen für Kaspersky Private Security Network enthält (Dateiformat PKCS7 oder PEM).

   Beispiel:
   ```
   avp.com KSN /private C:\kpsn_config.pkcs7
   ```

Künftig verwendet Kaspersky Endpoint Security das Kaspersky Private Security Network, um die Reputation von Dateien, Programmen und Websites zu ermitteln. Im Abschnitt **Kaspersky Security Network** der Richtlinieneinstellungen wird der folgende Betriebsstatus angezeigt: *Infrastruktur: Kaspersky Private Security Network*.

Sie müssen den erweiterten KSN-Modus aktivieren, damit „Managed Detection and Response“ funktioniert.

3 Aktivieren von Kaspersky Managed Detection and Response

Ab Kaspersky Endpoint Security für Windows 12.10 können Sie die Funktionalität „Managed Detection and Response“ auch mit einem Schlüsseldatei aktivieren (anstatt mit einem Aktivierungscodes).

Sie müssen eine separate Lizenz für MDR erwerben (Add-on für Kaspersky Managed Detection and Response).

Die Funktionalität ist verfügbar, nachdem ein separater Schlüssel für das Kaspersky Managed Detection and Response-Add-on hinzugefügt wurde. Die Lizenzverwaltung für die eigenständige Funktionalität von Managed Detection and Response entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

Stellen Sie sicher, dass die MDR-Funktionalität in der Lizenz enthalten ist und dass sie auf der lokalen App-Oberfläche funktioniert.

4 Aktivieren der Komponente „Managed Detection and Response“

Laden Sie die BLOB-Konfigurationsdatei in die Richtlinie von Kaspersky Endpoint Security (siehe Anleitung unten). 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“.

Ab Kaspersky Endpoint Security 12.6 für Windows ist das Hinzufügen einer BLOB-Datei für Kaspersky Managed Detection and Response ohne Mandanten optional, wenn Sie über eine aktuelle Lizenz verfügen.

So aktivieren Sie die Komponente „Managed Detection and Response“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** aus.

4. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response (Industrial CyberSecurity)**.

5. Klicken Sie im Block **Einstellungen** auf **Hochladen** und wählen Sie die BLOB-Datei aus, die in der Konsole von Kaspersky Managed Detection and Response empfangen wurde. Die Datei hat die Erweiterung p7.

   Der Benutzer ist standardmäßig berechtigt, die Programmeinstellungen zu verwalten (das „Vorhängeschloss“ ist geöffnet). Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Komponente „Managed Detection and Response“ über „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten → Managed Detection and Response**.

5. Aktivieren Sie den Schalter **Managed Detection and Response AKTIVIERT**.

6. Klicken Sie auf **Hochladen** und wählen Sie die BLOB-Datei aus, die über die Konsole von Kaspersky Managed Detection and Response abgerufen wurde. Die Datei hat die Erweiterung p7.

   Der Benutzer ist standardmäßig berechtigt, die Richtlinieneinstellungen zu verwalten (das „Vorhängeschloss“ ist geöffnet). Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Komponente „Managed Detection and Response“ über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.

2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

3. Führen Sie den folgenden Befehl aus:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **App-Einstellungen anpassen** besitzen.

Daraufhin verifiziert Kaspersky Endpoint Security die BLOB-Datei. Zur Verifizierung der BLOB-Datei gehört auch die Überprüfung der digitalen Signatur und der Gültigkeitsdauer der Lizenz. Wenn die BLOB-Datei erfolgreich verifiziert wurde, lädt Kaspersky Endpoint Security die Datei herunter und sendet sie bei der nächsten Synchronisierung mit Kaspersky Security Center an den Computer. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Managed Detection and Response** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

5. **Andere Programmkomponenten für den Empfang von Telemetriedaten konfigurieren**

   Sie müssen die folgenden Komponenten aktivieren, damit „Managed Detection and Response“ funktioniert:

   - Kaspersky Security Network (erweiterter Modus).
   - Verhaltensanalyse.
   - Exploit-Prävention.
   - Schutz vor Web-Bedrohungen.
   - Schutz vor E-Mail-Bedrohungen.
   - Schutz vor bedrohlichen Dateien.
   - Schutz vor Netzwerkbedrohungen.
   - Firewall.
   - AMSI-Schutz.
   - Untersuchung im Hintergrund.

     1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
     2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

        Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
     3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
     4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Managed Detection and Response**.
     5. Aktivieren Sie den Schalter **Managed Detection and Response AKTIVIERT**.
     6. Speichern Sie die vorgenommenen Änderungen.

     1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
     2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
     3. Wählen Sie im Richtlinienfenster **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** aus.

4. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response (Industrial CyberSecurity)**.

5. Speichern Sie die vorgenommenen Änderungen.

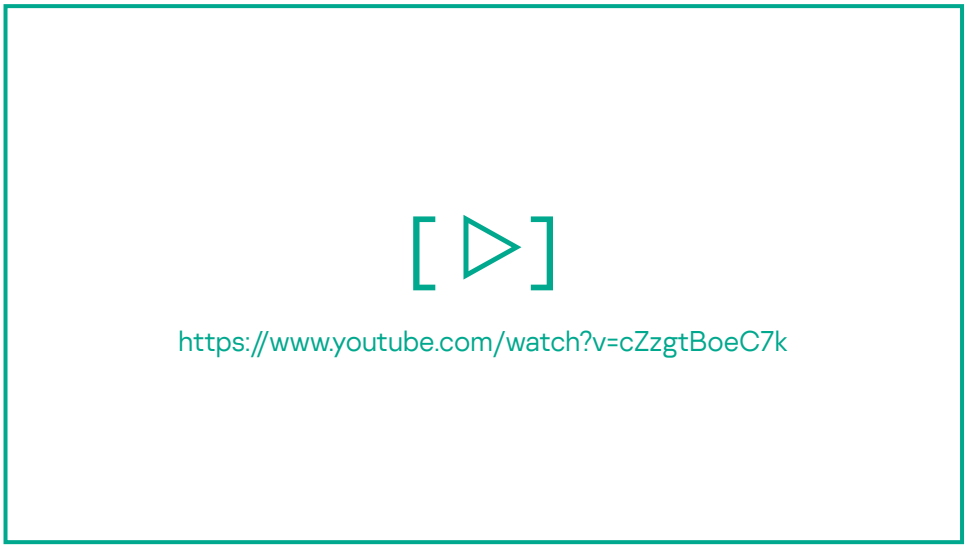
Integration von EDR Agent in EDR (KATA)

EDR Agent wird auf Workstations und Servern in der IT-Infrastruktur des Unternehmens installiert. Auf diesen Computern überwacht EDR Agent kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien und sendet über die Central Node-Komponente Überwachungsdaten an den Server.

Für die Integration in EDR (KATA) müssen Sie die Komponente Endpoint Detection and Response (KATA) aktivieren und EDR Agent konfigurieren.

Damit Endpoint Detection and Response (KATA) funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Anti Targeted Attack Platform Versionen 5.0–7.1.
- Kaspersky Security Center Version 14.2 oder höher. In älteren Versionen von Kaspersky Security Center kann die Funktion Endpoint Detection and Response (KATA) nicht aktiviert werden.



Die Integration in Endpoint Detection and Response (KATA) umfasst die folgenden Schritte:

1. **Aktivieren von Endpoint Detection and Response (KATA)**

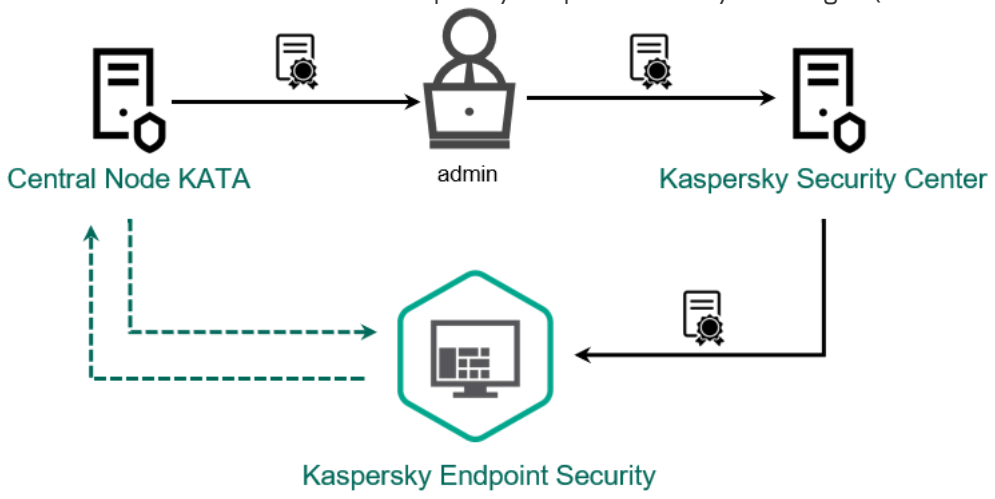
   Sie müssen eine separate Lizenz für EDR (KATA) kaufen (Add-on für Kaspersky Endpoint Detection and Response (KATA)).

   Die Funktionalität ist verfügbar, sobald ein separater Schlüssel für Kaspersky Endpoint Detection and Response (KATA) hinzugefügt wird. Die Lizenzverwaltung für die eigenständige Funktionalität von Endpoint Detection and Response (KATA) entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität von EDR (KATA) in der Lizenz enthalten ist und in der lokalen App-Oberfläche ausgeführt wird.

2. **Verbindung zu Central Node**

Kaspersky Anti Targeted Attack Platform erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und der Komponente Central Node. Zur Konfiguration einer vertrauenswürdigen Verbindung müssen Sie ein TLS-Zertifikat verwenden. 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). Anschließend müssen Sie das TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen (siehe Anleitung unten).



TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen

Standardmäßig überprüft Kaspersky Endpoint Security nur das TLS-Zertifikat des Central Node. Um die Verbindung sicherer zu machen, können Sie zusätzlich die Überprüfung des Computers auf dem Central Node (Zwei-Wege-Authentifizierung) aktivieren. Zum Aktivieren dieser Überprüfung müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Central Node und Kaspersky Endpoint Security aktivieren. Zur Verwendung der Zwei-Wege-Authentifizierung benötigen Sie außerdem einen Krypto-Container. 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).

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Verwaltungskonsole (MMC) mit Central Node

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Detection and Response → Endpoint Detection and Response Expert (on-premises)** aus.
5. Aktivieren Sie das Kontrollkästchen **Endpoint Detection and Response Expert (on-premises)**.
6. Klicken Sie auf **Einstellungen der Serververbindung**.
7. Konfigurieren Sie die Serververbindung:
   - **Timeout (Sek)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.
   - **TLS-Zertifikat des Servers**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).

- **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

  Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

8. Klicken Sie auf **OK**.
9. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

   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.
10. Konfigurieren Sie, falls erforderlich, die Telemetrie.
11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Web Console mit Central Node

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.
5. Aktivieren Sie den Schalter **Endpoint Detection and Response Expert (On-Premises) AKTIVIERT**.
6. Um EDR (KATA) zu konfigurieren, wählen in der Liste der Lösungen den Punkt **Endpoint Detection and Response Expert (Version 7.1 oder älter)** aus.
7. Klicken Sie auf **Verbindungseinstellungen**.

8. Konfigurieren Sie die Serververbindung:

   - **Timeout (Sek.)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.

   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).

   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

     Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

9. Klicken Sie auf **OK**.

10. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

    Sie können mehrere Serveradressen für Central Node hinzufügen. Kaspersky Endpoint Security versucht, sich über die erste IP-Adresse mit dem Server zu verbinden. Wenn keine Verbindung hergestellt werden kann, versucht Kaspersky Endpoint Security eine Verbindung mit der zweiten IP-Adresse in der Liste und so weiter.

11. Konfigurieren Sie, falls erforderlich, die Telemetrie.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Dadurch wird der Computer zur Kaspersky Anti Targeted Attack Platform-Konsole hinzugefügt. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Endpoint Detection and Response Expert (on-premises)** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Integration von EDR Agent in NDR (KATA)

EDR Agent wird auf Workstations und Servern in der IT-Infrastruktur des Unternehmens installiert. Auf diesen Computern überwacht EDR Agent kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien und sendet über die Central Node-Komponente Überwachungsdaten an den Server.

Für die Integration in NDR (KATA) müssen Sie die Komponente Network Detection and Response (KATA) aktivieren und EDR Agent konfigurieren.

Damit Network Detection and Response (KATA) funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Anti Targeted Attack Platform Version 7.0 oder höher.
- Kaspersky Security Center Version 14.2 oder höher. In älteren Versionen von Kaspersky Security Center kann die Funktion Network Detection and Response (KATA) nicht aktiviert werden.

https://www.youtube.com/watch?v=gd-rySv0ThQ

Die Integration in Network Detection and Response (KATA) umfasst die folgenden Schritte:

1. **Aktivieren von Network Detection and Response (KATA)**

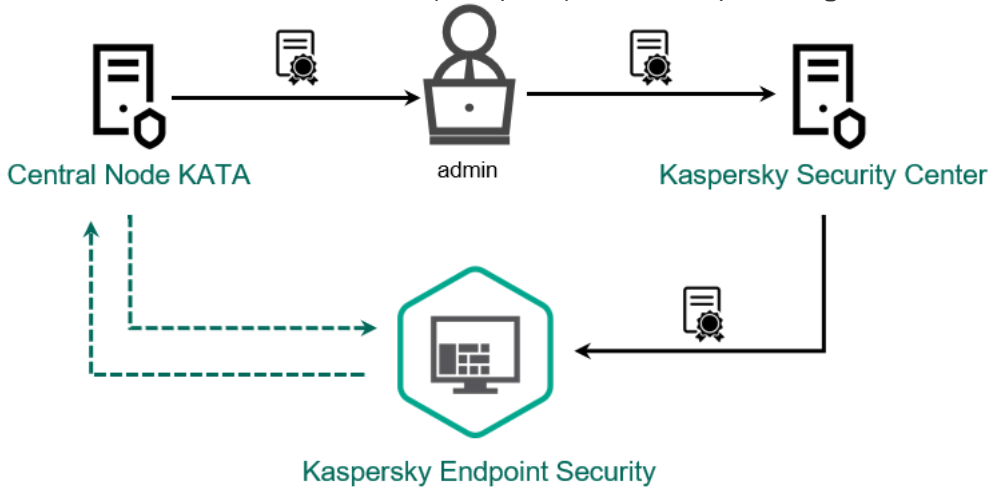
   Sie müssen eine separate Lizenz für NDR (KATA) kaufen (Add-on für Kaspersky Network Detection and Response (KATA)).

   Die Funktionalität ist verfügbar, sobald ein separater Schlüssel für Kaspersky Network Detection and Response (KATA) hinzugefügt wird. Die Lizenzverwaltung für die eigenständige Funktionalität von Network Detection and Response (KATA) entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität von NDR (KATA) in der Lizenz enthalten ist und in der lokalen App-Oberfläche ausgeführt wird.

2. **Verbindung zu Central Node**

   Kaspersky Anti Targeted Attack Platform erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und der Komponente Central Node. Zur Konfiguration einer vertrauenswürdigen Verbindung müssen Sie ein TLS-Zertifikat verwenden. 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). Anschließend müssen Sie das TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen (siehe Anleitung unten).



TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen

Standardmäßig überprüft Kaspersky Endpoint Security nur das TLS-Zertifikat des Central Node. Um die Verbindung sicherer zu machen, können Sie zusätzlich die Überprüfung des Computers auf dem Central Node (Zwei-Wege-Authentifizierung) aktivieren. Zum Aktivieren dieser Überprüfung müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Central Node und Kaspersky Endpoint Security aktivieren. Zur Verwendung der Zwei-Wege-Authentifizierung benötigen Sie außerdem einen Krypto-Container. 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).

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Verwaltungskonsole (MMC) mit Central Node

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Detection and Response → Network Detection and Response (KATA)** aus.
4. Aktivieren Sie das Kontrollkästchen **Network Detection and Response (KATA)**.
5. Klicken Sie auf **Verbindungseinstellungen**.
6. Konfigurieren Sie die Serververbindung:
   - **Timeout (Sek.)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.
   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).
   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

     Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.
7. Klicken Sie auf **OK**.
8. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

9. 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.

10. Konfigurieren Sie, falls erforderlich, die Telemetrie.

11. Speichern Sie die vorgenommenen Änderungen.

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Web Console mit Central Node

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Network Detection and Response (KATA)**.

5. Aktivieren Sie den Schalter **Network Detection and Response (KATA) AKTIVIERT**.

6. Klicken Sie auf **Verbindungseinstellungen**.

7. Konfigurieren Sie die Serververbindung:

   - **Timeout (Sek.)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.

   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).

   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

     Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

8. Klicken Sie auf **OK**.

9. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

10. Sie können mehrere Serveradressen für Central Node hinzufügen. Kaspersky Endpoint Security versucht, sich über die erste IP-Adresse mit dem Server zu verbinden. Wenn keine Verbindung hergestellt werden kann, versucht Kaspersky Endpoint Security eine Verbindung mit der zweiten IP-Adresse in der Liste und so weiter.

11. Konfigurieren Sie, falls erforderlich, die Telemetrie.

12. Speichern Sie die vorgenommenen Änderungen.

Dadurch wird der Computer zur Kaspersky Anti Targeted Attack Platform-Konsole hinzugefügt. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Network Detection and Response (KATA)** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Integration von EDR Agent in EDR Expert (on-premises)

EDR Agent wird auf Workstations und Servern in der IT-Infrastruktur des Unternehmens installiert. Auf diesen Computern überwacht EDR Agent kontinuierlich Prozesse, offene Netzwerkverbindungen sowie geänderte Dateien und sendet Überwachungsdaten an den Server von EDR Expert (on-premises).

Zur Integration in EDR Expert (on-premises) müssen Sie die Komponente „Endpoint Detection and Response Expert (on-premises)“ aktivieren und EDR Agent konfigurieren.

Die Integration in Endpoint Detection and Response (on-premises) umfasst die folgenden Schritte:

1. **Kaspersky Endpoint Detection and Response Expert (on-premises) aktivieren**

   Sie müssen eine separate Lizenz für EDR Expert (on-premises) kaufen (Add-on für Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Die Funktionalität ist verfügbar, sobald ein separater Schlüssel für Kaspersky Endpoint Detection and Response (on-premises) hinzugefügt wird. Die Lizenzverwaltung für die eigenständige Funktionalität von Endpoint Detection and Response (on-premises) entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität von EDR Expert (on-premises) in der Lizenz enthalten ist und in der lokalen Benutzeroberfläche des Programms ausgeführt wird.

2. **Verbindung mit dem Telemetrie-Erfassungsserver und dem Reaktionsserver herstellen**

   Kaspersky Endpoint Detection and Response Expert (on-premises) erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und zwei Servern:

   - Ein *Telemetrie-Erfassungsserver* ist Teil einer SIEM-Lösung, die Informationen über auf dem Computer auftretende Ereignisse sammelt, normalisiert, korreliert, analysiert und speichert.

   - Ein *Reaktionsserver* ist ein Server, der Daten empfängt und sendet, das Verhalten von Objekten analysiert und die Ergebnisse solcher Untersuchungen veröffentlicht.

   Zur Konfiguration einer vertrauenswürdigen Verbindung müssen Sie ein TLS-Zertifikat verwenden. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Anschließend müssen Sie das TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen (siehe Anleitung unten).

Standardmäßig überprüft Kaspersky Endpoint Security nur das TLS-Zertifikat der Server. Um die Verbindung sicherer zu machen, können Sie zusätzlich die Überprüfung des Computers auf dem Server aktivieren (Zwei-Wege-Authentifizierung). Um diese Überprüfung zu aktivieren, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers und von Kaspersky Endpoint Security aktivieren. Zur Verwendung der Zwei-Wege-Authentifizierung benötigen Sie außerdem einen Krypto-Container. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, mit EDR Expert (on-premises) (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.
5. Aktivieren Sie den Schalter **Endpoint Detection and Response Expert (On-Premises) AKTIVIERT**.
6. Um EDR Expert (on-premises) zu konfigurieren, wählen in der Liste der Lösungen den Punkt **Endpoint Detection and Response Expert (ab Version 8.0)** aus.
7. Konfigurieren Sie die Verbindung mit den *Telemetrie-Erfassungsservern*:

   a. Klicken Sie im Block **Verbindung mit Telemetrie-Erfassungsservern** auf den Link **Verbindungseinstellungen**.

   b. Konfigurieren Sie die Verbindung mit den Telemetrie-Erfassungsservern:

   - **Timeout (Sek.)**. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden.
   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers 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. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Nachdem Sie die Server-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.

   c. Klicken Sie auf **OK**.

d. Fügen Sie Telemetrie-Erfassungsserver hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

Sie können mehrere Adressen für 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.

e. Konfigurieren Sie, falls erforderlich, die Telemetrie.

8. Konfigurieren Sie die Verbindung mit den *Reaktionsservern*:

a. Konfigurieren Sie im Block **Verbindung mit Reaktionsservern** die Einstellung **Synchronisierungsanfrage an Server senden alle (Min.)**: Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung empfängt Kaspersky Endpoint Security Aufgaben zur Reaktion auf Bedrohungen und sendet Aufgabenergebnisse.

b. Klicken Sie auf den Link **Verbindungseinstellungen**.

c. Konfigurieren Sie die Verbindung mit den Reaktionsservern:

- **Timeout (Sek.)**. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden.
- **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers 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. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Nachdem Sie die Server-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.

d. Klicken Sie auf **OK**.

e. Fügen Sie Reaktionsserver hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

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.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Daraufhin wird der Computer zur Open Single Management Platform (OSMP) hinzugefügt. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Endpoint Detection and Response Expert (on-premises)** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Kompatibilität mit Drittanbieter-EPP-Anwendungen

EDR Agent unterstützt die Funktionalität der Kaspersky Detection and Response-Lösungen. Schutz- und Kontrollkomponenten sind für EDR Agent nicht verfügbar. Mit dieser Konfiguration können Sie in der Unternehmensinfrastruktur Drittanbieter-EPP-Anwendungen installieren und Kaspersky Detection and Response-Lösungen bereitstellen.

EDR Agent ist mit EPP-Anwendungen der folgenden Anbieter kompatibel:

- **Dr.Web**

  EDR Agent ist kompatibel mit Dr.Web Agent für Windows Version 13 und mit Dr.Web Server (x64) 13.0.0.10200.

- **Dallas Lock**

  EDR Agent ist kompatibel mit Dallas Lock 8.0-C Version 843.2.

  Damit EDR Agent auf einem Computer ausgeführt werden kann, auf dem die Software Dallas Lock installiert ist, müssen Sie die Verbindung mit externen Kaspersky-Diensten in den Einstellungen des Firewall-Moduls zulassen.

- **Secret Net Studio**

  EDR Agent ist kompatibel mit Secret Net Studio Version 8.11 (20851).

  Die Anwendung kann nicht auf einem Computer installiert werden, auf dem Secret Net Studio mit der Antivirus-Komponente bereitgestellt ist. Um die Interoperabilität zu ermöglichen, müssen Sie die Antivirus-Komponente aus Secret Net Studio entfernen.

- **Trend Micro**

  EDR Agent ist kompatibel mit Trend Micro Vision One (einschließlich Security Agent Version 14.0.20731).

  EDR Agent ist kompatibel mit Trend Micro Deep Security Version 20.0.3-18160 (einschließlich Security Agent).

- **Windows Defender**

- **Sophos**

  EDR Agent ist kompatibel mit Sophos Intercept X Version 2024.1.2 (einschließlich Endpoint Agent) und mit Sophos Core Agent Version 2026.2.1.3.

- **Bitdefender**

  EDR Agent ist kompatibel mit Bitdefender Endpoint Security Tools Version 8.26.7.647.

- **ESET**

  EDR Agent ist kompatibel mit ESET Endpoint Security Version 13.0.2044.0 und mit ESET Management Agent Version 13.2.1189.0.

Auf Computern mit Windows 11 für Arm64 ist EDR Agent nicht kompatibel mit Bitdefender Endpoint Security Tools.

Die Anwendungen müssen in der folgenden Reihenfolge installiert werden: Installieren Sie zuerst die EPP-Anwendung, dann den Kaspersky Security Center-Administrationsagenten und anschließend EDR Agent. Diese Reihenfolge ist erforderlich, da das Installationsprogramm der EPP-Anwendung EDR Agent und den Administrationsagenten möglicherweise als inkompatible Software erkennt und diese entfernt. Wenn die EPP-Anwendung eines Drittanbieters künftig aktualisiert wird, muss der Betrieb von EDR Agent und des Administrationsagenten überprüft werden, da das Installationsprogramm auf dem Computer möglicherweise erneut nach inkompatibler Software sucht und die genannten Anwendungen entfernt.

Sollte die Installation von EDR Agent auf einem Computer mit einer Drittanbieter-EPP-Anwendung fehlschlagen, weil das Installationsprogramm auf dem Computer inkompatible Software gefunden hat, können Sie die Überprüfung auf inkompatible Software überspringen.

Managed Detection and Response

Kaspersky Endpoint Security für Windows 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“.

Konfigurationen von Kaspersky Endpoint Security für die Integration in MDR

Die folgenden Konfigurationen können für die Arbeit mit MDR verwendet werden:

- **[KES+built-in agent]**. In dieser Konfiguration dient Kaspersky Endpoint Security sowohl als Programm, das die Sicherheit des Computers gewährleistet, als auch als Programm für die Interaktion mit MDR.

- **[third-party EPP+EDR Agent]**. In dieser Konfiguration wird die Sicherheit der IT-Infrastruktur durch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt. In der Konfiguration Endpoint Detection and Response Agent (EDR Agent) wird die Interaktion mit MDR durch Kaspersky Endpoint Security gewährleistet. In dieser Konfiguration ist EDR Agent mit Drittanbieter-EPP-Anwendungen kompatibel.

Integration des integrierten Agenten in MDR

Um die Integration mit Kaspersky Managed Detection and Response einzurichten, müssen Sie die Managed Detection and Response-Komponente aktivieren und Kaspersky Endpoint Security konfigurieren.

Damit Kaspersky Managed Detection and Response gemeinsam mit dem Administrationsserver über Kaspersky Security Center Web Console funktioniert, müssen Sie eine neue sichere Verbindung (*Hintergrundverbindung*) herstellen. Kaspersky Managed Detection and Response fordert Sie auf, eine Hintergrundverbindung herzustellen, wenn Sie die Lösung bereitstellen. Stellen Sie sicher, dass die Hintergrundverbindung hergestellt wurde.

Erstellung einer Hintergrundverbindung in Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Einstellungen** → **Integration** aus.
2. Wechseln Sie zum Abschnitt **Integration**.
3. Aktivieren Sie den Schalter **Background-Verbindung für die Integration Aktiviert**.
4. Speichern Sie die vorgenommenen Änderungen.

Zur Integration von Kaspersky Managed Detection and Response sind folgende Schritte erforderlich:

1. **Installation der Komponente Managed Detection and Response**

   Sie können die Komponente MDR während der Installation oder beim Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   > Um die Komponente Managed Detection and Response ohne Neustart des Computers mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern* zu installieren, müssen Sie in den Aufgabeneinstellungen die Option **Auf inkompatible Dritthersteller-Programme überprüfen** deaktivieren.

2. **Kaspersky Private Security Network konfigurieren**

   > Überspringen Sie diesen Schritt, wenn Sie „Kaspersky Security Center Cloud Console" verwenden. Kaspersky Security Center Cloud Console konfiguriert Kaspersky Private Security Network automatisch, wenn das MDR-Plug-in installiert wird.

   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.

   Laden Sie in den Eigenschaften des Administrationsservers die Konfigurationsdatei von Kaspersky Security Network hoch. Die Konfigurationsdatei von Kaspersky Security Network 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 über die Konfiguration von Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center. Die Konfigurationsdatei von Kaspersky Security Network kann auch über die Befehlszeile auf den Computer hochgeladen werden (siehe Anleitung unten).

   So konfigurieren Sie Kaspersky Private Security Network über die Befehlszeile

   1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
   2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
   3. Führen Sie den folgenden Befehl aus:

      ```
      avp.com KSN /private <file name>
      ```

wobei `<file name>` der Name der Konfigurationsdatei ist, welche die Einstellungen für Kaspersky Private Security Network enthält (Dateiformat PKCS7 oder PEM).

Beispiel:
`avp.com KSN /private C:\kpsn_config.pkcs7`

Künftig verwendet Kaspersky Endpoint Security das Kaspersky Private Security Network, um die Reputation von Dateien, Programmen und Websites zu ermitteln. Im Abschnitt **Kaspersky Security Network** der Richtlinieneinstellungen wird der folgende Betriebsstatus angezeigt: *Infrastruktur: Kaspersky Private Security Network*.

Sie müssen den erweiterten KSN-Modus aktivieren, damit „Managed Detection and Response“ funktioniert.

3 Aktivieren von Kaspersky Managed Detection and Response

Ab Kaspersky Endpoint Security für Windows 12.10 können Sie die Funktionalität „Managed Detection and Response“ auch mit einem Schlüsseldatei aktivieren (anstatt mit einem Aktivierungscodes).

Kaspersky Managed Detection and Response unterstützt die folgenden Lizenzierungsmethoden:

- Die Funktionalität von Managed Detection and Response wird durch die Lizenz für Kaspersky Endpoint Security für Windows abgedeckt.

  Die Funktionalität steht nach der Aktivierung von Kaspersky Endpoint Security für Windows sofort zur Verfügung.

- Eine separate Lizenz für MDR (Add-on für Kaspersky Managed Detection and Response) wird verwendet.

  Die Funktionalität ist verfügbar, nachdem ein separater Schlüssel für das Kaspersky Managed Detection and Response-Add-on hinzugefügt wurde. Dadurch werden zwei Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security und ein Schlüssel für Kaspersky Managed Detection and Response.

  Die Lizenzverwaltung für die eigenständige Funktionalität von Managed Detection and Response entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

Stellen Sie sicher, dass die MDR-Funktionalität in der Lizenz enthalten ist und dass sie auf der lokalen App-Oberfläche funktioniert.

4 Aktivieren der Komponente „Managed Detection and Response“

Laden Sie die BLOB-Konfigurationsdatei in die Richtlinie von Kaspersky Endpoint Security (siehe Anleitung unten). 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“.

Ab Kaspersky Endpoint Security 12.6 für Windows ist das Hinzufügen einer BLOB-Datei für Kaspersky Managed Detection and Response ohne Mandanten optional, wenn Sie über eine aktuelle Lizenz verfügen.

So aktivieren Sie die Komponente „Managed Detection and Response“ über die Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Wählen Sie im Richtlinienfenster **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)** aus.

4. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response (Industrial CyberSecurity)**.

5. Klicken Sie im Block **Einstellungen** auf **Hochladen** und wählen Sie die BLOB-Datei aus, die in der Konsole von Kaspersky Managed Detection and Response empfangen wurde. Die Datei hat die Erweiterung p7.

   Der Benutzer ist standardmäßig berechtigt, die Programmeinstellungen zu verwalten (das „Vorhängeschloss“ ist geöffnet). Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Komponente „Managed Detection and Response“ über „Web Console“ und „Cloud Console“

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten → Managed Detection and Response**.

5. Aktivieren Sie den Schalter **Managed Detection and Response AKTIVIERT**.

6. Klicken Sie auf **Hochladen** und wählen Sie die BLOB-Datei aus, die über die Konsole von Kaspersky Managed Detection and Response abgerufen wurde. Die Datei hat die Erweiterung p7.

   Der Benutzer ist standardmäßig berechtigt, die Richtlinieneinstellungen zu verwalten (das „Vorhängeschloss“ ist geöffnet). Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Komponente „Managed Detection and Response“ über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.

2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

3. Führen Sie den folgenden Befehl aus:

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **App-Einstellungen anpassen** besitzen.

Daraufhin verifiziert Kaspersky Endpoint Security die BLOB-Datei. Zur Verifizierung der BLOB-Datei gehört auch die Überprüfung der digitalen Signatur und der Gültigkeitsdauer der Lizenz. Wenn die BLOB-Datei erfolgreich verifiziert wurde, lädt Kaspersky Endpoint Security die Datei herunter und sendet sie bei der nächsten Synchronisierung mit Kaspersky Security Center an den Computer. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Managed Detection and Response** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

5. **Andere Programmkomponenten für den Empfang von Telemetriedaten konfigurieren**

   Sie müssen die folgenden Komponenten aktivieren, damit „Managed Detection and Response“ funktioniert:

   - Kaspersky Security Network (erweiterter Modus).
   - Verhaltensanalyse.
   - Exploit-Prävention.
   - Schutz vor Web-Bedrohungen.
   - Schutz vor E-Mail-Bedrohungen.
   - Schutz vor bedrohlichen Dateien.
   - Schutz vor Netzwerkbedrohungen.
   - Firewall.
   - AMSI-Schutz.
   - Untersuchung im Hintergrund.

   1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Managed Detection and Response**.
   5. Aktivieren Sie den Schalter **Managed Detection and Response AKTIVIERT**.
   6. Speichern Sie die vorgenommenen Änderungen.

   1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
   2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
   3. Wählen Sie im Richtlinienfenster **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)** aus.

4. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response (Industrial CyberSecurity)**.

5. Speichern Sie die vorgenommenen Änderungen.

Leitfaden zur Migration von KEA zu KES für MDR

Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten für die Lösung Kaspersky Managed Detection and Response. Sie benötigen Kaspersky Endpoint Agent nicht mehr als separate Anwendung, um mit MDR zu arbeiten. Alle Funktionen von Kaspersky Endpoint Agent werden von Kaspersky Endpoint Security ausgeführt.

Wenn Sie Kaspersky Endpoint Security auf Computern bereitstellen, auf denen Kaspersky Endpoint Agent installiert ist, funktioniert die Kaspersky Managed Detection and Response-Lösung weiterhin mit Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt. Das System verhält sich gleich, wenn Sie Kaspersky Endpoint Security auf Version 11.6.0 oder höher aktualisieren.

> Kaspersky Endpoint Security ist nicht mit Kaspersky Endpoint Agent kompatibel. Sie können diese beiden Apps nicht mehr auf demselben Computer installieren.

Damit Kaspersky Endpoint Security als Teil von Kaspersky Managed Detection and Response funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Security Center Version 13.2 oder höher (einschließlich Administrationsagent). In älteren Versionen von Kaspersky Security Center kann die Managed Detection and Response-Funktion nicht aktiviert werden.
- Es wird eine Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver hergestellt. Damit MDR mit dem Administrationsserver über Kaspersky Security Center Web Console funktioniert, müssen Sie eine neue sichere *Hintergrundverbindung* herstellen.

Schritte für die Migration der Konfiguration [KES+KEA] zu [KES+built-in agent] für MDR

1. **Upgrade des Verwaltungs-Plug-ins für Kaspersky Endpoint Security**

   Die Komponente MDR kann mit dem Verwaltungs-Plug-in von Kaspersky Endpoint Security Version 11.6 oder höher verwaltet werden. Je nachdem, welchen Konsolentyp von Kaspersky Security Center sie verwenden, aktualisieren Sie das Verwaltungs-Plug-in in der Verwaltungskonsole (MMC) oder das Web-Plug-in in der Web Console.

2. **Migration von Richtlinien und Aufgaben**

   Übertragen Sie die Einstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security für Windows. Folgende Varianten stehen zur Auswahl:

   - Ein Assistent für die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security. Der Assistent für die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security funktioniert nur in Web Console

     So migrieren Sie Richtlinien- und Aufgabeneinstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security über die Web Console

     Wählen Sie im „Web Console"-Hauptfenster den Punkt **Vorgänge → Migration von Kaspersky Endpoint Agent** aus.

Dadurch wird der Migrations-Assistent für Richtlinien und Aufgaben ausgeführt. Folgen Sie den Anweisungen.

Schritt 1. Migration der Richtlinien

Der Migrationsassistent erstellt eine neue Richtlinie, die die Einstellungen der Richtlinien von Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammenführt. Wählen Sie in der Richtlinienliste jene Richtlinien von Kaspersky Endpoint Agent aus, deren Einstellungen Sie mit der Richtlinie von Kaspersky Endpoint Security zusammenführen möchten. Klicken Sie auf eine Richtlinie von Kaspersky Endpoint Agent, um die Richtlinie von Kaspersky Endpoint Security auszuwählen, mit der Sie die Einstellungen zusammenführen möchten. Stellen Sie sicher, dass Sie die korrekten Richtlinien ausgewählt haben, und gehen Sie weiter zum nächsten Schritt

Schritt 2. Aufgabenmigration

Der Migrations-Assistent unterstützt keine MDR-Aufgaben. Überspringen Sie diesen Schritt.

Schritt 3. Assistent abschließen

Schließen Sie den Assistenten ab. Beim Ausführen des Assistenten wird eine neue Kaspersky Endpoint Security-Richtlinie erstellt. Die Richtlinie führt Einstellungen Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammen. Die Richtlinie heißt *<Kaspersky Endpoint Security-Richtlinienname> & <Kaspersky Endpoint Agent-Richtlinienname>*. Die neue Richtlinie hat den Status *Inaktiv*. Um fortzufahren, ändern Sie den Status der Richtlinien von Kaspersky Endpoint Agent und Kaspersky Endpoint Security in *Inaktiv* und aktivieren Sie die neue zusammengeführte Richtlinie.

- Assistent für das Massenkonvertieren von standardmäßigen Richtlinien und Aufgaben Der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben ist nur in der Verwaltungskonsole (MMC) verfügbar. Weitere Informationen zum Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

3. **Lizenzierung der MDR-Funktionalität**

   Um Kaspersky Endpoint Security als Teil der Kaspersky Managed Detection and Response-Lösung zu aktivieren, benötigen Sie eine separate Lizenz für das Add-on von Kaspersky Managed Detection and Response. Sie können den Schlüssel mithilfe der Aufgabe *Schlüssel hinzufügen* hinzufügen. Dadurch werden der Anwendung zwei Schlüssel hinzugefügt: *Kaspersky Endpoint Security* und *Kaspersky Managed Detection and Response*.

4. **Installation und Upgrade von Kaspersky Endpoint Security**

   Um die Funktionalität von MDR während einer Installation oder eines Upgrades der Anwendung zu migrieren, sollten Sie die Aufgabe zur Remote-Installation verwenden. Beim Erstellen einer Aufgabe zur Remote-Installation müssen Sie die Komponente MDR in den Einstellungen des Installationspakets auswählen.

   Sie können das Programm auch mit den folgenden Methoden upgraden:

   - Verwendung des Kaspersky-Update-Dienstes.
   - Lokal mithilfe des Installationsassistenten für das Programm.

Kaspersky Endpoint Security unterstützt die automatische Komponentenauswahl, wenn ein Programm-Upgrade auf einem Computer ausgeführt wird, auf dem das Programm „Kaspersky Endpoint Agent“ installiert ist. Die automatische Komponentenauswahl ist abhängig von den Berechtigungen des Benutzerkontos, unter dem das Programm upgegradet wird.

Wenn Sie Kaspersky Endpoint Security mithilfe der EXE- oder MSI-Datei unter dem Systemkonto (SYSTEM) upgraden, erhält Kaspersky Endpoint Security Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. Ist auf dem Computer Kaspersky Endpoint Agent installiert und die MDR-Lösung aktiviert, so konfiguriert das Kaspersky Endpoint Security-Installationsprogramm automatisch die Komponentenauswahl und wählt die Komponente MDR aus. Dadurch wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent. Gewöhnlich wird das MSI-Installationsprogramm unter dem Systemkonto (SYSTEM) ausgeführt, wenn ein Upgrade über den Kaspersky-Update-Dienst erfolgt oder wenn ein Installationspaket über Kaspersky Security Center bereitgestellt wird.

Wenn Sie Kaspersky Endpoint Security mithilfe einer MSI-Datei unter einem Benutzerkonto ohne Administratorrechte upgraden, hat Kaspersky Endpoint Security keinen Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. In diesem Fall wählt Kaspersky Endpoint Security automatisch die Komponenten aus und berücksichtigt dabei die Komponentenauswahl von Kaspersky Endpoint Agent. Anschließend wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

Kaspersky Endpoint Security unterstützt ein Upgrade ohne Neustart des Computers. Sie können den Modus für das App-Upgrade in den Richtlinieneigenschaften auswählen.

5. **Überprüfung des App-Betriebs**

   Falls der Computer nach der App-Installation oder dem Upgrade in der Konsole von Kaspersky Security Center den Status *Kritisch* anzeigt:

   - Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
   - Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*. Falls eine Komponente den Status *Nicht durch Lizenz abgedeckt* hat, stellen Sie sicher, dass Sie die Funktionalität des integrierten Agenten aktiviert haben.
   - Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

Endpoint Detection and Response

Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten für die Lösung Kaspersky Endpoint Detection and Response Optimum (im Folgenden auch „EDR Optimum“). Ab Version 11.8.0 enthält Kaspersky Endpoint Security für Windows einen integrierten Agenten für die Lösung Kaspersky Endpoint Detection and Response Expert (im Folgenden auch „EDR Expert“). *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. Im Vergleich zu „EDR Optimum“ bietet „EDR Expert“ eine erweiterte Funktionalität zur Überwachung von und zur Reaktion auf Bedrohungen. Einzelheiten zu diesen Lösungen finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

Threat Intelligence-Tools

Kaspersky Endpoint Detection and Response verwendet die folgenden Threat Intelligence-Tools:

- Integration in Kaspersky Threat Intelligence Portal, das Informationen über die Reputation von Dateien und Webadressen enthält und anzeigt.
- Kaspersky Threats-Datenbank.
- Die Cloud-Service-Infrastruktur von Kaspersky Security Network (im Folgenden auch „KSN" genannt), die Echtzeitzugriff auf Datei-, Website- und Software-Reputationsinformationen aus der Kaspersky-Wissensdatenbank bietet. Durch die Verwendung von Daten aus Kaspersky Security Network wird die Reaktion der Kaspersky-Programme auf Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.
- Die Cloud Sandbox-Technologie, mit der Sie erkannte Dateien in einer isolierten Umgebung ausführen und ihre Reputation überprüfen können.

Funktionsweise der Lösung

„Kaspersky Endpoint Detection and Response" prüft und analysiert, wie sich eine Bedrohung entwickelt, und versorgt die *Sicherheitsabteilung* oder den *Administrator* mit Informationen über den möglichen Angriff, um eine rechtzeitige Reaktion zu ermöglichen. Kaspersky Endpoint Detection and Response (EDR) zeigt Alarm-Details in einem separaten Fenster an. Ein *Alarm* ist ein Ereignis in der Unternehmens-IT-Infrastruktur, das von der App als ungewöhnlich oder verdächtig eingestuft wurde und möglicherweise eine Sicherheitsbedrohung für die IT-Infrastruktur des Unternehmens darstellt. *Alarm-Details* ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum" und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert".

Unterstützung für ältere Versionen von Kaspersky Endpoint Security

Wenn Sie Kaspersky Endpoint Security 11.2.0 – 11.6.0 für die Interoperabilität mit Kaspersky Endpoint Detection and Response Optimum verwenden, ist Kaspersky Endpoint Agent in der Anwendung enthalten. Sie können Kaspersky Endpoint Agent gleichzeitig mit Kaspersky Endpoint Security installieren. In Kaspersky Endpoint Security 11.9.0 ist das Verteilungspaket für Kaspersky Endpoint Agent nicht mehr Teil des Verteilungskits für Kaspersky Endpoint Security.

Die Lösung „Kaspersky Endpoint Detection and Response Expert" unterstützt die Interoperabilität mit „Kaspersky Endpoint Agent" nicht. Die Lösung „Kaspersky Endpoint Detection and Response Expert" nutzt Kaspersky Endpoint Security mit dem integrierten Agenten (Version 11.8.0 oder höher).

Integration des integrierten Agenten in EDR Optimum / EDR Expert

Um die Integration in Kaspersky Endpoint Detection and Response einzurichten, müssen Sie die Komponente Endpoint Detection and Response Optimum oder die Komponente Endpoint Detection and Response Expert (cloud) hinzufügen und Kaspersky Endpoint Security konfigurieren.

Die Komponenten Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) und Endpoint Detection and Response Expert (on-premises) sind nicht miteinander kompatibel.

Damit „Endpoint Detection and Response“ funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Security Center Version 13.2 oder höher. In älteren Versionen von Kaspersky Security Center kann die Funktion „Endpoint Detection and Response“ nicht aktiviert werden.
- Verwaltungs-Plug-in für Kaspersky Endpoint Detection and Response.

  Ab Kaspersky Endpoint Security Version 12.6 befinden sich die Warnungsdetails nicht mehr im Verwaltungs-Plug-in für Kaspersky Endpoint Security, sondern im EDR-Verwaltungs-Plug-in. Das EDR-Verwaltungs-Plug-in ist ein spezielles Plug-in für die Arbeit mit Agenten auf den Betriebssystemen Windows, Mac und Linux. Wenn Sie jetzt mit EDR Optimum arbeiten, benötigen Sie das Verwaltungs-Plug-in für Kaspersky Endpoint Security, um Aufgaben zur Reaktion auf Bedrohungen zu erstellen, und das EDR-Verwaltungs-Plug-in, um Details zu Warnungen anzuzeigen.
- Die Komponente Endpoint Detection and Response Optimum unterstützt als Teil von Kaspersky Endpoint Security die Interaktion mit der Lösung Kaspersky Endpoint Detection and Response Optimum 2.0. Die Interaktion mit „Kaspersky Endpoint Detection and Response Optimum“ Version 1.0 wird nicht unterstützt.
- „EDR Optimum“ kann über „Kaspersky Security Center Web Console“ und „Kaspersky Security Center Cloud Console“ verwaltet werden.

  „EDR Expert“ kann nur über „Kaspersky Security Center Cloud Console“ verwaltet werden. Sie können diese Funktionalität nicht über die Verwaltungskonsole (MMC) verwalten.
- Die Anwendung ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Die Komponente „Endpoint Detection and Response“ ist aktiviert.
- Die Programmkomponenten, von denen „Endpoint Detection and Response“ abhängt, sind aktiviert und betriebsbereit. „Endpoint Detection and Response“ ist von den folgenden Komponenten abhängig:
  - 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 Integration mit „Kaspersky Endpoint Detection and Response“ umfasst die folgenden Schritte:

1. **Installation der Komponenten von „Endpoint Detection and Response“**

   Sie können die Komponente Endpoint Detection and Response Optimum oder die Komponente Endpoint Detection and Response Expert (cloud) während der Installation oder beim Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   > Sie müssen Ihren Computer neu starten, um das Upgrade des Programms mit den neuen Komponenten abzuschließen.

2. **Aktivieren von „Kaspersky Endpoint Detection and Response“**

   Eine Lizenz für „Kaspersky Endpoint Detection and Response“ können Sie wie folgt erwerben:

   - Die Funktionalität von „Endpoint Detection and Response“ ist in der Lizenz für Kaspersky Endpoint Security für Windows enthalten.

     Die Funktionalität steht nach der Aktivierung von Kaspersky Endpoint Security für Windows sofort zur Verfügung.

   - Kauf einer separaten Lizenz für „EDR Optimum“ oder „EDR Expert“ („Kaspersky Endpoint Detection and Response“-Add-on).

     Die Funktionalität ist verfügbar, nachdem ein separater Schlüssel für Kaspersky Endpoint Detection and Response hinzugefügt wurde. Dadurch werden zwei Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security und ein Schlüssel für Kaspersky Endpoint Detection and Response.

     Die Lizenzverwaltung für die eigenständige Funktionalität von „Endpoint Detection and Response“ entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität „EDR Optimum“ oder „EDR Expert“ in der Lizenz enthalten ist und auf der lokalen Programmoberfläche ausgeführt wird.

   Weitere Informationen zum Endbenutzer-Lizenzvertrag für EDR Optimum finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

3. **Aktivieren der Komponenten von „Endpoint Detection and Response“**

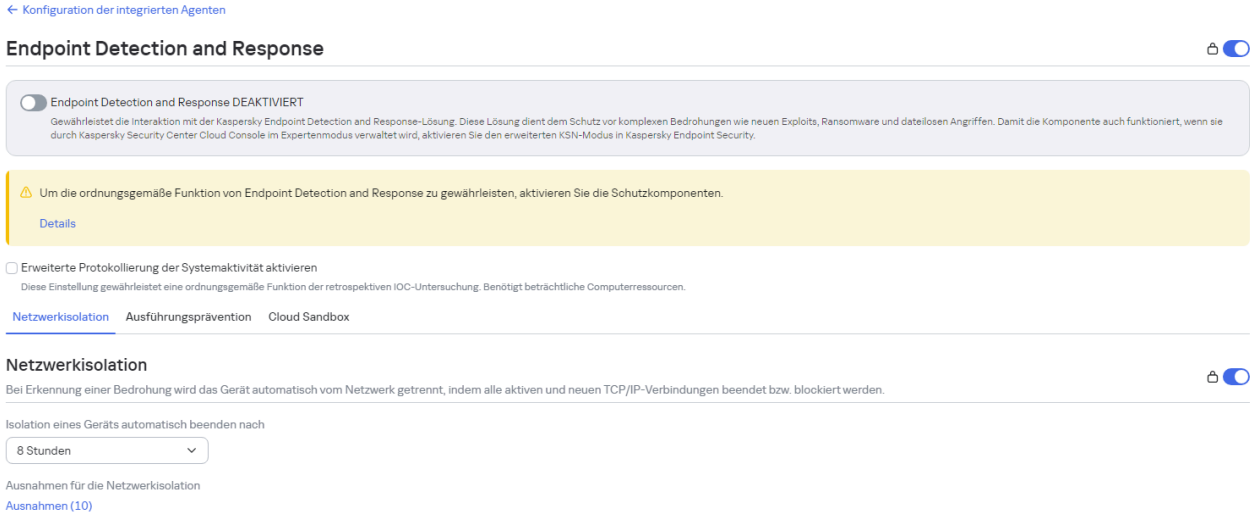
   Sie können die Komponente in den Richtlinieneinstellungen für Kaspersky Endpoint Security für Windows aktivieren oder deaktivieren.

   So aktivieren oder deaktivieren Sie die Komponente „Endpoint Detection and Response“ über die „Web Console“

   1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
   5. Aktivieren Sie den Schalter **Endpoint Detection and Response AKTIVIERT**.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Einstellungen der EDR-Integration

Die Komponente „Kaspersky Endpoint Detection and Response“ ist nun aktiviert. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Endpoint Detection and Response Optimum** oder **Endpoint Detection and Response Expert (cloud)** wird zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

4 Datenübertragung zum Administrationsserver aktivieren

Um alle Funktionen von „Endpoint Detection and Response“ zu aktivieren, muss die Datenübertragung für die folgenden Datentypen aktiviert sein:

- Daten zu Quarantänedateien.

  Diese Daten sind erforderlich, um via Web Console Informationen zu Dateien abzurufen, die sich auf dem Computer in der Quarantäne befinden. So können Sie z. B. in Web Console eine Datei aus der Quarantäne zur Analyse herunterladen.

- Daten zur Entwicklungskette der Bedrohung.

  Diese Daten sind erforderlich, um über die „Web Console“ Informationen zu den Bedrohungen abzurufen, die auf dem Computer gefunden wurden. In der „Web Console“ können Sie Alarm-Details anzeigen und Reaktionsmaßnahmen ergreifen.

So aktivieren Sie die Datenübertragung zum Administrationsserver in Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **KSC-Integration**.
5. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf den Link **Erweiterte Einstellungen**.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen:

   - **Über Quarantäne-Dateien**.
   - **Über eine Bedrohungsentwicklungskette**.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Untersuchung auf Kompromittierungsindikatoren (Standardaufgabe)

Ein *Kompromittierungsindikator (IOC)* ist ein Datensatz, der sich auf ein Objekt oder eine Aktivität bezieht und der auf unbefugten Zugriff auf den Computer (Kompromittierung von Daten) hinweist. Beispielsweise können viele erfolglose Versuche, sich beim System anzumelden, einen Kompromittierungsindikator darstellen. Mithilfe der Aufgabe *IOC-Untersuchung* können Kompromittierungsindikatoren auf dem Computer gefunden und Maßnahmen zur Reaktion auf Bedrohungen ergreifen werden.

Kaspersky Endpoint Security sucht mithilfe von IOC-Dateien nach Kompromittierungsindikatoren. *IOC-Dateien* sind Dateien, die Sätze von Indikatoren enthalten, mit denen die Anwendung nach Übereinstimmungen sucht. IOC-Dateien müssen dem OpenIOC-Standard entsprechen.

Ausführungsmodus der Aufgabe IOC-Untersuchung

Mit „Kaspersky Endpoint Detection and Response“ können Sie standardmäßige IOC-Untersuchungsaufgaben erstellen, um kompromittierte Daten zu erkennen. Eine *Standard-IOC-Untersuchungsaufgabe* ist eine Gruppenaufgabe oder lokale Aufgabe, die manuell über die „Web Console“ erstellt und konfiguriert wird. Aufgaben werden unter Verwendung von IOC-Dateien ausgeführt, die vom Benutzer erstellt wurden. Wenn Sie einen Kompromittierungsindikator manuell hinzufügen möchten, lesen Sie bitte die Anforderungen für IOC-Dateien.

Die Datei, die Sie über den unten stehenden Link herunterladen können, enthält eine Tabelle mit einer vollständigen Liste der IOC-Bedingungen gemäß OpenIOC-Standard.

DATEI „IOC_TERMS.XLSX“ HERUNTERLADEN

Kaspersky Endpoint Security unterstützt eigenständige IOC-Untersuchungsaufgaben auch, wenn die Anwendung als Teil der Lösung Kaspersky Sandbox verwendet wird.

IOC-Datei erstellen

Ab Kaspersky Endpoint Security 12.10 für Windows können Sie IOC-Dateien direkt in den Aufgabeneinstellungen erstellen. Um eine IOC-Datei zu erstellen, müssen Sie eine txt-Datei mit einer Liste von Kompromittierungsindikatoren erstellen. Sie können Listen mit den folgenden Objekte als Kompromittierungsindikatoren hinzufügen:

- Datei-Hashes (MD5/SHA256).

  Das Programm erstellt eine IOC-Datei mit dem Untersuchungsbereich FileItem/Md5sum oder FileItem/Sha256sum.

- IP-Adressen (IPv4, IPv6).

  Das Programm erstellt eine IOC-Datei mit dem Untersuchungsbereich PortItem/RemoteIP.

- DNS-Namen.

  Das Programm erstellt eine IOC-Datei mit dem Untersuchungsbereich DnsEntryItem/RecordName.

So erstellen Sie eine IOC-Datei (in der Web Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie die Aufgabe **IOC-Untersuchung** aus.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Erstellen Sie bei Bedarf die Aufgabe **IOC-Untersuchung**.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **Bedrohungsuntersuchung**.

5. Klicken Sie auf **IOC-Dateien neu definieren**.

6. Das Formular zum Erstellen einer IOC-Datei wird geöffnet:

   a. Wählen Sie unter **Quelle für IOC-Dateien** den Punkt **Aus Datei generieren** auswählen.

   b. Geben Sie den Namen für die IOC-Datei ein.

   c. Wählen Sie eine txt-Datei mit einer Liste der Kompromittierungsindikatoren aus.

   d. Wählen Sie den Typ der IOC-Datei aus: **DNS-Namen**, **Datei-Hashes**, **IP-Adressen**.

   e. Klicken Sie auf **Hochladen**.

   Kaspersky Endpoint Security fügt IOC-Dateien zu der IOC-Sammlung hinzu. Bei Bedarf können Sie IOC-Dateien vorübergehend aus dem Aufgabenbereich ausschließen.

7. Speichern Sie die vorgenommenen Änderungen.

Aufgabe IOC-Untersuchung erstellen

Sie können Aufgaben des Typs *IOC-Untersuchung* manuell erstellen:

- In den Alarm-Details (nur für „EDR Optimum“).

  Alarm-Details ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

- Mithilfe des Assistenten für das Erstellen einer Aufgabe.

Die Gruppenaufgabe *IOC-Untersuchung* kann nicht ausgeführt werden, wenn auf den zu untersuchenden Computern die Integration mit Kaspersky Endpoint Detection and Response Expert (on-premises) oder Kaspersky Endpoint Detection and Response Expert (cloud) konfiguriert ist. In diesem Fall empfehlen wir, mit der Reaktionsaktion *IOC-Untersuchung* nach Kompromittierungsindikatoren zu suchen. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises).

Sie können die Aufgabe für „EDR Optimum“ über „Web Console“ und „Cloud Console“ konfigurieren. Die Aufgabeneinstellungen für „EDR Expert“ sind nur in „Cloud Console“ verfügbar.

Um die Aufgabe IOC-Untersuchung zu erstellen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **IOC-Untersuchung**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechten Sie die Aufgabe ausführen möchten. Weiter zum nächsten Schritt

   Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

Das Systemkonto (SYSTEM) hat keine Berechtigung, die Aufgabe *IOC-Untersuchung* auf Netzlaufwerken auszuführen. Wenn Sie die Aufgabe für ein Netzlaufwerk ausführen möchten, wählen Sie das Konto eines Benutzers aus, der Zugriff auf dieses Laufwerk hat.

Für eigenständige IOC-Untersuchungsaufgaben auf Netzlaufwerken müssen Sie in den Aufgabeneigenschaften manuell das Benutzerkonto auswählen, das Zugriff auf dieses Laufwerk hat.

6. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Wechseln Sie zum Abschnitt **Bedrohungsuntersuchung**.

10. Laden Sie die IOC-Dateien hoch, um nach Kompromittierungsindikatoren zu suchen.

    Nachdem Sie die IOC-Dateien hochgeladen haben, zeigt das Programm eine Übersicht über die Datei an. Dazu gehört auch eine Liste der Indikatoren, die die Überprüfung nicht bestanden haben. Nachdem Sie IOC-Dateien hochgeladen haben, können Sie die Dateien im integrierten Editor direkt in den Aufgabeneigenschaften manuell bearbeiten. Kaspersky Endpoint Security unterstützt die Bearbeitung von IOC-Dateien, die dem OpenIOC 1.1-Standard entsprechen. Der Inhalt von IOC-Dateien, die der OpenIOC Version 1.0 entsprechen, kann nicht geändert werden.

    Kaspersky Endpoint Security fügt IOC-Dateien zu der IOC-Sammlung hinzu. Bei Bedarf können Sie IOC-Dateien vorübergehend aus dem Aufgabenbereich ausschließen.

    Es wird davon abgeraten, IOC-Dateien nach dem Ausführen der Aufgabe hinzuzufügen oder zu entfernen. Die Folge könnte sein, dass die IOC-Untersuchungsergebnisse für eine zuvor ausgeführte Aufgabe fehlerhaft angezeigt werden. Um Kompromittierungsindikatoren für neue IOC-Dateien zu suchen, wird empfohlen, neue Aufgaben hinzuzufügen.

11. Aktivieren Sie bei Bedarf das Kontrollkästchen **Retrospektive IOC-Untersuchung**. Die *retrospektive IOC-Untersuchung* ist ein Modus der Aufgabe *IOC-Untersuchung*. Dabei sucht Kaspersky Endpoint Security innerhalb eines bestimmten Zeitraums nach Kompromittierungsindikatoren. Dieser Modus ist für die Suche nach Kompromittierungsindikatoren anhand der Telemetrie des geschützten Computers vorgesehen (z. B. Netzwerkaktivität, Prozesse, Dateien und andere Telemetriedaten). Kaspersky Endpoint Security analysiert Daten aus den Protokollen des Betriebssystems und des Browsers auf dem Computer. Bei der retrospektiven IOC-Untersuchung werden die Protokolle der folgenden Browser analysiert: Google Chrome, Mozilla Firefox, Microsoft Edge (Version 79 oder höher).

12. Passen Sie die Aktionen bei der IOC-Erkennung an:

    - **Gerät vom Netzwerk isolieren**. Wenn diese Option ausgewählt ist, isoliert Kaspersky Endpoint Security den Computer vom Netzwerk, um eine Ausbreitung der Bedrohung zu verhindern. Die Isolationsdauer können Sie in den Einstellungen der Komponente „Endpoint Detection and Response“ anpassen.

      Wenn dieses Kontrollkästchen deaktiviert ist, können Sie den Computer vom Netzwerk isolieren, nachdem Sie die Aufgabe manuell ausgeführt haben. Wenn von der Aufgabe *IOC-Untersuchung* ein IOC gefunden wird, können Sie den Computer direkt über den IOC vom Netzwerk isolieren (Eigenschaften der Aufgabe *IOC-Untersuchung* → **Anwendungseinstellungen** → **IOC-Untersuchungsergebnisse**). In Kaspersky Endpoint Security können Sie auch die folgenden zusätzliche Einstellungen sofort anpassen: Zeitraum bis zum Aufheben der Netzwerkisolation sowie Ausnahmen für die Netzwerkisolation.

- **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 Objekts gelöscht wird, erstellt Kaspersky Endpoint Security eine Backup-Kopie für den Fall, dass das Objekt später wiederhergestellt werden muss. Kaspersky Endpoint Security verschiebt die Backup-Kopie in die Quarantäne.

  Wenn dieses Kontrollkästchen deaktiviert ist, können Sie die Datei manuell in die Quarantäne verschieben, nachdem Sie die Aufgabe manuell ausgeführt haben. Wenn von der Aufgabe *IOC-Untersuchung* eine Datei gefunden wird, die Daten kompromittieren kann, können Sie diese Datei direkt über die IOC-Untersuchungsergebnisse in die Quarantäne verschieben (**Anwendungseinstellungen → IOC-Untersuchungsergebnisse**). Daraufhin startet Kaspersky Endpoint Security den Assistenten für neue Aufgaben und füllt die Daten der gefundenen Datei automatisch aus. Sie müssen nur die zusätzlichen Aufgabeneinstellungen verwalten, z. B. einen Aufgabenzeitplan einrichten.

  Aktivieren Sie bei Bedarf das Kontrollkästchen **Auf systemkritische Objekte anwenden**. Systemkritische Objekte (SCOs) umfassen Dateien, die für die Funktion des Betriebssystems erforderlich sind.

  > Es wird davon abgeraten, Aktionen auf SCO-Dateien anzuwenden. Dies kann dazu führen, dass das Betriebssystem instabil wird oder nicht mehr gestartet werden kann.

- **Untersuchung wichtiger Bereiche ausführen**. Wenn diese Option ausgewählt ist, führt Kaspersky Endpoint Security die *Untersuchung wichtiger Bereiche* aus. Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden Prozesse und die Bootsektoren.

13. Wechseln Sie zum Abschnitt **Erweitert**.

14. Wählen Sie die Datentypen (IOC-Dokumente) aus, die im Rahmen der Aufgabe analysiert werden sollen.

    > Kaspersky Endpoint Security wählt automatisch Datentypen (IOC-Dokumente) für die Aufgabe *IOC-Untersuchung* aus, wobei der Inhalt der geladenen IOC-Dateien berücksichtigt wird. Es wird nicht empfohlen, die Auswahl von Datentypen aufzuheben.

    Sie können zusätzlich Scanbereiche für die folgenden Datentypen konfigurieren:

    - **Dateien – FileItem**. Legen Sie einen IOC-Scanbereich auf dem Computer über voreingestellte Bereiche fest.

      Standardmäßig untersucht Kaspersky Endpoint Security nur wichtige Bereiche des Computers auf IOCs. Dazu gehören beispielsweise der Ordner „Downloads“, der Desktop und der Ordner mit temporären Betriebssystemdateien. Sie können den Untersuchungsbereich auch manuell anpassen.

    - **Windows-Ereignisprotokoll – EventLogItem**. Geben Sie den Zeitraum ein, in dem die Ereignisse protokolliert wurden. Außerdem können Sie auswählen, welche Windows-Ereignisprotokolle für die IOC-Untersuchung verwendet werden sollen. Standardmäßig sind die folgenden Ereignisprotokolle ausgewählt: Anwendungsereignisprotokoll, Systemereignisprotokoll und Sicherheitsereignisprotokoll.

      > Verwenden Sie für den IOC-Ausdruck EventLogItem\source den Wert **Anbietername** aus dem XML-Schema des Ereignisses.

    - **Windows-Registrierung – RegistryItem**. Konfigurieren Sie den Bereich für die IOC-Untersuchung in der Registrierung.

      Standardmäßig untersucht Kaspersky Endpoint Security eine Auswahl von Registrierungsschlüsseln.

15. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

16. Passen Sie den Zeitplan für die Aufgabe an.

> Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

17. Speichern Sie die vorgenommenen Änderungen.

18. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

19. Klicken Sie auf **Starten**.

Daraufhin durchsucht Kaspersky Endpoint Security den Computer nach Kompromittierungsindikatoren. Die Ergebnisse der Aufgabe können Sie in den Aufgabeneigenschaften im Abschnitt **Ergebnisse** einsehen. Sie können die Informationen zu erkannten Kompromittierungsindikatoren in den Aufgabeneigenschaften anzeigen: **Anwendungseinstellungen → IOC-Untersuchungsergebnisse**. In den Ergebnissen der IOC-Untersuchung können Sie die gefundene Datei auch manuell in die Quarantäne verschieben oder den Computer manuell vom Netzwerk isolieren.

Kaspersky Endpoint Security untersucht die Einträge, die für eine IOC-Datei erstellt wurden, auf Duplikate und belässt nur eindeutige Einträge in den Aufgabenergebnissen. Duplikate sind Einträge des gleichen Typs, die in allen verglichenen Feldern identische Werte aufweisen. Das Programm erstellt möglicherweise auch keinen Eintrag, wenn in einem oder mehreren Feldern kein Wert vorhanden ist (siehe folgende Tabelle).

Typ	Verglichene Felder	Bedingung, bei der kein Eintrag erstellt wird
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• In den Feldern FullPath, Md5sum und Sha256sum fehlen Werte. • Im Feld FullPath fehlt ein Wert, und die Felder Md5sum und Sha256sum enthalten identische Werte.
RegistryItem	• Hive • KeyPath • ValueName • Text • Typ	In mindestens einem der folgenden Felder fehlt ein Wert: Hive, KeyPath, ValueName.
ProcessItem	• startTime • PID	In mindestens einem der Felder startTime und PID fehlt ein Wert.

> Das Fenster **Warnungsdetails** enthält möglicherweise RegistryItem-Einträge mit identischen Feldwerten. Solche Einträge sind keine Duplikate, da sie unterschiedliche Werte im Feld „Text“ haben, das nicht auf der Benutzeroberfläche angezeigt wird.

> IOC-Untersuchungsergebnisse werden für 30 Tage gespeichert. Nach diesem Zeitraum löscht Kaspersky Endpoint Security automatisch die ältesten Einträge.

Erweiterte Telemetrie für die IOC-Untersuchung

Für retrospektive IOC-Untersuchungen wird empfohlen die erweiterte Telemetrie auf dem Computer zu aktivieren. Die erweiterte Telemetrie verbessert die Genauigkeit der IOC-Erkennung, erfordert jedoch mehr Computerressourcen.

Die erweiterte Telemetrie umfasst die Unterstützung der folgenden zusätzlichen Bedingungen:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

Wenn die erweiterte Telemetrie deaktiviert ist, kann Kaspersky Endpoint Security die Informationen über gefundene Kompromittierungsindikatoren rotieren.

So aktivieren Sie die erweiterte Telemetrie:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Aktivieren Sie das Kontrollkästchen **Erweiterte Protokollierung der Systemaktivität aktivieren**.
6. Speichern Sie die vorgenommenen Änderungen.

Datei in die Quarantäne verschieben

Kaspersky Endpoint Detection and Response kann als Reaktion auf Bedrohungen Aufgaben des Typs *Datei in Quarantäne verschieben* erstellen. Dies ist erforderlich, um die Folgen der Bedrohung zu minimieren. Die *Quarantäne* ist ein spezieller lokaler Speicher auf dem Computer. Der Benutzer kann Dateien, die er für gefährlich für den Computer hält, in die Quarantäne verschieben. Unter Quarantäne stehende Dateien werden in verschlüsselter Form gespeichert und gefährden die Sicherheit des Gerätes nicht. Kaspersky Endpoint Security verwendet die Quarantäne nur dann, wenn das Programm in Kaspersky Detection and Response-Lösungen integriert ist. In anderen Fällen legt Kaspersky Endpoint Security die entsprechende Datei im Backup ab. Ausführliche Informationen zur Verwaltung der Quarantäne als Teil dieser Lösungen finden Sie in der Hilfe zu Kaspersky Sandbox, Hilfe zu Kaspersky Endpoint Detection and Response Optimum, Hilfe zu Kaspersky Endpoint Detection and Response Expert, Hilfe zu Kaspersky Anti Targeted Attack Platform, und Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises).

Aufgaben des Typs *Datei in Quarantäne verschieben* werden wie folgt erstellt:

- In den Alarm-Details (nur für „EDR Optimum“).

  Alarm-Details ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

- Mithilfe des Assistenten für das Erstellen einer Aufgabe.

  Sie müssen den Dateipfad oder Datei-Hash (SHA256 oder MD5) eingeben oder sowohl den Dateipfad als auch den Datei-Hash.

- In den Einstellungen der Aufgabe *IOC-Untersuchung*.

  Wenn von der Aufgabe *IOC-Untersuchung* eine Datei gefunden wird, die Daten kompromittieren kann, können Sie diese Datei direkt über die IOC-Untersuchungsergebnisse in die Quarantäne verschieben (**Anwendungseinstellungen** → **IOC-Untersuchungsergebnisse**). Daraufhin startet Kaspersky Endpoint Security den Assistenten für neue Aufgaben und füllt die Daten der gefundenen Datei automatisch aus. Sie müssen nur die zusätzlichen Aufgabeneinstellungen verwalten, z. B. einen Aufgabenzeitplan einrichten.

Die Aufgabe *Datei in Quarantäne verschieben* hat folgende Einschränkungen:

1. Die Datei darf maximal 100 MB groß sein.
2. Sie können keine Dateien löschen, die für den Betrieb von Kaspersky Endpoint Security für Windows erforderlich sind:
   - Dateien im Gültigkeitsbereich der Selbstschutztechnologie von Kaspersky Endpoint Security für Windows
   - Von Kaspersky digital signierte Dateien
3. Sie können die Aufgabe für „EDR Optimum“ über „Web Console“ und „Cloud Console“ konfigurieren. Die Aufgabeneinstellungen für „EDR Expert“ sind nur in „Cloud Console“ verfügbar.
4. Sie können ein Objekt nicht untersuchen, das aufgrund der Aufgabe *Datei in Quarantäne verschieben* in die Quarantäne verschoben wurde.

Um die Aufgabe Datei in Quarantäne verschieben zu erstellen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Datei in Quarantäne verschieben**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechten Sie die Aufgabe ausführen möchten. Klicken Sie auf **Weiter**.

   Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Aktivieren Sie bei Bedarf das Kontrollkästchen **Auf systemkritische Objekte anwenden**.

   System Critical Objects (SCOs) umfassen Dateien, die für die Funktion des Betriebssystems erforderlich sind.

   Es wird davon abgeraten, Aktionen auf SCO-Dateien anzuwenden. Dies kann dazu führen, dass das Betriebssystem instabil wird oder nicht mehr gestartet werden kann.

10. Klicken Sie in der Dateiliste auf **Hinzufügen**.

    Der Assistent zum Hinzufügen von Dateien wird gestartet.

11. Um die Datei hinzuzufügen, müssen Sie den vollständigen Dateipfad oder sowohl den Datei-Hash als auch den Pfad eingeben.

    Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Wenn der Dateipfad einen Netzlaufwerksbuchstaben enthält, erhalten Sie möglicherweise den Fehler *Datei wurde nicht gefunden*.

12. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

13. Passen Sie den Zeitplan für die Aufgabe an.

    Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

14. Speichern Sie die vorgenommenen Änderungen.

15. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

16. Klicken Sie auf **Starten**.

Daraufhin verschiebt Kaspersky Endpoint Security die Datei in die Quarantäne.

Ist die Datei durch einen anderen Prozess gesperrt, so wird für die Aufgabe der Status Ausgeführt angezeigt, die Datei selbst wird aber erst nach dem Neustart des Computers in die Quarantäne verschoben. Bestätigen Sie nach dem Neustart des Computers, dass die Datei gelöscht werden soll.

Ist die Datei durch einen anderen Prozess gesperrt, so wird für die Aufgabe der Status *Abgeschlossen* angezeigt, die Datei wird aber erst nach dem Neustart des Computers in die Quarantäne verschoben. Bestätigen Sie nach dem Neustart des Computers, dass die Datei gelöscht werden soll.

Die Aufgabe *Datei in Quarantäne verschieben* kann mit dem Fehler *Zugriff verweigert* abschließen, wenn Sie versuchen, eine ausführbare Datei, die gerade ausgeführt wird, in die Quarantäne zu verschieben. Erstellen Sie die Aufgabe „Prozess beenden“ für die Datei und versuchen Sie es erneut.

Die Aufgabe *Datei in Quarantäne verschieben* kann mit dem Fehler *Zu wenig Platz im Quarantäne-Speicher* abschließen, wenn Sie versuchen, eine zu große Datei in die Quarantäne zu verschieben. Leeren Sie den Quarantänebereich oder vergrößern Sie ihn. Dann versuchen Sie es erneut.

Sie können eine Datei aus der Quarantäne wiederherstellen oder die Quarantäne mithilfe der „Web Console“ leeren. Sie können Objekte über die Befehlszeile lokal auf dem Computer wiederherstellen.

Datei anfordern

Sie können Dateien von Benutzercomputern abrufen. Sie können beispielsweise das Abrufen einer Ereignisprotokolldatei konfigurieren, die von einem Drittanbieter-Programm erstellt wurde. Nachdem die Aufgabe ausgeführt wurde, wird eine Kopie der Datei in der Quarantäne gespeichert. Die *Quarantäne* ist ein spezieller lokaler Speicher auf dem Computer. Sie können diese Datei mithilfe der Web Console (**Vorgänge** → **Datenverwaltung** → **Quarantäne**) aus der Quarantäne auf Ihren Computer herunterladen. Die Datei verbleibt auf dem Computer des Benutzers im ursprünglichen Ordner.

Die Datei darf maximal 2 GB groß sein.

Sie können die Aufgabe für „EDR Optimum“ über „Web Console“ und „Cloud Console“ konfigurieren. Die Aufgabeneinstellungen für „EDR Expert“ sind nur in „Cloud Console“ verfügbar.

Um die Aufgabe Datei anfordern zu erstellen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Datei anfordern**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechten Sie die Aufgabe ausführen möchten. Klicken Sie auf **Weiter**.

   Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Klicken Sie in der Dateiliste auf **Hinzufügen**.

   Der Assistent zum Hinzufügen von Dateien wird gestartet.

10. Um die Datei hinzuzufügen, müssen Sie den vollständigen Dateipfad oder sowohl den Datei-Hash als auch den Pfad eingeben.

    Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Wenn der Dateipfad einen Netzlaufwerksbuchstaben enthält, erhalten Sie möglicherweise den Fehler *Datei wurde nicht gefunden*.

11. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

12. Passen Sie den Zeitplan für die Aufgabe an.

    Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

13. Speichern Sie die vorgenommenen Änderungen.

14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf **Starten**.

    Daraufhin erstellt Kaspersky Endpoint Security eine Kopie der Datei und verschiebt sie in die Quarantäne. Sie können die Datei über die „Web Console“ aus der Quarantäne herunterladen.

Datei löschen

Sie können Dateien mithilfe der Aufgabe *Datei löschen* per Fernzugriff löschen. Sie können beispielsweise eine Datei aus der Ferne löschen, um auf Bedrohungen zu reagieren.

Sie können keine Dateien löschen, die für den Betrieb von Kaspersky Endpoint Security für Windows erforderlich sind:

- Dateien im Gültigkeitsbereich der Selbstschutztechnologie von Kaspersky Endpoint Security für Windows
- Von Kaspersky digital signierte Dateien

Sie können die Aufgabe für „EDR Optimum“ über „Web Console“ und „Cloud Console“ konfigurieren. Die Aufgabeneinstellungen für „EDR Expert“ sind nur in „Cloud Console“ verfügbar.

Um die Aufgabe Datei löschen zu erstellen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Datei löschen**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechten Sie die Aufgabe ausführen möchten. Klicken Sie auf **Weiter**.

   Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Um die Datei hinzuzufügen, müssen Sie den vollständigen Dateipfad oder sowohl den Datei-Hash als auch den Pfad eingeben.

   Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Wenn der Dateipfad einen Netzlaufwerksbuchstaben enthält, erhalten Sie möglicherweise den Fehler *Datei wurde nicht gefunden*.

10. Aktivieren Sie bei Bedarf das Kontrollkästchen **Auf systemkritische Objekte anwenden**.

    System Critical Objects (SCOs) umfassen Dateien, die für die Funktion des Betriebssystems erforderlich sind.

    Es wird davon abgeraten, Aktionen auf SCO-Dateien anzuwenden. Dies kann dazu führen, dass das Betriebssystem instabil wird oder nicht mehr gestartet werden kann.

11. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

12. Passen Sie den Zeitplan für die Aufgabe an.

    Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

13. Speichern Sie die vorgenommenen Änderungen.

14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf **Starten**.

    Daraufhin löscht Kaspersky Endpoint Security die Datei vom entsprechenden Computer. Ist die Datei durch einen anderen Prozess gesperrt, so wird für die Aufgabe der Status *Ausgeführt* angezeigt, die Datei wird aber erst nach dem Neustart des Computers gelöscht. Bestätigen Sie nach dem Neustart des Computers, dass die Datei gelöscht werden soll.

Die Aufgabe *Datei löschen* kann mit dem Fehler *Zugriff verweigert oder Datei nicht gefunden* abschließen, wenn Sie versuchen, eine ausführbare Datei, die gerade ausgeführt wird, zu löschen. Erstellen Sie die Aufgabe „Prozess beenden“ für die Datei und versuchen Sie es erneut.

Prozess-Start

Sie können Dateien mithilfe der Aufgabe *Prozess-Start* per Fernzugriff ausführen. Sie können beispielsweise aus der Ferne ein Dienstprogramm ausführen, das die Computerkonfigurationsdatei erstellt. Anschließend können Sie die Aufgabe *Datei anfordern* verwenden, um die erstellte Datei in Kaspersky Security Center Web Console zu empfangen.

Sie können die Aufgabe für „EDR Optimum“ über „Web Console“ und „Cloud Console“ konfigurieren. Die Aufgabeneinstellungen für „EDR Expert“ sind nur in „Cloud Console“ verfügbar.

Um die Aufgabe Prozess-Start zu erstellen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Prozess-Start**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

   d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechten Sie die Aufgabe ausführen möchten. Klicken Sie auf **Weiter**.

   Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

8. Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

9. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

10. Geben Sie den Befehl zum Prozess-Start ein.

    Angenommen, Sie möchten ein Dienstprogramm (`utility.exe`) ausführen, das Informationen über die Computerkonfiguration (standardmäßig) in der Datei `conf.txt` im aktuellen Ordner speichert. Das Dienstprogramm befindet sich im Ordner `C:\Users\admin\Diagnostic\`. Sie müssen die Konfigurationsdatei im Ordner `C:\Users\admin\Documents\Configuration` speichern. Geben Sie die folgenden Werte ein:

    - **Ausführbarer Befehl** – `C:\Users\admin\Diagnostic\utility.exe`
    - **Befehlszeilenargumente (optional)** – `/R conf.txt`
    - **Pfad zum Arbeitsverzeichnis (optional)** – `C:\Users\admin\Documents\Configuration`

11. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

12. Passen Sie den Zeitplan für die Aufgabe an.

    Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

13. Speichern Sie die vorgenommenen Änderungen.

14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf **Starten**.

    Daraufhin führt Kaspersky Endpoint Security den Befehl im Hintergrund aus und startet den Prozess. Die Ergebnisse der Aufgabe können Sie in den Aufgabeneigenschaften im Abschnitt **Ausführungsergebnisse** einsehen.

Prozess beenden

Sie können Prozesse mithilfe der Aufgabe *Prozess beenden* ferngesteuert beenden. Beispielsweise können Sie ein Dienstprogramm ferngesteuert beenden, das zum Testen der Übertragungsrate dient und das mit der Aufgabe *Starten des Prozesses* gestartet wurde.

Wenn Sie das Ausführen einer Datei unterbinden möchten, können Sie die Ausführungsverhinderungskomponente konfigurieren. Sie können die Ausführung von ausführbaren Dateien, Skripten und Dateien im Office-Format verbieten.

Die Aufgabe *Prozess beenden* hat folgende Einschränkungen:

Sie können keine Dateiprozesse beenden, die für den Betrieb von Kaspersky Endpoint Security für Windows erforderlich sind:

- Dateien im Gültigkeitsbereich der Selbstschutztechnologie von Kaspersky Endpoint Security für Windows
- Von Kaspersky digital signierte Dateien

Sie können die Aufgabe für „EDR Optimum“ über „Web Console“ und „Cloud Console“ konfigurieren. Die Aufgabeneinstellungen für „EDR Expert“ sind nur in „Cloud Console“ verfügbar.

Um die Aufgabe Prozess beenden zu erstellen:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für neue Aufgaben wird gestartet.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Endpoint Security für Windows 14.2**.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Prozess beenden**.

c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein.

d. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

4. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Klicken Sie auf **Weiter**.

5. Geben Sie die Anmeldedaten für das Konto des Benutzers ein, mit dessen Rechten Sie die Aufgabe ausführen möchten. Klicken Sie auf **Weiter**.

   Standardmäßig führt Kaspersky Endpoint Security die Aufgabe unter dem Systembenutzerkonto (SYSTEM) aus.

6. Beenden Sie den Assistenten durch Klick auf **Fertigstellen**.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.

7. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

8. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

9. Aktivieren Sie bei Bedarf das Kontrollkästchen **Auf systemkritische Objekte anwenden**.

   System Critical Objects (SCOs) umfassen Dateien, die für die Funktion des Betriebssystems erforderlich sind.

   Es wird davon abgeraten, Aktionen auf SCO-Dateien anzuwenden. Dies kann dazu führen, dass das Betriebssystem instabil wird oder nicht mehr gestartet werden kann.

10. Zum Abschließen des Vorgangs müssen Sie die Datei auswählen, die Sie beenden möchten. Für die Auswahl einer Datei bestehen folgenden Möglichkeiten:

    - Geben Sie den vollständigen Namen der Datei ein.
    - Geben Sie den Datei-Hash und den Dateipfad ein.
    - Geben Sie die PID des Prozesses ein (nur für lokale Aufgaben).
    - Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Wenn der Dateipfad einen Netzlaufwerksbuchstaben enthält, erhalten Sie möglicherweise den Fehler *Datei wurde nicht gefunden*.

    Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Wenn der Dateipfad einen Netzlaufwerksbuchstaben enthält, erhalten Sie möglicherweise den Fehler *Datei nicht gefunden*.

11. Wählen Sie im Eigenschaftenfenster der Aufgabe die Registerkarte **Zeitplan** aus.

12. Passen Sie den Zeitplan für die Aufgabe an.

    Wake-on-LAN ist für diese Aufgabe nicht verfügbar. Stellen Sie sicher, dass der Computer eingeschaltet ist, damit die Aufgabe ausgeführt werden kann.

13. Klicken Sie auf **Speichern**.

14. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.

15. Klicken Sie auf **Starten**.

    Daraufhin löscht Kaspersky Endpoint Security den Prozess vom entsprechenden Computer. Beispiel: Wenn eine GAME-Anwendung ausgeführt wird und Sie den Prozess game.exe beenden, wird die Anwendung geschlossen, ohne Daten zu speichern. Die Ergebnisse der Aufgabe können Sie in den Aufgabeneigenschaften im Abschnitt **Ergebnisse** einsehen.

Ausführungsprävention

Die „Ausführungsprävention“ ermöglicht das Starten ausführbarer Dateien und Skripte sowie das Öffnen von Dateien in Office-Formaten. Dadurch können Sie beispielsweise die Ausführung von Anwendungen verhindern, die Sie für unsicher halten. Dadurch kann die Ausbreitung der Bedrohung gestoppt werden. Die Ausführungsverhinderung unterstützt eine Reihe von Office-Dateierweiterungen und Skriptinterpretern.

Regeln für die Ausführungsprävention

Die Ausführungsverhinderung verwaltet den Benutzerzugriff auf Dateien mit Ausführungsverhinderungsregeln. 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.

Sie können Regeln für die Ausführungsprävention erstellen:

- In den Alarm-Details (nur für „EDR Optimum“).

  Alarm-Details ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

- Verwenden einer Gruppenrichtlinie oder lokaler Anwendungseinstellungen.

  Sie müssen den Dateipfad oder Datei-Hash (SHA256 oder MD5) oder den Ordnerpfad und den Datei-Hash eingeben.

Sie können „Ausführungsverhinderung verwalten“ auch lokal über die Befehlszeile aktivieren oder deaktivieren.

Die Ausführungsprävention besitzt die folgenden Beschränkungen:

1. Präventionsregeln gelten nicht für Dateien auf CDs oder in ISO-Images. Die Anwendung blockiert nicht die Ausführung oder das Öffnen dieser Dateien.
2. Sie können keine Präventionsregel auf Dateien anwenden, die für den Betrieb von Kaspersky Endpoint Security für Windows erforderlich sind:
   - Dateien im Gültigkeitsbereich der Selbstschutztechnologie von Kaspersky Endpoint Security für Windows
   - Von Kaspersky digital signierte Dateien
3. Es wird nicht empfohlen, mehr als 5.000 Ausführungspräventionsregeln zu erstellen, da dies zu Systeminstabilität führen kann.

Regeln für die Ausführungsprävention

Ausführungsprävention kann in zwei Modi ausgeführt werden:

- **Nur Statistik**

  In diesem Modus veröffentlicht Kaspersky Endpoint Security im Windows-Ereignisprotokoll 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. Standardmäßig ist dieser Modus ausgewählt.

- **Aktiv**

  In diesem Modus sperrt die Anwendung die Ausführung von Objekten oder das Öffnen von Dokumenten, die den Kriterien der Präventionsregel entsprechen. Außerdem veröffentlicht die Anwendung im Windows-Ereignisprotokoll und im Kaspersky Security Center-Ereignisprotokoll ein Ereignis über Versuche, Objekte auszuführen oder Dokumente zu öffnen.

Verwaltung der Ausführungsprävention

Die Komponenteneinstellungen können nur über die „Web Console“ konfiguriert werden.

Um die Ausführung zu verhindern:

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Wählen Sie die Registerkarte **Ausführungsprävention** aus.

6. Aktivieren Sie den Schalter **Ausführungsprävention AKTIVIERT**.

7. Wählen Sie im Block **Aktion beim Ausführen oder Öffnen eines verbotenen Objekts** den Betriebsmodus der Komponente:

   - **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 die Anwendung im Windows-Ereignisprotokoll und im Kaspersky Security Center-Ereignisprotokoll ein Ereignis über Versuche, Objekte auszuführen oder Dokumente zu öffnen.

     Aktivieren Sie bei Bedarf das Kontrollkästchen **Auf systemkritische Objekte anwenden**. System Critical Objects (SCOs) umfassen Dateien, die für die Funktion des Betriebssystems erforderlich sind.

     Es wird davon abgeraten, Aktionen auf SCO-Dateien anzuwenden. Dies kann dazu führen, dass das Betriebssystem instabil wird oder nicht mehr gestartet werden kann.

   - **Dem Ereignisprotokoll hinzufügen**. In diesem Modus veröffentlicht Kaspersky Endpoint Security im Windows-Ereignisprotokoll 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. Standardmäßig ist dieser Modus ausgewählt.

8. Erstellen Sie eine Liste mit Regeln zur Prävention der Ausführung:

   a. Klicken Sie auf **Hinzufügen**.

   b. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster den Namen der Regeln zur Prävention der Ausführung (Beispielsweise, *Programm A*).

   c. Wählen Sie aus der Dropdown-Liste **Typ** die Aufgabe aus, die Sie blockieren möchten: **Ausführbare Datei**, **Skript**, **Microsoft Office-Dokument**.

      Falls Sie einen falschen Objekttyp auswählen, blockiert Kaspersky Endpoint Security die Datei oder das Skript nicht.

   d. Um die Datei hinzuzufügen, müssen Sie den Datei-Hash (SHA256 oder MD5), den vollständigen Dateipfad oder den Hash und den Ordnerpfad eingeben.

      Wenn sich die Datei auf einem Netzlaufwerk befindet, geben Sie vor dem Dateipfad die Zeichen `\\` ein, nicht den Laufwerksbuchstaben. Beispiel: `\\server\shared_folder\file.exe`. Falls der Dateipfad einen Netzlaufwerksbuchstaben enthält, wird Kaspersky Endpoint Security die Datei oder das Skript nicht blockieren.

      Die Ausführungsverhinderung unterstützt eine Reihe von Office-Dateierweiterungen und Skriptinterpretern.

9. Speichern Sie die vorgenommenen Änderungen.

Dadurch blockiert Kaspersky Endpoint Security die Ausführung von ausführbaren Dateien und Skripten sowie das Öffnen von Dateien im Office-Format. Sie können jedoch beispielsweise eine Skriptdatei in einem Texteditor öffnen, auch wenn die Ausführung des Skripts verhindert wird. Beim Blockieren der Ausführung eines Objekts zeigt Kaspersky Endpoint Security eine Standardbenachrichtigung an (siehe Abbildung unten), wenn die Benachrichtigungen in den Programmeinstellungen aktiviert sind.



Regeln für die Ausführungsprävention

Isolation des Computernetzwerks

Die Netzwerkisolation des Computers ermöglicht es, einen Computer automatisch vom Netzwerk zu isolieren, sobald ein Kompromittierungsindikator (IOC) erkannt wird – dies ist der *automatische Modus*. Sie können die Netzwerkisolierung manuell aktivieren, während Sie die erkannte Bedrohung untersuchen – dies ist der *manuelle Modus*.

Falls die Netzwerkisolation aktiviert ist, trennt die Anwendung alle aktiven Verbindungen und blockiert alle neuen TCP/IP-Verbindungen auf dem Computer, außer der Folgenden:

- Verbindungen, die als Ausnahmen von der Netzwerkisolation festgelegt sind.
- Verbindungen, die von Kaspersky Endpoint Security-Diensten initiiert werden.
- Verbindungen, die vom Kaspersky Security Center-Administrationsagenten initiiert werden.
- Verbindungen mit SVMs und Integrationsserver, wenn die App im Light Agent-Modus verwendet wird.
- Verbindungen mit KSN, wenn das Programm in Kaspersky Managed Detection and Response integriert wird.

Die Komponenteneinstellungen können nur über die „Web Console“ konfiguriert werden.

Modus zur automatischen Netzwerkisolation

Sie können die Netzwerkisolation so konfigurieren, dass sie als Reaktion auf eine IOC-Erkennung automatisch aktiviert wird. Sie können den Modus zur automatischen Netzwerkisolation mithilfe einer Gruppenrichtlinie konfigurieren.

Konfiguration der Netzwerkisolation, sodass sie als Reaktion auf eine IOC-Erkennung automatisch aktiviert wird.

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **IOC-Untersuchung**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

   Erstellen Sie bei Bedarf die Aufgabe *IOC-Untersuchung*.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie den Abschnitt **Reaktionseinstellungen** aus.

5. Wählen Sie im Block **Konfigurieren Sie die Reaktionen auf IOC-Funde** den Punkt **Alarm auslösen und reagieren** aus und aktivieren Sie das Kontrollkästchen **Gerät vom Netzwerk isolieren**.

6. Speichern Sie die vorgenommenen Änderungen.

   Wird ein IOC erkannt, isoliert die Anwendung den Rechner vom Netzwerk, um die Ausbreitung der Bedrohung zu verhindern.

Sie können die automatische Netzwerkisolation so konfigurieren, dass sie nach einem bestimmten Zeitraum deaktiviert wird. Das Programm deaktiviert die Netzwerkisolation standardmäßig 8 Stunden, nachdem diese aktiviert wurde. Sie können die Netzwerkisolation auch manuell deaktivieren (siehe folgende Anleitung). Nach dem Deaktivieren der Netzwerkisolierung kann der Computer das Netzwerk ohne Einschränkungen verwenden.

So konfigurieren Sie die verzögerte Abschaltung der Netzwerkisolation eines Computers im automatischen Modus

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

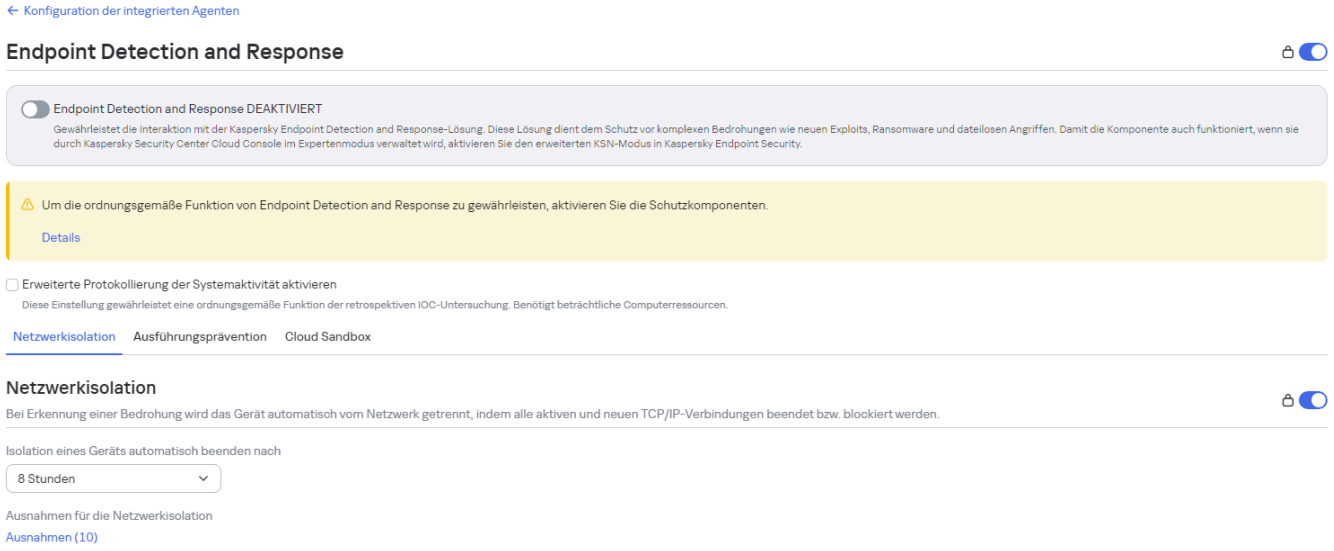
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.

5. Wählen Sie die Registerkarte **Netzwerkisolation** aus.

6. Wählen Sie aus, nach welcher Verzögerung die Netzwerkisolation deaktiviert werden soll.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.



Einstellungen der EDR-Integration

Modus zur manuellen Netzwerkisolation

Sie können die Netzwerkisolation manuell ein- und ausschalten. Den manuellen Modus zur Netzwerkisolation können Sie über die Computereigenschaften in der Kaspersky Security Center-Konsole anpassen.

Sie können die Netzwerkisolation aktivieren:

- In den Alarm-Details (nur für „EDR Optimum“).

  Alarm-Details ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

- Lokale Programmeinstellungen verwenden.

- In den Einstellungen der Aufgabe *IOC-Untersuchung*.

  Wenn von der Aufgabe *IOC-Untersuchung* ein IOC gefunden wird, können Sie den Computer direkt über den IOC vom Netzwerk isolieren (Eigenschaften der Aufgabe *IOC-Untersuchung* → **Anwendungseinstellungen** → **IOC-Untersuchungsergebnisse**). In Kaspersky Endpoint Security können Sie auch die folgenden zusätzliche Einstellungen sofort anpassen: Zeitraum bis zum Aufheben der Netzwerkisolation sowie Ausnahmen für die Netzwerkisolation.

Manuelle Aktivierung Netzwerkisolation eines Computers

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Assets (Geräte)** aus.

2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.

   Die Eigenschaften des Computers werden geöffnet.

3. Wählen Sie die Registerkarte **Anwendungen** aus.

4. Klicken Sie auf **Kaspersky Endpoint Security für Windows 14.2**.

   Die lokalen Programmeinstellungen werden geöffnet.

5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

6. Gehen Sie zu **Detection and Response → Endpoint Detection and Response**.

7. Klicken Sie im Block **Netzwerkisolation** auf **Computer vom Netzwerk isolieren**.

Sie können die automatische Netzwerkisolation so konfigurieren, dass sie nach einem bestimmten Zeitraum deaktiviert wird. Das Programm deaktiviert die Netzwerkisolation standardmäßig 8 Stunden, nachdem diese aktiviert wurde. Nach dem Deaktivieren der Netzwerkisolierung kann der Computer das Netzwerk ohne Einschränkungen verwenden.

So konfigurieren Sie die verzögerte Abschaltung der Netzwerkisolation eines Computers im manuellen Modus

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.

   Die Eigenschaften des Computers werden geöffnet.

3. Wählen Sie die Registerkarte **Aufgaben** aus.

   Dadurch wird die Liste der auf dem Computer verfügbaren Aufgaben angezeigt.

4. Wählen Sie die Aufgabe **Netzwerkisolation** aus.

5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

6. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die verzögerte Abschaltung der Netzwerkisolation aus.

7. Speichern Sie die vorgenommenen Änderungen.

Manuelle Deaktivierung der Netzwerkisolation eines Computers

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.

2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.

   Die Eigenschaften des Computers werden geöffnet.

3. Wählen Sie die Registerkarte **Anwendungen** aus.

4. Klicken Sie auf **Kaspersky Endpoint Security für Windows 14.2**.

   Die lokalen Programmeinstellungen werden geöffnet.

5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

6. Gehen Sie zu **Konfiguration der integrierten Agenten → Endpoint Detection and Response**.

7. Klicken Sie im Block **Netzwerkisolation** auf **Netzwerkisolation des Computers aufheben**.

Sie können „Netzwerkisolation" auch lokal über die Befehlszeile aktivieren oder deaktivieren.

Ab Kaspersky Endpoint Security 12.10 für Windows können Sie die Netzwerkisolation über die Warnungsdetails verwalten. Außerdem können Sie in den Warnungsdetails den Zeitraum für die Netzwerkisolation des Computers angeben. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

Ausnahmen von der Netzwerkisolation

Sie können Ausnahmen für die Netzwerkisolation konfigurieren. Netzwerkverbindungen, die diesen Regeln entsprechen, werden auf dem Computer 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. Sie können auch die Einstellungen von Standardnetzwerkprofilen ändern oder Ausschlüsse manuell definieren (siehe Anweisungen unten).

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.

Eine aktive Richtlinie verhindert nicht die Anwendung von Ausschlüssen von der Netzwerkisolation, die in den Computereigenschaften konfiguriert sind, da diese Parameter unterschiedliche Verwendungsszenarien haben.

So fügen Sie eine Ausnahme für die Netzwerkisolation im automatischen Modus hinzu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Wählen Sie die Registerkarte **Netzwerkisolation** aus.
6. Klicken Sie im Block **Ausnahmen für die Netzwerkisolation** auf **Ausnahmen**.
7. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf **Hinzufügen** → **Aus Profil hinzufügen** und wählen Sie Standard-Netzwerkprofile aus, um die Ausnahmen zu konfigurieren.

   Netzwerkisolationsausschlüsse aus dem Profil werden der Liste der Netzwerkisolationsausschlüsse hinzugefügt. Sie können die Eigenschaften von Netzwerkverbindungen anzeigen. Bei Bedarf können Sie die Netzwerkverbindungseinstellungen ändern.
8. Fügen Sie bei Bedarf eine Ausnahme für die Netzwerkisolation hinzu. Klicken Sie dazu im Fenster mit der Ausnahmeliste auf **Hinzufügen** → **Hinzufügen** und bearbeiten Sie die Netzwerkverbindungseinstellungen manuell.
9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine Ausnahme für die Netzwerkisolation im manuellen Modus hinzu

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.

   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie die Registerkarte **Aufgaben** aus.

   Dadurch wird die Liste der auf dem Computer verfügbaren Aufgaben angezeigt.
4. Wählen Sie die Aufgabe **Netzwerkisolation** aus.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf **Ausnahmen**.
7. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf **Aus Profil hinzufügen** wählen Sie Standard-Netzwerkprofile zur Konfiguration von Ausschlüssen.

   Netzwerkisolationsausschlüsse aus dem Profil werden der Liste der Netzwerkisolationsausschlüsse hinzugefügt. Sie können die Eigenschaften von Netzwerkverbindungen anzeigen. Bei Bedarf können Sie die Netzwerkverbindungseinstellungen ändern.
8. Fügen Sie bei Bedarf eine Ausnahme für die Netzwerkisolation hinzu. Klicken Sie dazu im Fenster mit der Ausnahmeliste auf **Hinzufügen** und bearbeiten Sie die Netzwerkverbindungseinstellungen manuell.
9. Speichern Sie die vorgenommenen Änderungen.

Sie können mit der Befehlszeile auch die Ausschlussliste der Netzwerkisolationen lokal einsehen. Dabei muss der Computer isoliert sein.

Ab Kaspersky Endpoint Security 12.10 für Windows können Sie Ausnahmen für die Netzwerkisolation über die Warnungsdetails hinzufügen. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

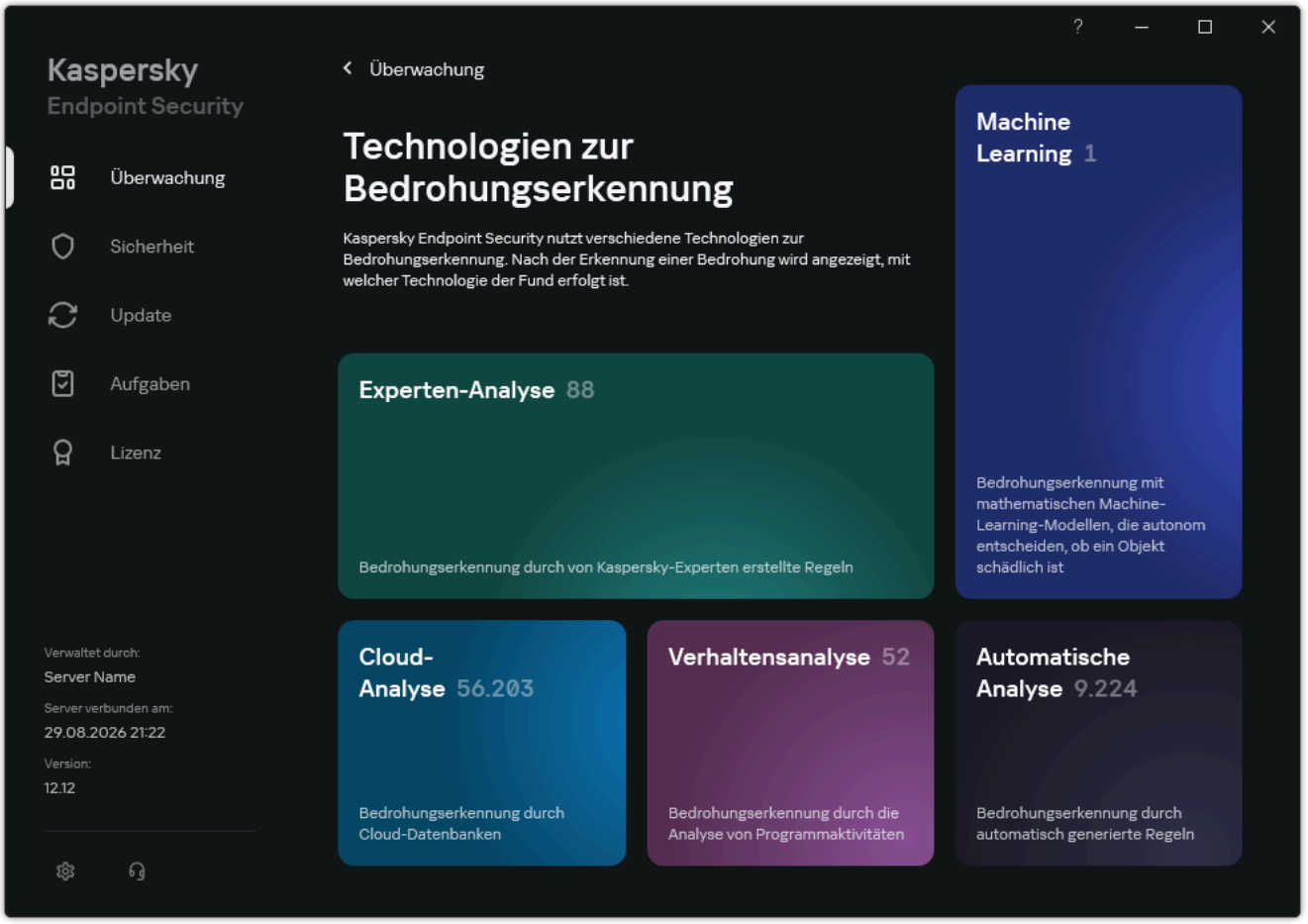
Cloud Sandbox

Mit der Technologie *Cloud Sandbox* können Sie komplexe Bedrohungen auf einem Computer erkennen. Kaspersky Endpoint Security leitet erkannte Dateien automatisch zur Analyse an „Cloud Sandbox“ weiter. „Cloud Sandbox“ führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivität zu erkennen, und entscheidet dann über ihre Reputation. Daten über diese Dateien werden an Kaspersky Security Network gesendet. Wenn „Cloud Sandbox“ eine schädliche Datei gefunden hat, führt Kaspersky Endpoint Security die passende Aktion aus, um diese Bedrohung auf allen Computern, auf denen die Bedrohung vorliegt, zu beseitigen.

Damit „Cloud Sandbox“ funktioniert, müssen Sie die Verwendung von Kaspersky Security Network aktivieren.

Wenn Sie Kaspersky Private Security Network verwenden, ist die „Cloud Sandbox“-Technologie nicht verfügbar.

Die Technologie „Cloud Sandbox“ ist ständig aktiviert und steht allen Benutzern von Kaspersky Security Network zur Verfügung, unabhängig vom Typ der genutzten Lizenz. Wenn Sie die Lösung Endpoint Detection and Response Optimum bereits bereitgestellt haben, können Sie einen separaten Indikator für durch Cloud Sandbox erkannte Bedrohungen aktivieren. Diesen Indikator können Sie verwenden, um bei der Analyse erkannter Bedrohungen Statistiken zu erstellen. Kaspersky Endpoint Security zeigt die Technologie zur Erkennung von Bedrohungen durch Cloud Sandbox im *Bericht über Bedrohungen* in der Kaspersky Security Center-Konsole an.



Bedrohungszähler

Um den „Cloud Sandbox“-Indikator zu aktivieren:

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response**.
5. Wählen Sie die Registerkarte **Cloud Sandbox** aus.

6. Aktivieren Sie den Schalter **Cloud Sandbox AKTIVIERT**.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Sobald eine Bedrohung erkannt wird, aktiviert Kaspersky Endpoint Security den Indikator für Bedrohungen, die mithilfe von „Cloud Sandbox“ erkannt wurden. Der Indikator befindet sich im Programmhauptfenster unter **Technologien zur Erkennung**. Kaspersky Endpoint Security verweist auch im *Bericht über Bedrohungen* in der Kaspersky Security Center-Konsole auf die „Cloud Sandbox“-Bedrohungserkennungstechnologie.

Richtlinienabschnitt für Endpoint Detection and Response

Leitfaden zur Migration von KEA zu KES für EDR Optimum

Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten für die Lösung Kaspersky Endpoint Detection and Response Optimum. Sie benötigen Kaspersky Endpoint Agent nicht mehr als separate Anwendung, um mit EDR Optimum zu arbeiten. Alle Funktionen von Kaspersky Endpoint Agent werden von Kaspersky Endpoint Security ausgeführt.

Wenn Sie Kaspersky Endpoint Security auf Computern bereitstellen, auf denen Kaspersky Endpoint Agent installiert ist, funktioniert die Kaspersky Endpoint Detection and Response Optimum-Lösung weiterhin mit Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt. Das System verhält sich gleich, wenn Sie Kaspersky Endpoint Security auf Version 11.7.0 oder höher aktualisieren.

Kaspersky Endpoint Security ist nicht mit Kaspersky Endpoint Agent kompatibel. Sie können diese beiden Apps nicht mehr auf demselben Computer installieren.

Damit Kaspersky Endpoint Security als Teil von Kaspersky Endpoint Detection and Response Optimum funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Endpoint Detection and Response Optimum 2.0 oder höher.
- Kaspersky Security Center Version 13.2 oder höher (einschließlich Administrationsagent). In älteren Versionen von Kaspersky Security Center kann die EDR Optimum-Funktion nicht aktiviert werden.
- EDR Optimum kann nur über Kaspersky Security Center Cloud Console verwaltet werden.
- Die Datenübertragung an den Administrationsserver ist aktiviert. Diese Daten sind erforderlich, um via Web Console Informationen zu Dateien abzurufen, die sich auf dem Computer in der Quarantäne befinden.
- Es wird eine Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver hergestellt. Damit EDR Optimum mit dem Administrationsserver über Kaspersky Security Center Web Console funktioniert, müssen Sie eine neue sichere *Hintergrundverbindung* herstellen.

Schritte für die Migration der Konfiguration [KES KEA] zu [KES+built-in agent] für EDR Optimum

1. **Upgrade des Web-Plug-ins für Kaspersky Endpoint Security**

   Die Komponente EDR Optimum kann mit dem Web-Plug-in von Kaspersky Endpoint Security Version 11.7.0 oder höher verwaltet werden.

2 Migration von Richtlinien und Aufgaben

Übertragen Sie die Einstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security für Windows. Verwenden Sie dazu den Assistenten für die Migration von Kaspersky Endpoint Agent in der Web Console.

So migrieren Sie Richtlinien- und Aufgabeneinstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security über die Web Console

Wählen Sie im „Web Console"-Hauptfenster den Punkt **Vorgänge** → **Migration von Kaspersky Endpoint Agent** aus.

Dadurch wird der Migrations-Assistent für Richtlinien und Aufgaben ausgeführt. Folgen Sie den Anweisungen.

Schritt 1. Migration der Richtlinien

Der Migrationsassistent erstellt eine neue Richtlinie, die die Einstellungen der Richtlinien von Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammenführt. Wählen Sie in der Richtlinienliste jene Richtlinien von Kaspersky Endpoint Agent aus, deren Einstellungen Sie mit der Richtlinie von Kaspersky Endpoint Security zusammenführen möchten. Klicken Sie auf eine Richtlinie von Kaspersky Endpoint Agent, um die Richtlinie von Kaspersky Endpoint Security auszuwählen, mit der Sie die Einstellungen zusammenführen möchten. Stellen Sie sicher, dass Sie die korrekten Richtlinien ausgewählt haben, und gehen Sie weiter zum nächsten Schritt

Schritt 2. Aufgabenmigration

Der Migrations-Assistent erstellt neue Aufgaben für Kaspersky Endpoint Security. Wählen Sie in der Aufgabenliste die Aufgaben von Kaspersky Endpoint Agent, die Sie für die Kaspersky Endpoint Security-Richtlinie erstellen möchten. Weiter zum nächsten Schritt

Schritt 3. Assistent abschließen

Schließen Sie den Assistenten ab. Als Ergebnis geht der Assistent wie folgt vor:

- Er erstellt eine neue Richtlinie für Kaspersky Endpoint Security.

  Die Richtlinie führt Einstellungen Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammen. Die Richtlinie heißt *<Kaspersky Endpoint Security-Richtlinienname> & <Kaspersky Endpoint Agent-Richtlinienname>*. Die neue Richtlinie hat den Status *Inaktiv*. Um fortzufahren, ändern Sie den Status der Richtlinien von Kaspersky Endpoint Agent und Kaspersky Endpoint Security in *Inaktiv* und aktivieren Sie die neue zusammengeführte Richtlinie.

  Stellen Sie nach der Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für Windows sicher, dass in der neuen Richtlinie die Funktion der Datenübertragung zum Administrationsserver (Daten zu Quarantänedateien und Daten zur Entwicklungskette der Bedrohung) eingerichtet ist. Es erfolgt keine Migration der Werte der Datenübertragungseinstellungen von den Richtlinien von Kaspersky Endpoint Agent.

- Er erstellt Aufgaben für Kaspersky Endpoint Security.

  Neue Aufgaben sind Kopien der Kaspersky Endpoint Agent-Aufgaben. Gleichzeitig lässt der Assistent die Aufgaben von Kaspersky Endpoint Agent unverändert.

3. **Lizenzierung der Funktionalität von EDR Optimum**

   Wenn Sie eine allgemeine Lizenz für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security zur Aktivierung von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Agent verwenden, wird nach dem Anwendungs-Upgrade auf Version 11.7.0 oder höher die EDR Optimum-Funktionalität automatisch aktiviert. Sie müssen keine zusätzlichen Aktionen ausführen.

   Wenn Sie eine eigenständige Lizenz für Kaspersky Endpoint Detection and Response Optimum Add-on zur Aktivierung der Funktionalität „EDR Optimum“ verwenden, müssen Sie sicherstellen, dass der Schlüssel für EDR Optimum zum Schlüsselspeicher von Kaspersky Security Center hinzugefügt und die Funktion zur automatischen Verteilung von Lizenzschlüsseln aktiviert ist. Nach dem Anwendungs-Upgrade auf Version 11.7.0 oder höher wird die EDR Optimum-Funktionalität automatisch aktiviert.

   Wenn Sie Kaspersky Endpoint Agent mit einer Lizenz für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security aktivieren und eine andere Lizenz zur Aktivierung von Kaspersky Endpoint Security für Windows verwenden, müssen Sie den Schlüssel für Kaspersky Endpoint Security für Windows mit dem gewöhnlichen Schlüssel für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security ersetzen. Sie können den Schlüssel mithilfe der Aufgabe *Schlüssel hinzufügen* ersetzen.

4. **Installation und Upgrade von Kaspersky Endpoint Security**

   Um die EDR Optimum-Funktionalität während einer Installation oder eines Upgrades der Anwendung zu migrieren, sollten Sie die Aufgabe zur Remote-Installation verwenden. Beim Erstellen einer Aufgabe zur Remote-Installation müssen Sie die Komponente EDR Optimum in den Einstellungen des Installationspakets auswählen.

   Sie können das Programm auch mit den folgenden Methoden upgraden:

   - Verwendung des Kaspersky-Update-Dienstes.
   - Lokal mithilfe des Installationsassistenten für das Programm.

   Kaspersky Endpoint Security unterstützt die automatische Komponentenauswahl, wenn ein Programm-Upgrade auf einem Computer ausgeführt wird, auf dem das Programm „Kaspersky Endpoint Agent“ installiert ist. Die automatische Komponentenauswahl ist abhängig von den Berechtigungen des Benutzerkontos, unter dem das Programm upgegradet wird.

   Wenn Sie Kaspersky Endpoint Security mithilfe der EXE- oder MSI-Datei unter dem Systemkonto (SYSTEM) upgraden, erhält Kaspersky Endpoint Security Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. Ist auf dem Computer beispielsweise Kaspersky Endpoint Agent installiert und die Lösung „EDR Optimum“ aktiviert, so konfiguriert das Kaspersky Endpoint Security-Installationsprogramm automatisch die Komponentenauswahl und wählt die Komponente „EDR Optimum“ aus. Dadurch wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent. Gewöhnlich wird das MSI-Installationsprogramm unter dem Systemkonto (SYSTEM) ausgeführt, wenn ein Upgrade über den Kaspersky-Update-Dienst erfolgt oder wenn ein Installationspaket über Kaspersky Security Center bereitgestellt wird.

   Wenn Sie Kaspersky Endpoint Security mithilfe einer MSI-Datei unter einem Benutzerkonto ohne Administratorrechte upgraden, hat Kaspersky Endpoint Security keinen Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. In diesem Fall wählt Kaspersky Endpoint Security die Komponenten automatisch auf Basis der Kaspersky Endpoint Agent-Konfiguration aus. Anschließend wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

   > Kaspersky Endpoint Security unterstützt ein Upgrade ohne Neustart des Computers. Sie können den Modus für das App-Upgrade in den Richtlinieneigenschaften auswählen.

5. **Überprüfung des App-Betriebs**

Falls der Computer nach der App-Installation oder dem Upgrade in der Konsole von Kaspersky Security Center den Status *Kritisch* anzeigt:

- Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
- Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*. Falls eine Komponente den Status *Nicht durch Lizenz abgedeckt* hat, stellen Sie sicher, dass Sie die Funktionalität des integrierten Agenten aktiviert haben.
- Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

Kaspersky Sandbox



Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten zur Integration mit der Lösung Kaspersky Sandbox. 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.

Integration des integrierten Agenten in Kaspersky Sandbox

Für die Integration in die Komponente Kaspersky Sandbox muss die Sandbox-Komponente hinzugefügt werden. Sie können die Komponente „Sandbox" während der Installation oder dem Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Um die Komponente zu verwenden, müssen folgende Bedingungen erfüllt sein:

- Kaspersky Security Center 13.2 In älteren Versionen von Kaspersky Security Center können keine eigenständigen IOC-Untersuchungsaufgaben zur Reaktion auf Bedrohungen erstellt werden.
- Die Komponente kann nur über die „Web Console" verwaltet werden. Sie können diese Komponente nicht mit der Verwaltungskonsole (MMC) verwalten.
- Die Anwendung ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Die Datenübertragung an den Administrationsserver ist aktiviert.

  Um alle Funktionen von Kaspersky Sandbox nutzen zu können, muss die Übertragung von Daten zu Quarantänedateien aktiviert sein. Diese Daten sind erforderlich, um via Web Console Informationen zu Dateien abzurufen, die sich auf dem Computer in der Quarantäne befinden. So können Sie z. B. in Web Console eine Datei aus der Quarantäne zur Analyse herunterladen.

  So aktivieren Sie die Datenübertragung zum Administrationsserver in Web Console

  1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
  2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

     Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → KSC-Integration**.
5. Aktivieren Sie im Block **Datenübertragung an den Administrationsserver** das Kontrollkästchen **Über Quarantäne-Dateien**.
6. Speichern Sie die vorgenommenen Änderungen.

- Es wird eine Hintergrundverbindung zwischen „Kaspersky Security Center Web Console“ und dem Administrationsserver hergestellt.

  Damit „Kaspersky Sandbox“ mit dem Administrationsserver über „Kaspersky Security Center Web Console“ funktioniert, müssen Sie eine neue sichere *Hintergrundverbindung* herstellen. Einzelheiten zur Integration von Kaspersky Security Center mit anderen Lösungen finden Sie in der Hilfe zu Kaspersky Security Center.

  Erstellung einer Hintergrundverbindung in Web Console

  1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Einstellungen → Integration** aus.
  2. Wechseln Sie zum Abschnitt **Integration**.
  3. Aktivieren Sie den Schalter **Background-Verbindung für die Integration Aktiviert**.
  4. Speichern Sie die vorgenommenen Änderungen.

  Wenn keine Hintergrundverbindung zwischen „Kaspersky Security Center Web Console“ und dem Administrationsserver hergestellt wird, können eigenständige IOC-Untersuchungsaufgaben nicht als Teil von „Threat Response“ erstellt werden.

- Um eine vertrauenswürdige Verbindung mit dem Sandbox-Server zu konfigurieren, müssen Sie ein TLS-Zertifikat erstellen. Anschließend müssen Sie das Zertifikat mithilfe einer Richtlinie dem Computer hinzufügen. Außerdem müssen Sie das Zertifikat zum Sandbox-Server hinzufügen.

  > Die Zwei-Wege-Authentifizierung mithilfe eines Krypto-Containers ist für Kaspersky Sandbox nicht verfügbar.

  Ein TLS-Zertifikat können Sie in der „Web Console“ oder lokal über die Befehlszeile hinzufügen.

- Die Komponente „Kaspersky Sandbox“ ist aktiviert.
- Die Programmkomponenten, die den Sandbox-Betrieb sicherstellen, sind aktiviert und betriebsbereit. Die folgenden Komponenten gewährleisten den Betrieb der Sandbox:
  - Schutz vor bedrohlichen Dateien.
  - Programm-Überwachung.
  - Firewall.
  - AMSI-Schutz.
  - Untersuchung im Hintergrund.

Um die Integration mit „Kaspersky Sandbox“ zu aktivieren oder zu deaktivieren:

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten → Sandbox**.
5. Verwenden Sie den Schalter **Integration it Sandbox AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Wählen Sie im Block **Integrationsmodus** den Betriebsmodus der Komponente: **Kaspersky Sandbox**.
7. Klicken Sie auf den Link **Verbindungseinstellungen**.

   Dadurch wird das Fenster für die Einstellungen der Verbindung mit den „Sandbox“-Servern geöffnet.
8. Klicken Sie im Block **TLS-Serverzertifikat** auf **Hochladen** und wählen Sie die TLS-Zertifikatsdatei aus.

   Kaspersky Endpoint Security kann nur ein TLS-Zertifikat für einen „Sandbox“-Server haben. Wenn Sie bereits ein TLS-Zertifikat hinzugefügt haben, wird dieses Zertifikat widerrufen. Nur das zuletzt hinzugefügte Zertifikat wird verwendet.
9. Konfigurieren Sie die erweiterten Verbindungseinstellungen für Sandbox-Server:

   - **Timeout (ms)**. Verbindungstimeout für den Sandbox-Server. 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.
10. Klicken Sie im Block **Verbindung mit Sandbox-Servern** auf **Hinzufügen**.
11. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster die Serveradresse (IPv4, IPv6, DNS) und den Port für Sandbox ein.

    Einzelheiten zur Bereitstellung virtueller Images und zur Konfiguration von Kaspersky Sandbox-Servern finden Sie in der Hilfe zu Kaspersky Sandbox.
12. Speichern Sie die vorgenommenen Änderungen.

Daraufhin überprüft Kaspersky Endpoint Security das TLS-Zertifikat. Wenn das Zertifikat erfolgreich verifiziert wurde, lädt Kaspersky Endpoint Security das Zertifikat bei der nächsten Synchronisierung mit Kaspersky Security Center auf den Computer hoch. Wenn Sie zwei TLS-Zertifikate hinzugefügt haben, verwendet Kaspersky Sandbox beim Herstellen einer vertrauenswürdigen Verbindung das aktuellere Zertifikat. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Sandbox** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Sie können die Integration mit „Kaspersky Sandbox“ in der „Web Console“ oder lokal über die Befehlszeile aktivieren oder deaktivieren.

Kaspersky Endpoint Security speichert Informationen über die Komponente „Kaspersky Sandbox“ in einem Bericht. Der Bericht enthält auch Informationen über Fehler. Wenn Sie eine Fehlermeldung mit einer Beschreibung im Format `Error code: XXX` (zum Beispiel `0xa67b01f4`) erhalten, wenden Sie sich an den Technischen Support.

Untersuchung auf Kompromittierungsindikatoren (eigenständige Aufgabe)

Ein *Kompromittierungsindikator (IOC)* ist ein Datensatz, der sich auf ein Objekt oder eine Aktivität bezieht und der auf unbefugten Zugriff auf den Computer (Kompromittierung von Daten) hinweist. Beispielsweise können viele erfolglose Versuche, sich beim System anzumelden, einen Kompromittierungsindikator darstellen. Mithilfe der Aufgabe *IOC-Untersuchung* können Kompromittierungsindikatoren auf dem Computer gefunden und Maßnahmen zur Reaktion auf Bedrohungen ergreifen werden.

Kaspersky Endpoint Security sucht mithilfe von IOC-Dateien nach Kompromittierungsindikatoren. *IOC-Dateien* sind Dateien, die Sätze von Indikatoren enthalten, mit denen die Anwendung nach Übereinstimmungen sucht. IOC-Dateien müssen dem OpenIOC-Standard entsprechen. Kaspersky Endpoint Security generiert automatisch IOC-Dateien für „Kaspersky Sandbox“.

Ausführungsmodus der Aufgabe IOC-Untersuchung

Das Programm erstellt eigenständige IOC-Untersuchungsaufgaben für „Kaspersky Sandbox“. Eine *eigenständige IOC-Untersuchungsaufgabe* ist eine Gruppenaufgabe, die automatisch erstellt wird, wenn auf eine durch „Kaspersky Sandbox“ erkannte Bedrohung reagiert wird. Kaspersky Endpoint Security erstellt die IOC-Datei automatisch. Benutzerdefinierte IOC-Dateien werden nicht unterstützt. Aufgaben werden 30 Tage nach dem Erstellen automatisch gelöscht. Weitere Informationen zu eigenständigen IOC-Untersuchungsaufgaben finden Sie in der Hilfe zur Kaspersky Sandbox.

Einstellungen der Aufgabe IOC-Untersuchung

Kaspersky Sandbox kann als Reaktion auf Bedrohungen automatisch *IOC-Untersuchung*-Aufgaben erstellen und ausführen.

Die Einstellungen können nur über die „Web Console“ konfiguriert werden.

Damit die eigenständigen IOC-Untersuchungsaufgaben von „Kaspersky Sandbox“ funktionieren, benötigen Sie Kaspersky Security Center 13.2.

Um die Einstellungen der Aufgabe IOC-Untersuchung zu ändern:

1. Wählen Sie im Hauptfenster der Web Console **Aufgaben** aus.

   Die Aufgabenliste wird geöffnet.

2. Klicken Sie auf die Kaspersky Endpoint Security-Aufgabe **IOC-Untersuchung**.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wechseln Sie zum Abschnitt **IOC-Untersuchungseinstellungen**.

5. Passen Sie die Aktionen bei der IOC-Erkennung an:

   - **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 Objekts gelöscht wird, erstellt Kaspersky Endpoint Security eine Backup-Kopie für den Fall, dass das Objekt später wiederhergestellt werden muss. 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. Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden Prozesse und die Bootsektoren.

   - **Nur ausführen, wenn der Computer inaktiv ist**. Schiebt den Start der Aufgabe auf, wenn die Computerressourcen ausgelastet sind. Kaspersky Endpoint Security startet die Untersuchungsaufgabe, wenn der Computer gesperrt oder der Bildschirmschoner eingeschaltet ist. Wenn Sie die Aufgabenausführung unterbrochen haben (z. B. den Computer entsperrt haben), führt Kaspersky Endpoint Security die Aufgabe automatisch aus und setzt sie an der Stelle fort, an der sie unterbrochen wurde. Mit dieser Zeitplanoption können Sie die Computerressourcen schonen, während der Computer verwendet wird.

6. Speichern Sie die vorgenommenen Änderungen.

Die Ergebnisse der Aufgabe können Sie in den Aufgabeneigenschaften im Abschnitt **Ergebnisse** einsehen. Sie können die Informationen zu erkannten Kompromittierungsindikatoren in den Aufgabeneigenschaften anzeigen: **Anwendungseinstellungen** → **IOC-Untersuchungsergebnisse**.

IOC-Untersuchungsergebnisse werden für 30 Tage gespeichert. Nach diesem Zeitraum löscht Kaspersky Endpoint Security automatisch die ältesten Einträge.

Leitfaden zur Migration von KEA zu KES für Kaspersky Sandbox

Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten für die Lösung Kaspersky Sandbox. Sie benötigen Kaspersky Endpoint Agent nicht mehr als separate Anwendung, um mit Kaspersky Sandbox zu arbeiten. Alle Funktionen von Kaspersky Endpoint Agent werden von Kaspersky Endpoint Security ausgeführt.

Wenn Sie Kaspersky Endpoint Security auf Computern bereitstellen, auf denen Kaspersky Endpoint Agent installiert ist, funktioniert die Kaspersky Sandbox-Lösung weiterhin mit Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt. Das System verhält sich gleich, wenn Sie Kaspersky Endpoint Security auf Version 11.7.0 oder höher aktualisieren.

Kaspersky Endpoint Security ist nicht mit Kaspersky Endpoint Agent kompatibel. Sie können diese beiden Apps nicht mehr auf demselben Computer installieren.

Damit Kaspersky Endpoint Security als Teil von Kaspersky Sandbox funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Sandbox Version 2.0 oder höher.
- Kaspersky Security Center Version 13.2 oder höher (einschließlich Administrationsagent). In älteren Versionen von Kaspersky Security Center kann die Funktion „Kaspersky Sandbox“ nicht aktiviert werden.
- Kaspersky Sandbox kann nur über Kaspersky Security Center Web Console verwaltet werden.
- Die Datenübertragung an den Administrationsserver ist aktiviert. Diese Daten sind erforderlich, um via Web Console Informationen zu Dateien abzurufen, die sich auf dem Computer in der Quarantäne befinden.
- Es wird eine Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver hergestellt. Damit „Kaspersky Sandbox“ mit dem Administrationsserver über „Kaspersky Security Center Web Console“ funktioniert, müssen Sie eine neue sichere *Hintergrundverbindung* herstellen.

Schritte für die Migration der Konfiguration [KES+KEA] zu [KES+built-in agent] für Kaspersky Sandbox

1. **Upgrade des Web-Plug-ins für Kaspersky Endpoint Security**

   Die Komponente Kaspersky Sandbox kann mit dem Web-Plug-in von Kaspersky Endpoint Security Version 11.7.0 oder höher verwaltet werden.

2. **Migration von Richtlinien und Aufgaben**

   Übertragen Sie die Einstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security für Windows. Verwenden Sie dazu den Assistenten für die Migration von Kaspersky Endpoint Agent in der Web Console.

   So migrieren Sie Richtlinien- und Aufgabeneinstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security über die Web Console

   Wählen Sie im „Web Console“-Hauptfenster den Punkt **Vorgänge** → **Migration von Kaspersky Endpoint Agent** aus.

   Dadurch wird der Migrations-Assistent für Richtlinien und Aufgaben ausgeführt. Folgen Sie den Anweisungen.

Schritt 1. Migration der Richtlinien

Der Migrationsassistent erstellt eine neue Richtlinie, die die Einstellungen der Richtlinien von Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammenführt. Wählen Sie in der Richtlinienliste jene Richtlinien von Kaspersky Endpoint Agent aus, deren Einstellungen Sie mit der Richtlinie von Kaspersky Endpoint Security zusammenführen möchten. Klicken Sie auf eine Richtlinie von Kaspersky Endpoint Agent, um die Richtlinie von Kaspersky Endpoint Security auszuwählen, mit der Sie die Einstellungen zusammenführen möchten. Stellen Sie sicher, dass Sie die korrekten Richtlinien ausgewählt haben, und gehen Sie weiter zum nächsten Schritt

Schritt 2. Aufgabenmigration

Der Migrations-Assistent erstellt neue Aufgaben für Kaspersky Endpoint Security. Wählen Sie in der Aufgabenliste die Aufgaben von Kaspersky Endpoint Agent, die Sie für die Kaspersky Endpoint Security-Richtlinie erstellen möchten. Weiter zum nächsten Schritt

Schritt 3. Assistent abschließen

Schließen Sie den Assistenten ab. Als Ergebnis geht der Assistent wie folgt vor:

- Er erstellt eine neue Richtlinie für Kaspersky Endpoint Security.

  Die Richtlinie führt Einstellungen Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammen. Die Richtlinie heißt *<Kaspersky Endpoint Security-Richtlinienname> & <Kaspersky Endpoint Agent-Richtlinienname>*. Die neue Richtlinie hat den Status *Inaktiv*. Um fortzufahren, ändern Sie den Status der Richtlinien von Kaspersky Endpoint Agent und Kaspersky Endpoint Security in *Inaktiv* und aktivieren Sie die neue zusammengeführte Richtlinie.

  Stellen Sie nach der Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für Windows sicher, dass in der neuen Richtlinie die Funktion der Datenübertragung zum Administrationsserver (Daten zu Quarantänedateien und Daten zur Entwicklungskette der Bedrohung) eingerichtet ist. Es erfolgt keine Migration der Werte der Datenübertragungseinstellungen von den Richtlinien von Kaspersky Endpoint Agent.

- Er erstellt Aufgaben für Kaspersky Endpoint Security.

  Neue Aufgaben sind Kopien der Kaspersky Endpoint Agent-Aufgaben. Gleichzeitig lässt der Assistent die Aufgaben von Kaspersky Endpoint Agent unverändert.

3. **Lizenzierung der Kaspersky Sandbox-Funktionalität**

   Um Kaspersky Endpoint Security als Teil der Kaspersky Sandbox-Lösung zu aktivieren, benötigen Sie eine separate Lizenz für das Kaspersky Sandbox-Add-on. Sie können den Schlüssel mithilfe der Aufgabe *Schlüssel hinzufügen* hinzufügen. Dadurch werden der Anwendung zwei Schlüssel hinzugefügt: *Kaspersky Endpoint Security* und *Kaspersky Sandbox*.

4. **Installation und Upgrade von Kaspersky Endpoint Security**

Um die Funktionalität von Kaspersky Sandbox während einer Installation oder eines Upgrades der Anwendung zu migrieren, sollten Sie die Aufgabe zur Remote-Installation verwenden. Beim Erstellen einer Aufgabe zur Remote-Installation müssen Sie die Komponente Kaspersky Sandbox in den Einstellungen des Installationspakets auswählen.

Sie können das Programm auch mit den folgenden Methoden upgraden:

- Verwendung des Kaspersky-Update-Dienstes.
- Lokal mithilfe des Installationsassistenten für das Programm.

Kaspersky Endpoint Security unterstützt die automatische Komponentenauswahl, wenn ein Programm-Upgrade auf einem Computer ausgeführt wird, auf dem das Programm „Kaspersky Endpoint Agent“ installiert ist. Die automatische Komponentenauswahl ist abhängig von den Berechtigungen des Benutzerkontos, unter dem das Programm upgegradet wird.

Wenn Sie Kaspersky Endpoint Security mithilfe der EXE- oder MSI-Datei unter dem Systemkonto (SYSTEM) upgraden, erhält Kaspersky Endpoint Security Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. Ist auf dem Computer beispielsweise Kaspersky Endpoint Agent installiert und die Kaspersky Sandbox-Lösung aktiviert, so konfiguriert das Kaspersky Endpoint Security-Installationsprogramm automatisch die Komponentenauswahl und wählt die Kaspersky Sandbox-Komponente aus. Dadurch wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent. Gewöhnlich wird das MSI-Installationsprogramm unter dem Systemkonto (SYSTEM) ausgeführt, wenn ein Upgrade über den Kaspersky-Update-Dienst erfolgt oder wenn ein Installationspaket über Kaspersky Security Center bereitgestellt wird.

Wenn Sie Kaspersky Endpoint Security mithilfe einer MSI-Datei unter einem Benutzerkonto ohne Administratorrechte upgraden, hat Kaspersky Endpoint Security keinen Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. In diesem Fall wählt Kaspersky Endpoint Security die Komponenten automatisch auf Basis der Kaspersky Endpoint Agent-Konfiguration aus. Anschließend wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

Kaspersky Endpoint Security unterstützt ein Upgrade ohne Neustart des Computers. Sie können den Modus für das App-Upgrade in den Richtlinieneigenschaften auswählen.

5 Überprüfung des App-Betriebs

Falls der Computer nach der App-Installation oder dem Upgrade in der Konsole von Kaspersky Security Center den Status *Kritisch* anzeigt:

- Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
- Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*. Falls eine Komponente den Status *Nicht durch Lizenz abgedeckt* hat, stellen Sie sicher, dass Sie die Funktionalität des integrierten Agenten aktiviert haben.
- Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security für Windows unterstützt die Arbeit mit 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“. Die App enthält integrierte Agenten für die EDR- und NDR-Komponenten. Die App unterstützt auch die Arbeit mit dem Sandbox-Komponente, die zu KATA gehört.

Threat Intelligence-Tools

Kaspersky Endpoint Detection and Response verwendet die folgenden Threat Intelligence-Tools:

- Integration in Kaspersky Threat Intelligence Portal, das Informationen über die Reputation von Dateien und Webadressen enthält und anzeigt.
- Kaspersky Threats-Datenbank.
- Die Cloud-Service-Infrastruktur von Kaspersky Security Network (im Folgenden auch „KSN“ genannt), die Echtzeitzugriff auf Datei-, Website- und Software-Reputationsinformationen aus der Kaspersky-Wissensdatenbank bietet. Durch die Verwendung von Daten aus Kaspersky Security Network wird die Reaktion der Kaspersky-Programme auf Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

Funktionsweise der Lösung

Kaspersky Endpoint Security wird auf den einzelnen Computern einer IT-Unternehmensinfrastruktur installiert und überwacht kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien. Informationen über Ereignisse auf dem Computer (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.

Kaspersky Endpoint Security-Konfigurationen für die Arbeit mit EDR / NDR (KATA)

Die folgenden Konfigurationen können für die Arbeit mit EDR / NDR (KATA) verwendet werden:

- **[KES+built-in agent]**. In dieser Konfiguration dient Kaspersky Endpoint Security sowohl als Programm, das die Sicherheit des Computers gewährleistet, als auch als Programm für die Interaktion mit EDR / NDR (KATA). Der integrierte Agent für EDR (KATA) ist in Kaspersky Endpoint Security 12.1 für Windows oder höher verfügbar. Der integrierte Agent für NDR (KATA) ist in Kaspersky Endpoint Security 12.7 für Windows oder höher verfügbar.

- **[third-party EPP+EDR Agent]**. In dieser Konfiguration wird die Sicherheit der IT-Infrastruktur durch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt. In der Konfiguration Endpoint Detection and Response Agent (EDR Agent) wird die Interaktion mit EDR/NDR (KATA) durch Kaspersky Endpoint Security gewährleistet. In dieser Konfiguration ist EDR Agent mit Drittanbieter-EPP-Anwendungen kompatibel. EDR Agent für EDR (KATA) ist in Kaspersky Endpoint Security 12.3 für Windows oder höher verfügbar. EDR Agent für NDR (KATA) ist in Kaspersky Endpoint Security 12.7 für Windows oder höher verfügbar.

Unterstützung für ältere Versionen von Kaspersky Endpoint Security

Wenn Sie Kaspersky Endpoint Security 11.2.0 – 11.8.0 für die Interoperabilität mit Kaspersky Anti Targeted Attack Platform (EDR) verwenden, ist Kaspersky Endpoint Agent in der Anwendung enthalten. Sie können Kaspersky Endpoint Agent gleichzeitig mit Kaspersky Endpoint Security installieren.

Wenn Sie Kaspersky Endpoint Security 11.9.0 – 12.0 verwenden, müssen Sie Kaspersky Endpoint Agent separat installieren, da das Verteilungspaket von Kaspersky Endpoint Security ab Kaspersky Endpoint Security 11.9.0 nicht mehr Teil der Distribution von Kaspersky Endpoint Security ist.

Integration des integrierten Agenten in EDR / NDR (KATA)

Für die Integration in EDR bzw. NDR (KATA) müssen Sie die entsprechende Komponente hinzufügen: Endpoint Detection and Response (KATA) oder Network Detection and Response (KATA). Sie können die Komponenten für die Integration in EDR bzw. NDR (KATA) entweder während der Installation oder beim Upgrade der App auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Ab Kaspersky Endpoint Security für Windows Version 12.11 hat die Komponente EDR (KATA) den neuen Namen **Endpoint Detection and Response Expert (ab Version 8.0)**. In dieser Programmversion ist die Komponente kompatibel mit Kaspersky Anti Targeted Attack Platform 7.1 und älteren Versionen sowie mit Kaspersky Endpoint Detection and Response Expert (on-premises).

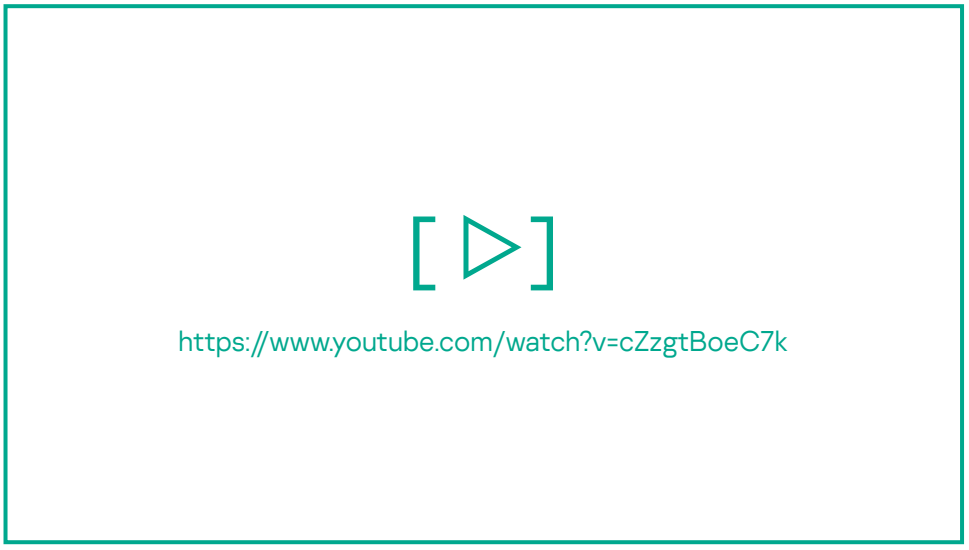
Die Komponenten Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) und Endpoint Detection and Response Expert (on-premises) sind nicht miteinander kompatibel.

Für die Verwendung von EDR bzw. NDR (KATA) müssen folgende Bedingungen erfüllt sein:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform Versionen 5.0 –7.1.

- NDR (KATA): Kaspersky Anti Targeted Attack Platform Version 7.0 oder höher.

- EDR (KATA): Kaspersky Endpoint Security für Windows 12.1 oder höher. Weitere Informationen zur Kompatibilität von KATA mit verschiedenen Versionen von Kaspersky Endpoint Security finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.
- NDR (KATA): Kaspersky Endpoint Security für Windows 12.7 oder höher.
- Kaspersky Security Center Version 14.2 oder höher. In älteren Versionen von Kaspersky Security Center kann die Funktionalität EDR bzw. NDR (KATA) nicht aktiviert werden.
- Die Anwendung ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Die Komponenten Endpoint Detection and Response (KATA) und Network Detection and Response (KATA) sind aktiviert.
- Die App-Komponenten, die den Betrieb von EDR bzw. NDR (KATA) sicherstellen, sind aktiviert und betriebsbereit. Die folgenden Komponenten gewährleisten den Betrieb von EDR / NDR (KATA):
  - 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.



https://www.youtube.com/watch?v=cZzgtBoeC7k

https://www.youtube.com/watch?v=gd-rySv0ThQ

Die Integration in Endpoint Detection and Response (KATA) umfasst die folgenden Schritte:

1. **Installieren der Komponenten Endpoint Detection and Response (KATA) und Network Detection and Response (KATA)**

   Sie können die Komponenten EDR (KATA) und NDR (KATA) entweder während der Installation oder beim Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   Sie müssen Ihren Computer neu starten, um das Upgrade des Programms mit den neuen Komponenten abzuschließen.

2. **Aktivieren von Endpoint Detection and Response (KATA) und Network Detection and Response (KATA)**

   Sie müssen eine separate Lizenz für EDR (KATA) und NDR (KATA) kaufen (Add-on für Kaspersky Endpoint Detection and Response (KATA)).

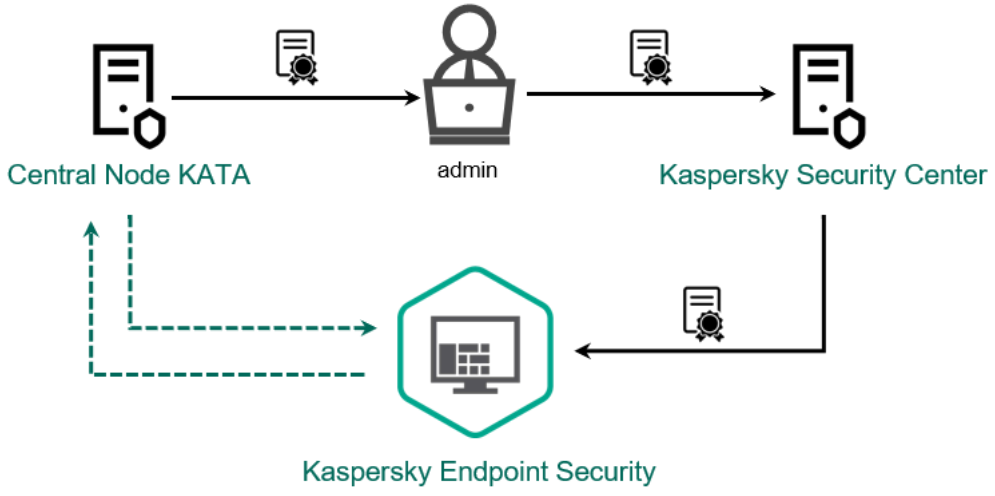
   Die Funktionalität ist verfügbar, nachdem ein separater Schlüssel hinzugefügt wurde, der die Funktionalität EDR (KATA) und NDR (KATA) abdeckt. Dadurch werden mehrere Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security sowie die Schlüssel für Kaspersky Endpoint Detection and Response (KATA) und Network Detection and Response (KATA).

   Die Lizenzverwaltung für die eigenständige Funktionalität von EDR (KATA) und NDR (KATA) entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität von EDR (KATA) und NDR (KATA) in der Lizenz enthalten ist und in der lokalen App-Oberfläche ausgeführt wird.

3. **Verbindung zu Central Node**

   Kaspersky Anti Targeted Attack Platform erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und der Komponente Central Node. Zur Konfiguration einer vertrauenswürdigen Verbindung müssen Sie ein TLS-Zertifikat verwenden. 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). Anschließend müssen Sie das TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen (siehe Anleitung unten).



TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen

Standardmäßig überprüft Kaspersky Endpoint Security nur das TLS-Zertifikat des Central Node. Um die Verbindung sicherer zu machen, können Sie zusätzlich die Überprüfung des Computers auf dem Central Node (Zwei-Wege-Authentifizierung) aktivieren. Zum Aktivieren dieser Überprüfung müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Central Node und Kaspersky Endpoint Security aktivieren. Zur Verwendung der Zwei-Wege-Authentifizierung benötigen Sie außerdem einen Krypto-Container. 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).

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Verwaltungskonsole (MMC) mit Central Node

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Detection and Response** aus und wählen Sie die Komponente aus, die Sie konfigurieren möchten: **Endpoint Detection and Response Expert (on-premises)** oder **Network Detection and Response (KATA)**.
5. Aktivieren Sie das entsprechende Kontrollkästchen: **Endpoint Detection and Response Expert (Version 7.1 oder älter)** oder **Network Detection and Response (KATA)**.
6. Klicken Sie auf **Einstellungen der Serververbindung**.
7. Konfigurieren Sie die Serververbindung:
   - **Timeout (Sek)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.
   - **TLS-Zertifikat des Servers**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).
   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

     Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.
8. Klicken Sie auf **OK**.

9. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

   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.

10. Konfigurieren Sie, falls erforderlich, die Telemetrie.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Web Console mit Central Node

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zum Abschnitt **Konfiguration der integrierten Agenten** und wählen Sie die Komponente aus, die Sie konfigurieren möchten: **Endpoint Detection and Response Expert (On-Premises)** oder **Network Detection and Response (KATA)**.

5. Aktivieren Sie den entsprechenden Schalter: **Endpoint Detection and Response Expert (On-Premises) AKTIVIERT** oder **Network Detection and Response (KATA) AKTIVIERT**.

6. Um EDR (KATA) zu konfigurieren, wählen in der Liste der Lösungen den Punkt **Endpoint Detection and Response Expert (Version 7.1 oder älter)** aus.

7. Klicken Sie auf **Verbindungseinstellungen**.

8. Konfigurieren Sie die Serververbindung:

   - **Timeout (Sek.)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden.

   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform).

- **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.

  Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

9. Klicken Sie auf **OK**.
10. Fügen Sie Central Node-Server hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

    Sie können mehrere Serveradressen für Central Node hinzufügen. Kaspersky Endpoint Security versucht, sich über die erste IP-Adresse mit dem Server zu verbinden. Wenn keine Verbindung hergestellt werden kann, versucht Kaspersky Endpoint Security eine Verbindung mit der zweiten IP-Adresse in der Liste und so weiter.
11. Konfigurieren Sie, falls erforderlich, die Telemetrie.
12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Ein TLS-Zertifikat können Sie auch lokal über die Befehlszeile hinzufügen.

Dadurch wird der Computer zur Kaspersky Anti Targeted Attack Platform-Konsole hinzugefügt. Überprüfen Sie den Betriebsstatus der Komponenten, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus der Komponenten können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponenten **Endpoint Detection and Response Expert (ab Version 8.0)** und **Network Detection and Response (KATA)** werden zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Den Status der Komponenten können Sie in der Kaspersky Security Center-Konsole in den Computereigenschaften im Abschnitt **Komponenten** überprüfen. Beachten Sie folgende Aspekte, wenn Sie den Status der Komponente in der Konsole überprüfen. Wenn die Komponente nicht installiert ist und die Funktionalität nicht durch Ihre Lizenz abgedeckt ist, zeigt die Konsole den Status **Von der Lizenz nicht unterstützt** an (anstatt **Nicht installiert**).

Ab Kaspersky Endpoint Security 12.6 für Windows können Sie den Status der Komponente EDR (KATA) in der Verwaltungskonsole (MMC) von Kaspersky Security Center überwachen. Der aktuelle Status der Komponente wird in den Computereigenschaften in der Spalte **Status der Komponente "Endpoint Sensor"** angezeigt (*Wird ausgeführt*, *Wird gestartet*, *Beendet*, *Angehalten*, *Fehlgeschlagen*, *Unbekannt*). Die Web Console zeigt den Status von Endpoint Sensor nicht an.

EDR-Telemetrie (KATA) konfigurieren

Telemetrie ist eine Liste von Ereignissen, die auf dem geschützten Computer aufgetreten sind. Kaspersky Endpoint Security analysiert Telemetriedaten und sendet sie während der Synchronisierung an Kaspersky Anti Targeted Attack Platform. Telemetrie-Ereignisse treffen fast kontinuierlich auf dem Server ein. Kaspersky Endpoint Security startet die Synchronisierung mit dem Server, wenn eine der folgenden Bedingungen erfüllt ist:

- Das Synchronisierungsintervall ist abgelaufen.
- Die Anzahl der Ereignisse im Puffer überschreitet die Höchstgrenze.

Dann synchronisiert die App standardmäßig alle 30 Sekunden oder immer, wenn der Puffer 1024 Ereignisse enthält. Sie können das Synchronisierungsverhalten in der Richtlinie von Kaspersky Endpoint Security anpassen und optimale Werte für Ihre Netzwerklast auswählen (siehe Anleitung unten).

Bei fehlender Verbindung zwischen Kaspersky Endpoint Security und dem Server stellt die App neue Ereignisse in die Warteschlange. Sobald die Verbindung wiederhergestellt wird, sendet Kaspersky Endpoint Security die Ereignisse aus der Warteschlange in der richtigen Reihenfolge an den Server. Um eine Überlastung des Servers zu vermeiden, kann Kaspersky Endpoint Security bestimmte Ereignisse überspringen. Diese Option können Sie in den Einstellungen für die Ereignisübertragung optimieren und dafür beispielsweise einen Höchstwert für Ereignisse pro Stunde festlegen (siehe Anleitung unten).

Wenn Sie Kaspersky Anti Targeted Attack Platform zusammen mit einer anderen Lösung verwenden, die ebenfalls Telemetrie verwendet, können Sie die Telemetrie für KATA (EDR) deaktivieren (siehe Anleitung unten). Dadurch lässt sich die Serverlast für diese Lösungen optimieren. Wenn Sie beispielsweise die Managed Detection and Response-Lösung und KATA (EDR) bereitgestellt haben, können Sie MDR-Telemetrie verwenden und Threat Response-Aufgaben in KATA (EDR) erstellen.

So konfigurieren Sie die Telemetrie über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Detection and Response** aus und wählen Sie die Komponente aus, die Sie konfigurieren möchten: **Endpoint Detection and Response Expert (on-premises)** oder **Network Detection and Response (KATA)**.
5. Konfigurieren Sie die Einstellung **Synchronisierungsanfrage an KATA-Server senden alle (Min.)**. Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung sendet Kaspersky Endpoint Security Informationen über geänderte Einstellungen und Aufgaben der App.
6. Stellen Sie sicher, dass das Kontrollkästchen **Telemetriedaten an KATA senden** aktiviert ist.

7. Passen Sie bei Bedarf im Block **Einstellungen für die Datenübertragung** die Synchronisierung mit den Server-Einstellungen an:

   - **Maximale Verzögerung der Ereignisübertragung (Sek.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.

   - **Maximale Anzahl der Ereignispakete**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.

8. Aktivieren Sie, sofern erforderlich, das Kontrollkästchen **Anforderungsbegrenzung aktivieren** im Block **Anforderungsbegrenzung**.

   Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen.

9. Konfigurieren Sie die Optimierungseinstellungen für das Senden von Ereignissen an den Server:

   - **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.

   - **Prozentsatz für die Überschreitung des Ereignislimits**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

10. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die Telemetrie über die Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.

5. Um EDR (KATA) zu konfigurieren, wählen in der Liste der Lösungen den Punkt **Endpoint Detection and Response Expert (Version 7.1 oder älter)** aus.

6. Stellen Sie sicher, dass das Kontrollkästchen **Telemetrie an KATA-Server senden** im Block **Einstellungen für die Datenübertragung** aktiviert ist.

7. Konfigurieren Sie die Einstellung **Synchronisierungsanfrage an Server senden alle (Min.)**. Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung sendet Kaspersky Endpoint Security Informationen über geänderte Einstellungen und Aufgaben der App.

8. Stellen Sie sicher, dass das Kontrollkästchen **Telemetrie an KATA-Server senden** aktiviert ist.

9. Passen Sie bei Bedarf im Block **Einstellungen für die Datenübertragung** die Synchronisierung mit den Server-Einstellungen an:

   - **Maximale Verzögerung der Ereignisübertragung (Sek.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.

   - **Maximale Anzahl der Ereignispakete**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.

10. Aktivieren Sie, sofern erforderlich, das Kontrollkästchen **Anforderungsbegrenzung aktivieren** im Block **Anforderungsbegrenzung**.

    Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen.

11. Konfigurieren Sie die Optimierungseinstellungen für das Senden von Ereignissen an den Server:

    - **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.

    - **Prozentsatz für die Überschreitung des Ereignislimits**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zum Abschnitt **KATA-Integration → Telemetrie-Ausnahmen**.

5. Aktivieren Sie unter **Einstellungen für die Datenübertragung** das Kontrollkästchen **Ausnahmen verwenden**.

6. Klicken Sie auf **Hinzufügen** und konfigurieren Sie die Ausnahmen:

Kriterien werden mit logischem *UND* kombiniert.

- **Pfad**. Vollständiger Pfad der Datei, einschließlich Name und Erweiterung. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. Damit die Ausnahme funktioniert, muss der Dateipfad angegeben werden.
- **Befehlszeile**. Befehl zum Ausführen des Objekts.
- **Beschreibung**. Wert des Parameters FileDescription aus einer RT_VERSION-Ressource (VersionInfo). Weitere Informationen über die VersionInfo-Ressource finden Sie auf der Microsoft-Website.
- **Ursprünglicher Dateiname**. Wert des Parameters OriginalFilename aus einer RT_VERSION-Ressource (VersionInfo).
- **Version**. Wert des Parameters FileVersion aus einer RT_VERSION-Ressource (VersionInfo).
- **MD5**. MD5-Hash der Datei.
- **SHA256**. SHA256-Hash der Datei.
- **Ereignistypen**. Damit die Ausnahme funktioniert, müssen Sie mindestens einen Ereignistyp auswählen.

7. Speichern Sie die vorgenommenen Änderungen.

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.
   Die Aufgabenliste wird geöffnet.
2. Klicken Sie auf **Neue Aufgabe**.

Der Assistent für neue Aufgaben wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Aufgabentyp auswählen

1. Wählen Sie **Kaspersky Endpoint Security für Windows (14.2)** → **Update-Rollback** aus.

Schritt 2. Geräte auswählen, denen die Aufgabe zugewiesen wird

Wählen Sie die Computer aus, auf denen die Aufgabe ausgeführt werden soll. Folgende Varianten stehen zur Auswahl:

- Aufgabe der Administrationsgruppe zuweisen. In diesem Fall wird die Aufgabe jenen Computern zugewiesen, die zu einer früher erstellten Administrationsgruppe gehören.
- Auswahl von Computern, die vom Administrationsserver im Netzwerk gefunden wurden – *nicht zugeordnete Geräte*. In eine Geräteauswahl können Sie sowohl Geräte aus Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.
- Geräteadressen manuell festlegen oder aus einer Liste importieren. Sie können die NetBIOS-Namen, IP-Adressen und IP-Adressbereiche der Geräte festlegen, denen die Aufgabe zugewiesen werden soll.

Schritt 3. Zeitplan des Aufgabenstarts anpassen

Konfigurieren Sie den Aufgabenzeitplan, z. B. mit der Option „manuell“.

Schritt 4. Aufgabennamen festlegen

Geben Sie einen Namen für die Aufgabe ein.

Schritt 7. Erstellung der Aufgabe abschließen

Schließen Sie den Assistenten ab. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**. Den Fortschritt der Aufgabenausführung können Sie in den Aufgabeneigenschaften verfolgen.

Ausnahmen für die EDR (KATA)-Telemetrie

Um die Leistung zu verbessern und die Datenübertragung an den Telemetrie-Server zu optimieren, können Sie Telemetrie-Ausnahmen konfigurieren. Sie können beispielsweise festlegen, dass für einzelne Anwendungen keine Netzwerkkommunikationsdaten gesendet werden.

So erstellen Sie eine Telemetrie-Ausnahme in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.

4. Klicken Sie im Block **Telemetrie-Einstellungen → Telemetrie für EDR (KATA)/NDR (KATA)** auf **Einstellungen**.

5. Konfigurieren Sie im folgenden Fenster die Telemetrie-Ausnahmen (siehe folgende Tabelle).

   Das Programm kombiniert Ausschlussbedingungen mit dem logischen UND. Um eine Regel zu erstellen, müssen Sie im Feld **Vollständiger Pfad** einen Wert angeben und in der Liste **Für die folgenden Ereignistypen verwenden** mindestens einen Ereignistyp auswählen.

6. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Telemetrie-Ausnahme in der Web Console und Cloud Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen → Telemetrie-Einstellungen**.

5. Wählen Sie die Registerkarte **Telemetrie für EDR (KATA)/NDR (KATA)** aus.

6. Konfigurieren Sie im folgenden Fenster die Telemetrie-Ausnahmen (siehe folgende Tabelle).

   Das Programm kombiniert Ausschlussbedingungen mit dem logischen UND. Um eine Regel zu erstellen, müssen Sie im Feld **Vollständiger Pfad** einen Wert angeben und mindestens einen Ereignistyp auswählen.

7. Speichern Sie die vorgenommenen Änderungen.

Einstellung	Beschreibung
Ausgeschlossene Prozesse	**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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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**. • **WMI-Abfrage**. • **Pipe**. • **LDAP**. • **AMSI**.
Ausgeschlossene Netzwerkkommunikationen	**Regelname**. **Richtung**. **Protokoll**. **Raw-Socket**. **Protokollnummer**. **TLS-Zertifikat**. **Lokaler Port oder Bereich**. **Remote-Port oder -Bereich**. **Lokale Adresse**. Die Netzwerkadresse des Computers, für den Kaspersky Endpoint Security Telemetriedaten aus dem Netzwerkverkehr ausschließt. **Remote-Adresse**. Die Netzwerkadresse des Computers, für den Kaspersky Endpoint Security Telemetriedaten aus dem Netzwerkverkehr ausschließt. Für IP-Adressen wird nur das IPv4-Format unterstützt. **Programme**. Liste der ausführbaren Dateien von Anwendungen, für die Kaspersky Endpoint Security die EDR-Telemetrie aus dem Netzwerkverkehr ausschließt.

Einstellung	Beschreibung
Ausgeschlossene Vorgänge mit Dateien	**Regelname**. **Dateiname oder Maske**. Name oder Maske einer Datei bzw. eines Ordners; Kaspersky Endpoint Security wendet die Ausnahmeregel an, wenn auf diese Datei oder diesen Ordner zugegriffen wird. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske. **Vorgangstyp**. **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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.
Ausgeschlossene DNS-Vorgänge	**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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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**: • **IP-Adresse des DNS-Servers**. • **Abfrageoptionen**. • **Status**. • **Domänenname**. • **ID des Einstellungstyps**. • **Antwortdaten**.

Einstellung	Beschreibung
Ausgeschlossene LDAP-Vorgänge	**Regelname**. **LDAP-Suchbereich**. **Filter**. **Definierter Name für Suche nach LDAP-Objekten**. **Objekt-Attribute**. 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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.
Ausgeschlossene Prozesszugriffsabfragen	**Regelname**. **Vorgangstyp**. **Zugriff auf den Prozess angefordert**. **Aufruflistenüberwachung**. 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. • **Geben Sie Auslösekriterien für die Regel an sowie die Ereignistypen, für die diese Regel verwendet wird**. 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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.

Einstellung	Beschreibung
Ausgeschlossene Code-Injektionen	**Regelname**. **Zugriffsmethode**. **Aufrufliste**. **Modifizierte Befehlszeile**. **Injektionsadresse**. **Eingefügter DLL-Name**. 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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.

Einstellung	Beschreibung
Ausgeschlossene WMI-Abfragen	**Regelname**. **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**. 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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.
Ausgeschlossene Pipe-Vorgänge	**Regelname**. **Pipe-Name**. **Vorgangstyp**. 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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.

Einstellung	Beschreibung
Ausgeschlossene Registrierungsänderungen	**Regelname**. **Vorgangstyp**. **Pfad**. **Name des Wertes**. **Wert**. **Vollständiger Name einer Registrierungsdatei**. 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 die App die Parameterfelder der ausführbaren Datei mit den Daten aus den Eigenschaften der 32-Bit-Version der gleichen 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.
Ausgeschlossene Vorgänge mit Geräten	**Regelname**. **Gerätetyp**. **Geräte-ID**. **Gerätename**.

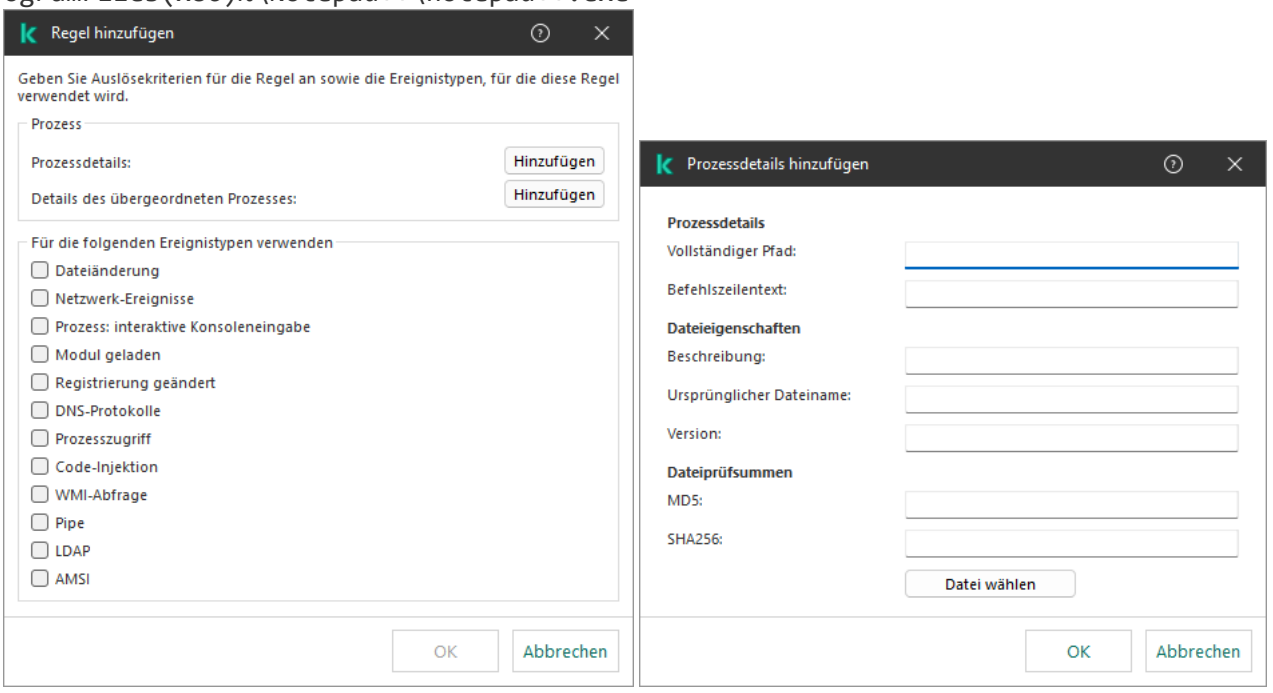
Beispiel 1. Ausgeschlossene Prozesse

Um Ereignisse eines Drittanbieter-Programms (Prozesses) von der Telemetrie auszuschließen, öffnen Sie das Fenster mit den EDR-Telemetrie-Ausnahmen auf der Registerkarte **Ausgeschlossene Prozesse** und fügen Sie die ausführbare Datei des Programms hinzu.

Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND.

Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. Beispielsweise:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



Einen Prozess ausschließen

Beispiel 1. Dateiänderung

Wenn Sie im Programm Notepad++ häufig Skripte bearbeiten und die Änderungsereignisse für die entsprechenden Skripte ausschließen möchten, fügen Sie die ausführbare Datei Notepad++ zu den Telemetrie-Ausnahmen hinzu.

Legen Sie die folgenden Einstellungen fest:

- **Vollständiger Pfad**: `C:\Program Files\Notepad++\notepad++.exe`
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34
- **Für die folgenden Ereignistypen verwenden**: Dateiänderung

Beispiel 2. Netzwerk-Ereignisse

Wenn Sie das Programm WinSCP zur Verwaltung von Dateien auf einem Remote-Server verwenden und Netzwerk-Ereignisse ausschließen möchten, fügen Sie die ausführbare Datei WinSCP zu den Telemetrie-Ausnahmen hinzu.

Legen Sie die folgenden Einstellungen fest:

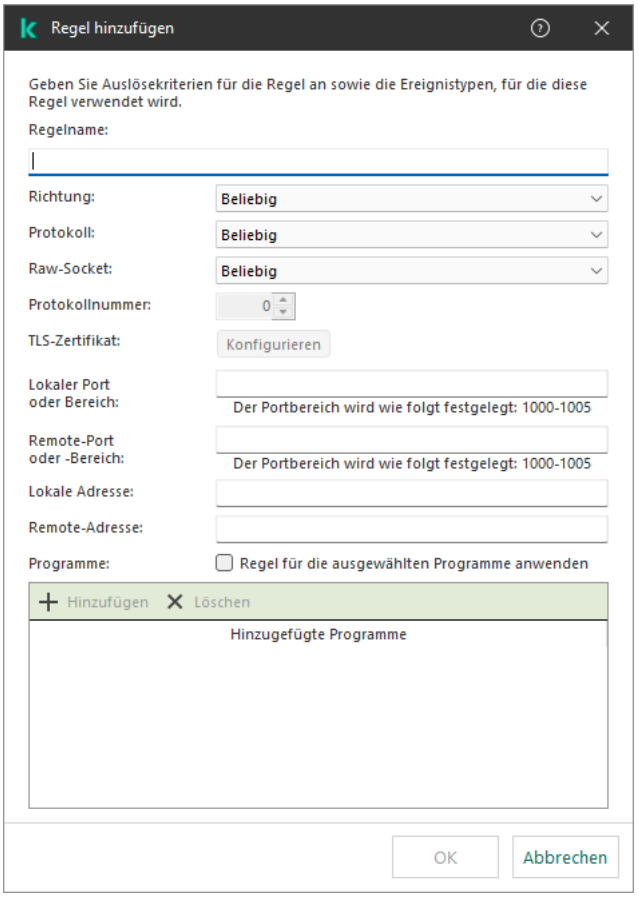
- **Vollständiger Pfad**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (optional).
- **Für die folgenden Ereignistypen verwenden**: Netzwerk-Ereignisse

Beispiel 2. Ausgeschlossene Netzwerkkommunikationen

Um Ereignisse, die Remote-Dienst-Verbindungen betreffen, von der Telemetrie auszuschließen, öffnen Sie das Fenster mit den EDR-Telemetrie-Ausnahmen auf der Registerkarte **Ausgeschlossene Netzwerkkommunikationen** und fügen Sie die entsprechenden Verbindungseinstellungen hinzu (Protokoll, Port, Richtung, IP-Adresse, TLS-Zertifikat und andere).

Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND.

Eine Subnetzadresse (z. B. 10.28.0.0/24) kann nicht angegeben werden. Das Programm erlaubt nur die Angabe einer IP-Adresse (z. B. 10.28.0.105).



Netzwerkkommunikation ausschließen

Wenn Sie einen Unternehmens-Webserver verwenden und Browser-Ereignisse bei der Verbindung mit diesem Webserver ausschließen möchten, fügen Sie die IP-Adresse des Servers und die ausführbare Datei des Browsers zu den Telemetrie-Ausnahmen hinzu.

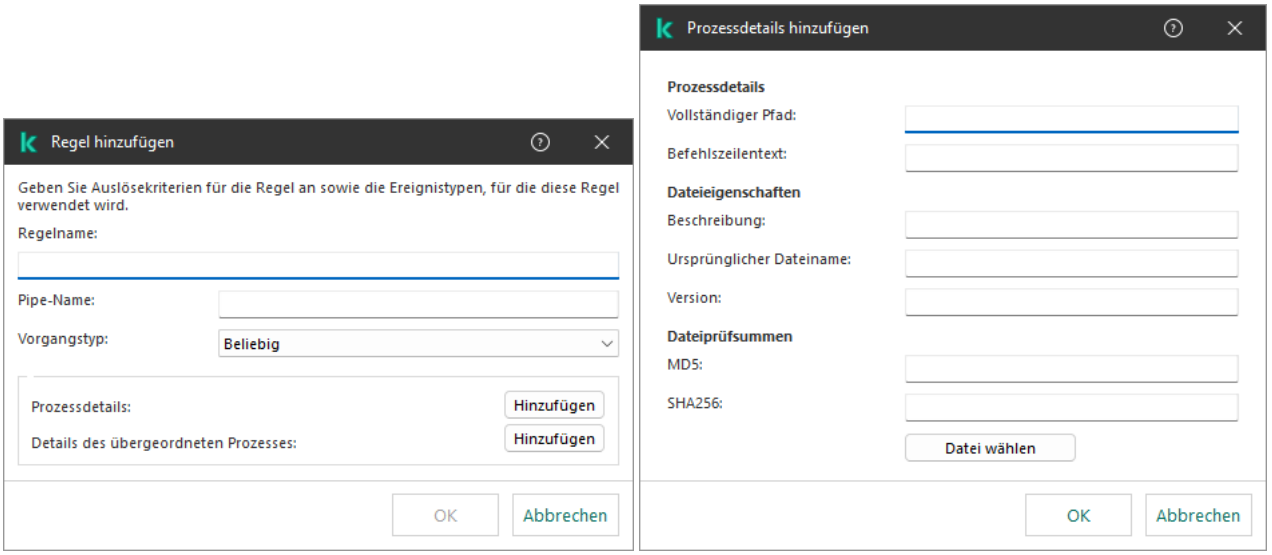
Legen Sie die folgenden Einstellungen fest:

- **Protokoll**: TCP.
- **Remote-Port oder -Bereich**: 443.
- **Remote-Adresse**: 10.28.0.105.
- **Programme**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`; `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`

Beispiel 3. Ausgeschlossene Dateivorgänge

Um Ereignisse, betreffen Vorgänge mit vertrauenswürdigen Dateien betreffen, von der Telemetrie auszuschließen, öffnen Sie das Fenster mit den EDR-Telemetrie-Ausnahmen auf der Registerkarte **Ausgeschlossene Vorgänge mit Dateien** und fügen Sie die vertrauenswürdige Datei hinzu.

Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND.



Dateivorgänge ausschließen

Wenn ein Programm in ein Protokoll schreibt und Sie Ereignisse zur Änderung der Protokolldatei ausschließen möchten, fügen Sie die Protokolldatei und die ausführbare Datei des Programms zu den Telemetrie-Ausnahmen hinzu.

Legen Sie die folgenden Einstellungen fest:

- **Dateiname oder Maske**: `C:\Apache24\logs\error.log`
- **Vorgangstyp**: Dateiänderung
- **Vollständiger Pfad**: `C:\Apache24\bin\httpd.exe`
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34

Beispiel 4. Ausgeschlossene Registrierungsänderungen

Um Registrierungsänderungen von der Telemetrie auszuschließen, öffnen Sie das Fenster mit den EDR-Telemetrie-Ausnahmen auf der Registerkarte **Ausgeschlossene Registrierungsänderungen** und fügen Sie einen Registrierungsschlüssel hinzu.

Kaspersky Endpoint Security kombiniert Kriterien für die Regelauslösung mit einem logischen UND.

Wenn ein Programm seine Registrierungswerte häufig ändert und Sie die Ereignisse, die Registrierungsänderungen betreffen, von der Telemetrie ausschließen möchten, fügen Sie den Registrierungsschlüssel und die ausführbare Datei des Programms zu den Telemetrie-Ausnahmen hinzu.

Legen Sie die folgenden Einstellungen fest:

- **Vorgangstyp**: Ändern
- **Pfad**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64
- **Vollständiger Pfad**: `C:\Program Files\PuTTY\putty.exe`
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34

KATA Sandbox

Kaspersky Anti Targeted Attack Platform enthält die Komponente Sandbox (KATA Sandbox). Mit der *Sandbox*-Technologie können Sie komplexe Bedrohungen auf einem Computer erkennen. „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 Anti Targeted Attack Platform“.

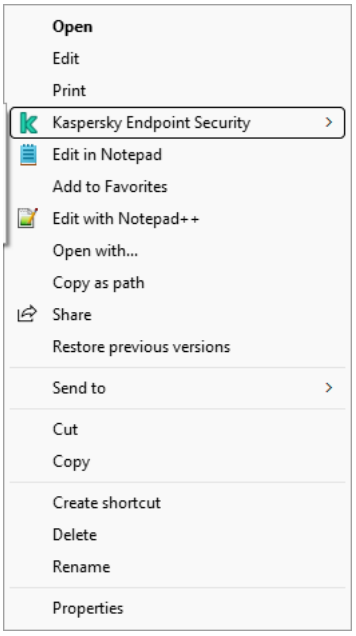
Um KATA Sandbox zu aktivieren, benötigen Sie einen Lizenzschlüssel, der die KATA- oder KEDR-Funktionalität enthält. Einzelheiten zu den verfügbaren Funktionalitäten finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

KATA Sandbox bietet die folgenden Untersuchungsmodi für Dateien:

- *Manuell*. Der Benutzer übermittelt die zu untersuchende Datei manuell über das Kontextmenü (**An Sandbox senden**). Wenn eine Datei an Sandbox gesendet wird, untersucht die App diese Datei auch mithilfe der Antiviren-Datenbanken.
- *Automatisch*. Das Programm erkennt Objekte automatisch und sendet sie zur Untersuchung an die Sandbox.

Nachdem die Datei an Sandbox gesendet wurde, kann der Benutzer weiterhin auf die Datei zugreifen. Kaspersky Endpoint Security protokolliert das entsprechende Ereignis und sendet das Ereignis an Kaspersky Security Center und an die Konsole von Kaspersky Anti Targeted Attack Platform. Wenn die Sandbox bösartige Aktivitäten erkennt, reagiert Kaspersky Endpoint Security automatisch (z. B. löscht das Objekt und startet eine Untersuchung wichtiger Bereiche).

Damit KATA Sandbox im manuellen Modus funktioniert, muss Kaspersky Anti Targeted Attack Platform 7.0 oder höher bereitgestellt werden. Damit KATA Sandbox im automatischen Modus funktioniert, muss Kaspersky Anti Targeted Attack Platform 8.0 oder höher bereitgestellt werden.



In KATA Sandbox über das Kontextmenü untersuchen

Integration des integrierten Agenten in KATA Sandbox

Für die Integration in die Komponente KATA Sandbox muss die Sandbox-Komponente hinzugefügt werden. Sie können die Komponente „Sandbox“ während der Installation oder dem Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Um Dateien zur Untersuchung zu senden, müssen Sie die Integration in KATA Sandbox aktivieren und einen Central Node-Server hinzufügen, der innerhalb der Lösung bereitgestellt wird. Die Komponente kann nur über die „Kaspersky Security Center Web Console“ verwaltet werden. Sie können diese Komponente nicht mit der Verwaltungskonsole (MMC) verwalten.

Um die Integration mit „KATA Sandbox“ zu aktivieren oder zu deaktivieren:

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Sandbox**.

5. Verwenden Sie den Schalter **Integration it Sandbox AKTIVIERT**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Wählen Sie einen Funktionsmodus für KATA Sandbox aus:

   - **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**.

7. Klicken Sie auf den Link **Verbindungseinstellungen**.

8. Konfigurieren Sie die Einstellungen der Verbindung zum Central Node-Server:

   - **Timeout (ms)**. Verbindungstimeout für den Central Node-Server. 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 Central Node-Server zu konfigurieren, müssen Sie ein TLS-Zertifikat erstellen. Anschließend müssen Sie das Zertifikat mithilfe einer Richtlinie dem Computer hinzufügen. Außerdem müssen Sie das Zertifikat zum Central Node-Server hinzufügen.
   - **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.

9. Klicken Sie im Block **Verbindung mit Sandbox-Servern** auf **Hinzufügen**.

10. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster die Serveradresse (IPv4, IPv6, DNS) und den Port für Central Node ein.

    Einzelheiten zur Bereitstellung virtueller Images und zur Konfiguration von Central Node-Servern finden Sie in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Die Komponente „Sandbox“ ist nun aktiviert. Überprüfen Sie den Betriebsstatus der Komponente, indem Sie sich den *Bericht über den Status der Programmkomponenten* ansehen. Den Betriebsstatus einer Komponente

können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Sandbox** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Konfigurieren von Aktionen zur Reaktion auf Bedrohungen

Wenn die Sandbox bösartige Aktivitäten erkennt, reagiert Kaspersky Endpoint Security automatisch (z. B. löscht das Objekt und startet eine Untersuchung wichtiger Bereiche).

So konfigurieren Sie Aktionen zur Reaktion auf Bedrohungen:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Sandbox**.
5. Wählen Sie die entsprechende Aktion im Block **Aktion beim Fund einer Bedrohung**:

   - **Kopie in die Quarantäne verschieben, Objekt löschen**. Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security das auf dem Computer gefundene schädliche Objekt. Bevor das Objekts gelöscht wird, erstellt Kaspersky Endpoint Security eine Backup-Kopie für den Fall, dass das Objekt später wiederhergestellt werden muss. 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. Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden 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.
6. Konfigurieren Sie, sofern erforderlich, die Einstellungen der Aufgabe *IOC-Untersuchung* im Block **IOC-Untersuchungsbereich**.

   - **Bereiche mit kritischen Dateien**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security nur kritische Dateibereiche des Computers auf IOCs. Dazu zählen Kernel-Speicher und Bootsektoren.
   - **Dateibereiche auf dem Systemlaufwerk des Computers**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security das Systemlaufwerk des Computers auf IOCs.

7. Konfigurieren Sie, sofern erforderlich, die Einstellungen der Aufgabe *IOC-Untersuchung* im Block **IOC-Untersuchungsaufgabe ausführen**.

   - **Manuell**. In diesem Ausführungsmodus können Sie die Aufgabe *IOC-Untersuchung* zu einem geeigneten Zeitpunkt manuell starten.

   - **Automatisch**. Ausführungsmodus, in dem Kaspersky Endpoint Security die Aufgabe *IOC-Untersuchung* automatisch ausführt, nachdem eine Bedrohung erkannt wurde.

   - **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.

8. Konfigurieren Sie die erweiterten Einstellungen der Aufgabe *IOC-Untersuchung*.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Leitfaden für die Migration von KEA zu KES, für EDR (KATA)

Ab Version 12.1 enthält Kaspersky Endpoint Security für Windows einen integrierten Agenten zur Verwaltung der Komponente Kaspersky Endpoint Detection and Response als Teil der Lösung Kaspersky Anti Targeted Attack Platform. Sie benötigen Kaspersky Endpoint Agent nicht mehr als separate Anwendung, um mit EDR (KATA) zu arbeiten. Alle Funktionen von Kaspersky Endpoint Agent werden von Kaspersky Endpoint Security ausgeführt. Die Auslastung der Kaspersky Anti Targeted Attack Platform-Server bleibt gleich.

Wenn Sie Kaspersky Endpoint Security auf Computern bereitstellen, auf denen Kaspersky Endpoint Agent installiert ist, funktioniert die Lösung Kaspersky Anti Targeted Attack Platform (EDR) weiterhin mit Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt. Das System verhält sich gleich, wenn Sie Kaspersky Endpoint Security auf Version 12.1 oder höher aktualisieren.

> Kaspersky Endpoint Security ist nicht mit Kaspersky Endpoint Agent kompatibel. Sie können diese beiden Apps nicht mehr auf demselben Computer installieren.

Damit Kaspersky Endpoint Security als Teil von Endpoint Detection and Response (KATA) funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Kaspersky Anti Targeted Attack Platform Version 5.0 oder höher.

- Kaspersky Security Center Version 14.2 oder höher (einschließlich Administrationsagent). In älteren Versionen von Kaspersky Security Center kann die Funktion Endpoint Detection and Response (KATA) nicht aktiviert werden.

Schritte für die Migration der Konfiguration [KES KEA] zu [KES+built-in agent] für EDR (KATA)

1. **Upgrade des Verwaltungs-Plug-ins für Kaspersky Endpoint Security**

   Die Komponente EDR (KATA) kann mit dem Verwaltungs-Plug-in von Kaspersky Endpoint Security Version 12.1 oder höher verwaltet werden. Je nachdem, welchen Konsolentyp von Kaspersky Security Center sie verwenden, aktualisieren Sie das Verwaltungs-Plug-in in der Verwaltungskonsole (MMC) oder das Web-Plug-in in der Web Console.

2. **Migration von Richtlinien und Aufgaben**

   Übertragen Sie die Einstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security für Windows. Folgende Varianten stehen zur Auswahl:

   - Ein Assistent für die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security. Der Assistent für die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security funktioniert nur in Web Console

     So migrieren Sie Richtlinien- und Aufgabeneinstellungen von Kaspersky Endpoint Agent nach Kaspersky Endpoint Security über die Web Console

     Wählen Sie im „Web Console"-Hauptfenster den Punkt **Vorgänge** → **Migration von Kaspersky Endpoint Agent** aus.

     Dadurch wird der Migrations-Assistent für Richtlinien und Aufgaben ausgeführt. Folgen Sie den Anweisungen.

Schritt 1. Migration der Richtlinien

Der Migrationsassistent erstellt eine neue Richtlinie, die die Einstellungen der Richtlinien von Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammenführt. Wählen Sie in der Richtlinienliste jene Richtlinien von Kaspersky Endpoint Agent aus, deren Einstellungen Sie mit der Richtlinie von Kaspersky Endpoint Security zusammenführen möchten. Klicken Sie auf eine Richtlinie von Kaspersky Endpoint Agent, um die Richtlinie von Kaspersky Endpoint Security auszuwählen, mit der Sie die Einstellungen zusammenführen möchten. Stellen Sie sicher, dass Sie die korrekten Richtlinien ausgewählt haben, und gehen Sie weiter zum nächsten Schritt

Schritt 2. Aufgabenmigration

Der Migrations-Assistent unterstützt keine Aufgaben von EDR (KATA). Überspringen Sie diesen Schritt.

Schritt 3. Assistent abschließen

Schließen Sie den Assistenten ab. Beim Ausführen des Assistenten wird eine neue Kaspersky Endpoint Security-Richtlinie erstellt. Die Richtlinie führt Einstellungen Kaspersky Endpoint Security und Kaspersky Endpoint Agent zusammen. Die Richtlinie heißt *<Kaspersky Endpoint Security-Richtlinienname> & <Kaspersky Endpoint Agent-Richtlinienname>*. Die neue Richtlinie hat den Status *Inaktiv*. Um fortzufahren, ändern Sie den Status der Richtlinien von Kaspersky Endpoint Agent und Kaspersky Endpoint Security in *Inaktiv* und aktivieren Sie die neue zusammengeführte Richtlinie.

Der Migrations-Assistent in Web Console überspringt die folgenden Richtlinieneinstellungen und migriert diese nicht:

- Verbot von Einstellungsänderungen **Verbindungseinstellungen** („Schloss“).

  Die Einstellungen können standardmäßig geändert werden (das „Schloss“ ist geöffnet). Die Einstellungen werden daher nicht auf dem Computer übernommen. Sie müssen Einstellungsänderungen verbieten und das „Schloss“ verriegeln.

- Krypto-Container.

  Wenn Sie die Zwei-Wege-Authentifizierung zur Verbindung mit Central Node-Servern verwenden, müssen Sie den Krypto-Container erneut hinzufügen.

Da der Migrations-Assistent diese Einstellungen nicht migriert, können beim Verbinden des Computers mit Central Node-Servern Fehler auftreten. Zur Fehlerbehebung müssen Sie zu den Richtlinieneigenschaften gehen und die Verbindungseinstellungen konfigurieren.

- Assistent für das Massenkonvertieren von standardmäßigen Richtlinien und Aufgaben Der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben ist nur in der Verwaltungskonsole (MMC) verfügbar. Weitere Informationen zum Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben finden Sie in der Hilfe zu Kaspersky Security Center.

Um das korrekte Funktionieren von Kaspersky Endpoint Security auf den Servern sicherzustellen, wird empfohlen, Dateien, die für das Funktionieren von Servern wichtig sind, der vertrauenswürdigen Zone hinzuzufügen. Für SQL-Server müssen Sie MDF- und LDF-Datenbankdateien hinzufügen. Für Microsoft Exchange-Server müssen Sie CHK-, EDB-, JRS-, LOG- und JSL-Dateien hinzufügen. Sie können Masken verwenden, z. B. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen.

Ausnahmen der EDR-Telemetrie werden nicht aus der Kaspersky Endpoint Agent-Richtlinie in die Kaspersky Endpoint Security-Richtlinie migriert. Kaspersky Endpoint Security verfügt über eigene Tools für Ausnahmen und vertrauenswürdige Anwendungen. Der Betrieb von Kaspersky Endpoint Security ist optimiert. Wenn einzelne EDR-Telemetrie-Ausnahmen fehlen, verursacht dies keine zusätzliche Belastung Ihres Computers im Vergleich zu Kaspersky Endpoint Agent. Kaspersky Endpoint Security verwendet Telemetrie nicht nur für EDR (KATA), sondern auch für den Betrieb der App-Schutzkomponenten. Daher ist es nicht notwendig, einzelne EDR-Telemetrie-Ausnahmen zu übertragen. Wenn Sie feststellen, das die Computerleistung sinkt, überprüfen Sie den Betrieb der App (siehe Schritt 7, Überprüfung der Leistung).

3 Lizenzierung der Funktionalität von EDR (KATA)

Um Kaspersky Endpoint Security als Teil der Lösung Kaspersky Anti Targeted Attack Platform zu aktivieren, benötigen Sie eine separate Lizenz für das Add-on von Kaspersky Endpoint Detection and Response (KATA). Sie können den Schlüssel mithilfe der Aufgabe *Schlüssel hinzufügen* hinzufügen. Dadurch werden der Anwendung zwei Schlüssel hinzugefügt: *Kaspersky Endpoint Security* und *Kaspersky Endpoint Detection and Response (KATA)*.

Bei der Lizenzierung des Add-ons für Kaspersky Endpoint Detection and Response (KATA) auf Computern mit bereits aktivierten EDR Optimum- oder EDR Expert-Funktionen müssen Sie die folgenden Punkte beachten:

- Wenn Sie eine *Schlüsseldatei* für die Lizenzierung von Kaspersky Endpoint Security mit EDR Optimum- oder EDR Expert-Funktionen verwenden, können Sie keinen separaten Schlüssel für das Add-on von Kaspersky Endpoint Detection and Response (KATA) hinzufügen. Sie können entweder auf die Verwendung eines Aktivierungscodes für die Lizenzierung umsteigen oder bei Ihrem Dienstanbieter eine neue Schlüsseldatei zur Aktivierung der Kaspersky Endpoint Security- und EDR-Funktionen anfordern. Für die Lizenzierung stellt der Dienstanbieter eine oder mehrere Schlüsseldateien zur Verfügung.

- Wenn Sie eine *Schlüsseldatei* für die Lizenzierung von Kaspersky Endpoint Security ohne EDR Optimum- oder EDR Expert-Funktionen verwenden, können Sie einen separaten Schlüssel für das Add-on von Kaspersky Endpoint Detection and Response (KATA) hinzufügen, ohne neue Schlüsseldateien anzufordern.

- Wenn Sie eine *Aktivierungscode* für die Lizenzierung verwenden, stellt der Kaspersky-Aktivierungsserver die Schlüssel automatisch neu aus und die EDR (KATA)-Funktionen werden automatisch verfügbar. In diesem Fall werden EDR Optimum und EDR Expert deaktiviert.

- Mit Kaspersky Endpoint Security können Sie maximal zwei aktive Schlüssel hinzufügen: einen Kaspersky Endpoint Security-Schlüssel und einen Schlüssel des Typs „Add-on“. Sie können auch maximal zwei Reserveschlüssel hinzufügen. Einen Reserveschlüssel für Kaspersky Endpoint Security und einen Reserveschlüssel des Typs „Add-on“.

4 Installation und Upgrade von Kaspersky Endpoint Security

Um die Funktionalität von EDR (KATA) während einer Installation oder eines Upgrades der App zu migrieren, sollten Sie die Aufgabe zur Remote-Installation verwenden. Beim Erstellen einer Aufgabe zur Remote-Installation müssen Sie die Komponente EDR (KATA) in den Einstellungen des Installationspakets auswählen.

Sie können das Programm auch mit den folgenden Methoden upgraden:

- Verwendung des Kaspersky-Update-Dienstes.

- Lokal mithilfe des Installationsassistenten für das Programm.

Kaspersky Endpoint Security unterstützt die automatische Komponentenauswahl, wenn ein Programm-Upgrade auf einem Computer ausgeführt wird, auf dem das Programm „Kaspersky Endpoint Agent“ installiert ist. Die automatische Komponentenauswahl ist abhängig von den Berechtigungen des Benutzerkontos, unter dem das Programm upgegradet wird.

Wenn Sie Kaspersky Endpoint Security mithilfe der EXE- oder MSI-Datei unter dem Systemkonto (SYSTEM) upgraden, erhält Kaspersky Endpoint Security Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. Ist auf dem Computer Kaspersky Endpoint Agent installiert und die EDR (KATA)-Lösung aktiviert, so konfiguriert das Kaspersky Endpoint Security-Installationsprogramm automatisch die Komponentenauswahl und wählt die Komponente EDR (KATA) aus. Dadurch wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent. Gewöhnlich wird das MSI-Installationsprogramm unter dem Systemkonto (SYSTEM) ausgeführt, wenn ein Upgrade über den Kaspersky-Update-Dienst erfolgt oder wenn ein Installationspaket über Kaspersky Security Center bereitgestellt wird.

Wenn Sie Kaspersky Endpoint Security mithilfe einer MSI-Datei unter einem Benutzerkonto ohne Administratorrechte upgraden, hat Kaspersky Endpoint Security keinen Zugriff auf die aktuellen Lizenzen für Kaspersky-Lösungen. In diesem Fall wählt Kaspersky Endpoint Security automatisch die Komponenten aus und berücksichtigt dabei die Komponentenauswahl von Kaspersky Endpoint Agent. Anschließend wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

Kaspersky Endpoint Security unterstützt ein Upgrade ohne Neustart des Computers. Sie können den Modus für das App-Upgrade in den Richtlinieneigenschaften auswählen.

5 Überprüfung des App-Betriebs

Falls der Computer nach der App-Installation oder dem Upgrade in der Konsole von Kaspersky Security Center den Status *Kritisch* anzeigt:

- Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
- Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*. Falls eine Komponente den Status *Nicht durch Lizenz abgedeckt* hat, stellen Sie sicher, dass Sie die Funktionalität des integrierten Agenten aktiviert haben.
- Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

6 Überprüfung der Verbindung zum Kaspersky Anti Targeted Attack Platform-Server

Überprüfen Sie die Verbindung zum Server von Kaspersky Anti Targeted Attack Platform. Gehen Sie dazu folgendermaßen vor:

1. Überprüfen Sie, ob Sie über ein gültiges Zertifikat verfügen.
2. Überprüfen Sie die Einstellungen der Serververbindung.
3. Überprüfen Sie das Ereignisprotokoll.

   Wenn eine Verbindung zum Server hergestellt wird, sendet die App das Ereignis *Erfolgreiche Verbindung zum EDR Expert-Server*. Wenn es kein Ereignis über eine erfolgreiche Verbindung gibt und keine Ereignisse mit Verbindungsfehlern vorliegen, überprüfen Sie die Einstellungen der Ereignisprotokollierung und aktivieren Sie das Senden von Ereignissen für Endpoint Detection and Response (KATA).

Der Status der Serververbindung hat keinen Einfluss auf den Computerstatus in der Kaspersky Security Center-Konsole. Wenn also keine Verbindung zum Server besteht, kann der Computer trotzdem den Status *OK* haben. Sehen Sie im Ereignisprotokoll nach, um die Verbindung zum Server zu überprüfen.

7 Überprüfung der Leistung

Wenn die Leistung Ihres Computers nach der Installation oder dem Update einer Anwendung sinkt, können Sie die Datenübertragung optimieren. Gehen Sie dazu folgendermaßen vor:

1. Deaktivieren Sie die EDR (KATA)-Komponente und überprüfen Sie, ob der Leistungsabfall auf EDR (KATA) zurückzuführen ist.
2. Deaktivieren Sie für vertrauenswürdige Anwendungen die Telemetrie-Erfassung bei Konsoleneingabevorgängen (standardmäßig aktiviert).
3. Fügen Sie Anwendungen, die die Computerleistung beeinträchtigen, zur Liste vertrauenswürdiger Anwendungen hinzu.
4. Kontaktieren Sie den Technischen Support von Kaspersky. Unsere Support-Experten unterstützen Sie bei der Konfiguration der Telemetriefilterung in Kaspersky Anti Targeted Attack Platform. Dadurch wird der Datenverkehr reduziert. Wenn die Leistung Ihres Computers durch eine bestimmte Anwendung beeinträchtigt wird, fügen Sie der Anfrage das Verteilungspaket dieser Anwendung bei.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security für Windows unterstützt die Integration in die Lösung Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* ist eine Cybersicherheits-Lösung für Unternehmen. Mit den darin enthaltenen Kaspersky-Programmen kann sich ein Unternehmen vor den meisten Arten von Cyber-Risiken schützen und die wichtigsten Verbreitungsszenarien für Bedrohungen abdecken. Die Komponenten von EDR Expert (on-premises) werden auf der Open Single Management Platform (OSMP) bereitgestellt. Diese Plattform führt plattformübergreifende Szenarien auf einer einzigen Benutzeroberfläche aus und ermöglicht die Integration von Kaspersky-Programmen in Drittthersteller-Programme, um ein umfassendes Sicherheitssystem zu gestalten.

Eines der zentralen Elemente dieser Lösung ist *SIEM*. SIEM verfolgt Ereignisse, die von allen Komponenten stammen, und stellt mithilfe von Herstellerregeln und benutzerdefinierten Regeln Zusammenhänge zwischen diesen Ereignissen her. EDR Expert (on-premises) 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-premises) erfassten Ereignisse kombiniert, einschließlich der Ereignisse aus Kaspersky-Programmen und Informationssicherheitsprodukten von Drittanbietern.

Zur Reaktion auf komplexe Vorfälle verwendet EDR Expert (on-premises) vordefinierte und benutzerdefinierte Szenarien. Sie können auch Reaktionen aus Drittanbieter-Programmen sowie Reaktionsszenarien verwenden, an denen mehrere Programme beteiligt sind.

Threat Intelligence-Tools

Kaspersky Endpoint Detection and Response verwendet die folgenden Threat Intelligence-Tools:

- Integration in Kaspersky Threat Intelligence Portal, das Informationen über die Reputation von Dateien und Webadressen enthält und anzeigt.
- Kaspersky Threats-Datenbank.
- Die Cloud-Service-Infrastruktur von Kaspersky Security Network (im Folgenden auch „KSN“ genannt), die Echtzeitzugriff auf Datei-, Website- und Software-Reputationsinformationen aus der Kaspersky-Wissensdatenbank bietet. Durch die Verwendung von Daten aus Kaspersky Security Network wird die Reaktion der Kaspersky-Programme auf Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

Funktionsweise der Lösung

Kaspersky Endpoint Security wird auf den einzelnen Computern einer IT-Unternehmensinfrastruktur installiert und überwacht kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien.

Wenn Kaspersky Endpoint Security im Standardmodus in der VDI-Infrastruktur installiert wird, unterstützt die Anwendung die Integration in EDR Expert (on-premises). Die Einsatzfähigkeit der anderen Anwendungsfunktionen kann jedoch nicht gewährleistet werden. Für den Schutz von virtuellen Maschinen in der VDI-Infrastruktur wird empfohlen, Kaspersky Endpoint Security im Light Agent-Modus zu verwenden.

Informationen über Ereignisse auf dem Computer (Telemetrie) werden an den Server von EDR Expert (on-premises) gesendet. In diesem Fall sendet Kaspersky Endpoint Security an die Telemetrie-Erfassungsserver auch Informationen über die vom Programm erkannten Bedrohungen sowie Informationen über die Verarbeitungsergebnisse dieser Bedrohungen.

Die Integration von EDR Expert (on-premises) wird in der Kaspersky Security Center-Konsole konfiguriert. Anschließend wird der integrierte Agent über Open Single Management Platform (OSMP) verwaltet. Dies bezieht sich beispielsweise auch auf folgende Vorgänge: Aufgaben ausführen, Objekte in der Quarantäne verwalten und Berichte anzeigen.

Kaspersky Endpoint Security-Konfigurationen für die Verwendung mit EDR Expert (on-premises)

Die folgenden Konfigurationen können für EDR Expert (on-premises) verwendet werden:

- **[KES+built-in agent]**. In dieser Konfiguration dient Kaspersky Endpoint Security sowohl als Programm, das die Sicherheit des Computers gewährleistet, als auch als Programm für die Interaktion mit EDR Expert (on-premises). Der integrierte Agent für EDR Expert (on-premises) ist in Kaspersky Endpoint Security 12.11 für Windows oder höher verfügbar.
- **[third-party EPP+EDR Agent]**. In dieser Konfiguration wird die Sicherheit der IT-Infrastruktur durch die Endpoint Protection Platform (EPP) eines Drittanbieters bereitgestellt. In der Konfiguration Endpoint Detection and Response Agent (EDR Agent) wird die Interaktion mit EDR Expert (on-premises) durch Kaspersky Endpoint Security gewährleistet. In dieser Konfiguration ist EDR Agent mit Drittanbieter-EPP-Anwendungen kompatibel. EDR Agent für EDR Expert (on-premises) ist in Kaspersky Endpoint Security 12.11 für Windows oder höher verfügbar.

Integration des integrierten Agenten in EDR Expert (on-premises)

Zur Integration in die Lösung „Kaspersky Endpoint Detection and Response Expert (on-premises)“ müssen Sie die Komponente „Endpoint Detection and Response Expert (on-premises)“ hinzufügen und Kaspersky Endpoint Security konfigurieren.

> Die Komponenten Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) und Endpoint Detection and Response Expert (on-premises) sind nicht miteinander kompatibel.

Damit Endpoint Detection and Response Expert (on-premises) funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- OSMP (Open Single Management Platform) ist installiert.
- Die Anwendung ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Die Komponente „Endpoint Detection and Response Expert (on-premises)“ ist aktiviert.
- Die Programmkomponenten, die den Betrieb von EDR Expert (on-premises) sicherstellen, sind aktiviert und betriebsbereit. Der Betrieb von EDR Expert (on-premises) wird durch die folgenden Komponenten gewährleistet:
  - 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 Einrichtung der Integration von EDR Expert (on-premises) umfasst die folgenden Schritte:

1. **Die Komponente „EDR Expert (on-premises)“ installieren**

   Sie können die Komponente „EDR Expert (on-premises)“ während der Installation oder beim Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   > Sie müssen Ihren Computer neu starten, um das Upgrade der App mit der neuen Komponente abzuschließen.

2. **Kaspersky Endpoint Detection and Response Expert (on-premises) aktivieren**

   Sie müssen eine separate Lizenz für EDR Expert (on-premises) kaufen (Add-on für Kaspersky Endpoint Detection and Response Expert (on-premises)).

   Die Funktionalität ist verfügbar, sobald ein separater Schlüssel für Kaspersky Endpoint Detection and Response (on-premises) hinzugefügt wird. Dadurch werden zwei Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security und ein Schlüssel für Kaspersky Endpoint Detection and Response (on-premises).

   Die Lizenzverwaltung für die eigenständige Funktionalität von Endpoint Detection and Response (on-premises) entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität von EDR Expert (on-premises) in der Lizenz enthalten ist und in der lokalen Benutzeroberfläche des Programms ausgeführt wird.

3. **Verbindung mit dem Telemetrie-Erfassungsserver und dem Reaktionsserver herstellen**

   Kaspersky Endpoint Detection and Response Expert (on-premises) erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und zwei Servern:

   - Ein *Telemetrie-Erfassungsserver* ist Teil einer SIEM-Lösung, die Informationen über auf dem Computer auftretende Ereignisse sammelt, normalisiert, korreliert, analysiert und speichert.
   - Ein *Reaktionsserver* ist ein Server, der Daten empfängt und sendet, das Verhalten von Objekten analysiert und die Ergebnisse solcher Untersuchungen veröffentlicht.

   Zur Konfiguration einer vertrauenswürdigen Verbindung müssen Sie ein TLS-Zertifikat verwenden. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Anschließend müssen Sie das TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen (siehe Anleitung unten).

   Standardmäßig überprüft Kaspersky Endpoint Security nur das TLS-Zertifikat der Server. Um die Verbindung sicherer zu machen, können Sie zusätzlich die Überprüfung des Computers auf dem Server aktivieren (Zwei-Wege-Authentifizierung). Um diese Überprüfung zu aktivieren, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers und von Kaspersky Endpoint Security aktivieren. Zur Verwendung der Zwei-Wege-Authentifizierung benötigen Sie außerdem einen Krypto-Container. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, mit EDR Expert (on-premises) (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.
5. Aktivieren Sie den Schalter **Endpoint Detection and Response Expert (On-Premises) AKTIVIERT**.
6. Um EDR Expert (on-premises) zu konfigurieren, wählen in der Liste der Lösungen den Punkt **Endpoint Detection and Response Expert (ab Version 8.0)** aus.
7. Konfigurieren Sie die Verbindung mit den *Telemetrie-Erfassungsservern*:

   a. Klicken Sie im Block **Verbindung mit Telemetrie-Erfassungsservern** auf den Link **Verbindungseinstellungen**.

   b. Konfigurieren Sie die Verbindung mit den Telemetrie-Erfassungsservern:

   - **Timeout (Sek.)**. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden.
   - **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).
   - **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers 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. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Nachdem Sie die Server-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.

   c. Klicken Sie auf **OK**.

d. Fügen Sie Telemetrie-Erfassungsserver hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

Sie können mehrere Adressen für 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.

e. Konfigurieren Sie, falls erforderlich, die Telemetrie.

8. Konfigurieren Sie die Verbindung mit den *Reaktionsservern*:

a. Konfigurieren Sie im Block **Verbindung mit Reaktionsservern** die Einstellung **Synchronisierungsanfrage an Server senden alle (Min.)**: Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung empfängt Kaspersky Endpoint Security Aufgaben zur Reaktion auf Bedrohungen und sendet Aufgabenergebnisse.

b. Klicken Sie auf den Link **Verbindungseinstellungen**.

c. Konfigurieren Sie die Verbindung mit den Reaktionsservern:

- **Timeout (Sek.)**. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden.
- **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers 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. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Nachdem Sie die Server-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.

d. Klicken Sie auf **OK**.

e. Fügen Sie Reaktionsserver hinzu. Geben Sie dazu die Serveradresse (IPv4, IPv6) und den Port für die Serververbindung an.

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.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Sie können den Komponentenstatus mithilfe von *Bericht über den Status der Programmkomponenten* überprüfen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Endpoint Detection and Response Expert (on-premises)** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Telemetrie-Einstellungen für EDR Expert (on-premises) konfigurieren

Telemetrie ist eine Liste von Ereignissen, die auf dem geschützten Computer aufgetreten sind. Kaspersky Endpoint Security analysiert Telemetrie-Daten und sendet diese während der Synchronisierung an Telemetrie-Erfassungsserver. Weitere Informationen zu den übertragenen Telemetrieereignissen finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (On-Premises).

Telemetrie-Ereignisse treffen fast kontinuierlich auf dem Server ein. Kaspersky Endpoint Security startet die Synchronisierung mit dem Server, wenn eine der folgenden Bedingungen erfüllt ist:

- Das Synchronisierungsintervall ist abgelaufen.
- Die Anzahl der Ereignisse im Puffer überschreitet die Höchstgrenze.

Dann synchronisiert die App standardmäßig alle 30 Sekunden oder immer, wenn der Puffer 1024 Ereignisse enthält. Sie können das Synchronisierungsverhalten in der Richtlinie von Kaspersky Endpoint Security anpassen und optimale Werte für Ihre Netzwerklast auswählen (siehe Anleitung unten).

Bei fehlender Verbindung zwischen Kaspersky Endpoint Security und dem Server stellt die App neue Ereignisse in die Warteschlange. Sobald die Verbindung wiederhergestellt wird, sendet Kaspersky Endpoint Security die Ereignisse aus der Warteschlange in der richtigen Reihenfolge an den Server. Um eine Überlastung des Servers zu vermeiden, kann Kaspersky Endpoint Security bestimmte Ereignisse überspringen. Diese Option können Sie in den Einstellungen für die Ereignisübertragung optimieren und dafür beispielsweise einen Höchstwert für Ereignisse pro Stunde festlegen (siehe Anleitung unten).

Führen Sie die folgenden Schritte aus, um die Telemetrie-Einstellungen zu konfigurieren:

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.
5. Um EDR Expert (on-premises) zu konfigurieren, wählen in der Liste der Lösungen den Punkt **Endpoint Detection and Response Expert (ab Version 8.0)** aus.
6. Stellen Sie sicher, dass das Kontrollkästchen **Telemetrie an Telemetrie-Erfassungsserver senden** im Block **Einstellungen für die Datenübertragung** aktiviert ist.
7. Aktivieren Sie bei Bedarf das Kontrollkästchen **Telemetrie nur mit IOA senden**. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen.

8. Passen Sie bei Bedarf im Block **Einstellungen für die Datenübertragung** die Synchronisierung mit den Server-Einstellungen an:

   - **Maximale Verzögerung der Ereignisübertragung (Sek.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.

   - **Maximale Anzahl der Ereignispakete**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.

9. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Anforderungsbegrenzung aktivieren** im Block **Anforderungsbegrenzung**.

   Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Diese Option ist standardmäßig aktiviert.

10. Konfigurieren Sie die Optimierungseinstellungen für das Senden von Ereignissen an den Server:

    - **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.

    - **Prozentsatz für die Überschreitung des Ereignislimits**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

11. Geben Sie im Block **Verbindung mit Reaktionsservern** einen Wert für den Parameter **Synchronisierungsanfrage an Server senden alle (Min.)** ein.

12. Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung sendet Kaspersky Endpoint Security Informationen über geänderte Einstellungen und Aufgaben der App.

13. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Telemetrie-Ausnahmen für EDR Expert (on-premises)

Um die Leistung zu verbessern und die Datenübertragung an den Telemetrie-Erfassungsserver zu optimieren, können Sie Telemetrie-Ausnahmen hinzufügen. Sie können beispielsweise festlegen, dass für einzelne Anwendungen keine Netzwerkkommunikationsdaten gesendet werden.

Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des Servers für die Erfassung von Telemetriedaten erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So erstellen Sie eine Telemetrie-Ausnahme (in der Web Console und Cloud Console):

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (On-Premises)** aus.
6. Klicken Sie im Block **Allgemeine Ausnahmen** auf **Hinzufügen**.

   Das Fenster **Ausschlussregel hinzufügen** wird geöffnet.
7. Ändern Sie bei Bedarf den Status der Regel. Die Regel ist standardmäßig aktiviert.
8. Geben Sie einen Namen für die Regel ein.
9. Wählen Sie die Aktion aus, die bei Auslösung der Regel ausgeführt werden soll:
   - **Nicht sammeln**. Das gefilterte Ereignis wird aus den zu sendenden Telemetriedaten ausgeschlossen.
   - **IOA ausschließen**. Das Trigger-Ereignis der IOA-Regel wird aus den zu sendenden Telemetriedaten ausgeschlossen.
10. Wenn die Option **IOA ausschließen** ausgewählt ist, geben Sie an, welche IOA-Regeln zu den Ausnahmen hinzugefügt werden sollen:
    - **Alle ausschließen**. Wenn die angegebene Bedingung erfüllt ist, werden die Ereignisse, die basierend auf allen IOA-Regeln generiert wurden, von der Telemetrie ausgeschlossen.
    - **Nach GUID ausschließen**. Geben Sie die GUID der IOA-Regel an. Sie können mehrere GUIDs durch `,` getrennt angeben. Details über die IOA-Regeln finden Sie in der Hilfe zu EDR Expert (on-premises).
11. Geben Sie die Filterbedingung an:
    a. Wählen Sie den Namen des Feldes aus, nach dem gefiltert werden soll.
    b. Wählen Sie einen Operator aus (siehe folgende Tabelle) und geben Sie den Wert an, mit dem der Feldwert aus dem Ereignis verglichen werden soll.

Liste der Bedingungsoperatoren

Operator	Beschreibung
<	Wenn der Feldwert kleiner ist als der in der Bedingung angegebene Wert, wird das Ereignis herausgefiltert.
≤	Wenn der Feldwert kleiner oder gleich dem in der Bedingung angegebenen Wert ist, wird das Ereignis herausgefiltert.
=	Wenn der Feldwert mit dem in der Bedingung angegebenen Wert übereinstimmt, wird das Ereignis herausgefiltert.
≥	Wenn der Feldwert größer oder gleich dem in der Bedingung angegebenen Wert ist, wird das Ereignis herausgefiltert.
>	Wenn der Feldwert größer als der in der Bedingung angegebene Wert ist, wird das Ereignis herausgefiltert.
≠	Wenn der Feldwert nicht mit dem in der Bedingung angegebenen Wert übereinstimmt, wird das Ereignis herausgefiltert.

Operator	Beschreibung
ist ähnlich	Wenn der Feldwert mit der in der Bedingung angegebenen Maske übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen `*` und `?`:
ist nicht ähnlich	Wenn der Feldwert nicht mit der in der Bedingung angegebenen Maske übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen `*` und `?`:
ein Element von	Wenn der Feldwert mit einem der Werte in der Liste übereinstimmt, die in der Bedingung angegeben sind, gilt das Ereignis als gefiltert.
kein Element von	Wenn der Feldwert mit keinem der Werte in der Liste übereinstimmt, die in der Bedingung angegeben sind, gilt das Ereignis als gefiltert.
entspricht einem Element von	Wenn der Feldwert mit einer der in der Bedingung angegebenen Masken übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen * und ?.
entspricht keinem Element von	Wenn der Feldwert mit keiner der in der Bedingung angegebenen Masken übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen * und ?.
vorhanden	Wenn das in der Bedingung angegebene Feld im Ereignis vorhanden ist, wird das Ereignis herausgefiltert.
nicht vorhanden	Wenn das in der Bedingung angegebene Feld nicht im Ereignis vorhanden ist, wird das Ereignis herausgefiltert.
enthält	Wenn der in der Bedingung angegebene Wert im Feldwert vorhanden ist, wird das Ereignis herausgefiltert.
ist gleich	Wenn der Feldwert mit dem in der Bedingung angegebenen Wert übereinstimmt, wird das Ereignis herausgefiltert. Bei der Untersuchung wird die Groß-/Kleinschreibung nicht berücksichtigt.
bitweises UND	Wenn das Ergebnis der bitweisen UND-Operation (&) zwischen dem Feldwert und dem in der Bedingung angegebenen Wert gleich 1 ist, wird das Ereignis herausgefiltert.

12. Bei Bedarf können Sie komplexe Filterkriterien erstellen, indem Sie mehrere Filterbedingungen und Bedingungsgruppen hinzufügen. Sie können einer Bedingungsgruppe auch verschachtelte Bedingungen und Bedingungsgruppen hinzufügen. Sie können die folgenden Operatoren angeben:

    - **UND** bedeutet, dass der Filter die Ereignisse auswählt, die alle angegebenen Bedingungen erfüllen.
    - **ODER** bedeutet, dass der Filter die Ereignisse auswählt, die eine der angegebenen Bedingungen erfüllen.
    - **NICHT** (Um diesen Operator zu verwenden, wählen Sie die Option **Davor NICHT einfügen**) bedeutet, dass der Filter die Ereignisse auswählt, die keine der angegebenen Bedingungen erfüllen.

    Bedingungen und Bedingungsgruppen der ersten Ebene werden mit dem Operator **UND** kombiniert.

13. Wenn auf Ihrem Computer die Open Single Management Platform (OSMP) ausgeführt wird, können Sie die erstellte Filterregel überprüfen. Klicken Sie zur Überprüfung auf **Regel überprüfen**.

    Im nächsten Fenster wird eine Ereignistabelle angezeigt, die nach der erstellten Regel gefiltert wurde. Weitere Informationen finden Sie in der Hilfe zu EDR Expert (on-premises).

14. Fügen Sie bei Bedarf unter **Alle Ereignistypen** Telemetrie-Ausnahmen hinzu, die vom Ereignistyp abhängen.

    a. Klicken Sie auf den Namen des Ereignistyps.

    b. Klicken Sie im angezeigten Fenster auf **Manuell einrichten**.

    c. Konfigurieren Sie bei Bedarf die Telemetrie-Übertragung für den ausgewählten Ereignistyp. Verwenden Sie dazu den Schalter **Ereignis senden**. Standardmäßig ist die Telemetrie-Übertragung für alle Ereignistypen aktiviert.

    d. Klicken Sie im Block **Ausschlussregeln** auf **Hinzufügen**.

    Das Fenster **Ausschlussregel hinzufügen** wird geöffnet.

    e. Führen Sie für jede hinzugefügte Regel die in den Schritten 7 bis 13 beschriebenen Aktionen aus.

15. Für einige Ereignistypen können Sie auch Einschlussregeln hinzufügen, um die gesammelten Telemetriedaten zu erweitern:

    a. Klicken Sie im Block **Einschlussregeln** auf **Hinzufügen**.

    Das Fenster **Einschlussregeln hinzufügen** wird geöffnet.

    b. Geben Sie einen Namen für die Regel ein.

    c. Geben Sie unter **Bedingung** die Werte für die angezeigten Felder ein. Der Typ der verfügbaren Felder hängt vom ausgewählten Ereignis ab.

> Ausschlussregeln haben höhere Priorität als Einschlussregeln.

16. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Ereignisfilter für EDR Expert (on-premises) exportieren und importieren

Sie können die Ausnahmeliste in eine json-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Ereignis-IDs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup der Ereignisfilter anzulegen oder die Listen auf einen anderen Server zu migrieren.

> Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des Servers für die Erfassung von Telemetriedaten erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So exportieren und importieren Sie Ereignisfilter (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
5. Klicken Sie im Block **Telemetrie-Einstellungen → Telemetrie für EDR Expert (on-premises)** auf **Einstellungen**.
6. So exportieren Sie die Ereignisfilter:

    a. Klicken Sie auf **Exportieren**.

    Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

    b. Speichern Sie die Datei.

    Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.

7. So importieren Sie Ereignisfilter:

    a. Klicken Sie auf **Importieren**.

    b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.

    c. Öffnen Sie die Datei.

    Falls auf dem Computer bereits Ereignisfilterungsregeln vorhanden sind, ersetzt Kaspersky Endpoint Security während des Importvorgangs.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So exportieren und importieren Sie Ereignisfilter (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

    Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.

5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (On-Premises)** aus.

6. So exportieren Sie die Ereignisfilter:

    a. Klicken Sie auf **Exportieren**.

    b. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

    c. Speichern Sie die Datei.

    Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.

7. So importieren Sie Ereignisfilter:

    a. Klicken Sie auf **Import**.

    b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.

    c. Wählen Sie aus, auf welche Weise die Regeln für die Ereignisfilterung importiert werden sollen: Regeln zu vorhandenen Regeln hinzufügen oder vorhandene Regeln verwerfen und durch neue ersetzen.

    d. Öffnen Sie die Datei.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Sie können Ereignisfilter auch über die Befehlszeile exportieren oder importieren.

Besonderheiten bei der Verwendung von Richtlinienprofilen zur Konfiguration der Integration mit EDR Expert (on-premises) und EDR (KATA)

Um im Rahmen einer einzigen Richtlinie die Integration mit EDR (KATA) für bestimmte Administrationsgruppen und mit EDR Expert (on-premises) für andere Administrationsgruppen zu konfigurieren, müssen Sie Richtlinienprofile verwenden. Sie müssen die Einstellungen für die Integration mit EDR (KATA) in den Richtlinieneigenschaften konfigurieren. Die Integration mit EDR Expert (on-premises) für ausgewählte Administrationsgruppen sollte in den Eigenschaften der Richtlinienprofile konfiguriert werden.

Beim Verwenden von Richtlinienprofilen zum Konfigurieren der Integration mit EDR Expert (on-premises) gelten die folgenden Einschränkungen:

- Wenn Sie die Integration mit EDR Expert (on-premises) in den Richtlinieneigenschaften konfigurieren, gelten diese Einstellungen für alle Administrationsgruppen. Integrationseinstellungen aus Richtlinienprofilen werden nicht angewendet.

- Wenn Sie Richtlinienprofile verwenden, um die Integration mit EDR Expert (on-premises) zu konfigurieren, können Sie keine Richtlinien über die Verwaltungskonsole (MMC) verwalten. Wenn Sie die Richtlinieneigenschaften in der Verwaltungskonsole öffnen, werden die Einstellungen für die Integration mit EDR Expert (on-premises) in den Richtlinienprofilen durch die Einstellungen aus der Richtlinie überschrieben, wodurch die Komponente nicht ordnungsgemäß funktioniert. Sie müssen die Einstellungen der Komponente Endpoint Detection and Response Expert (on-premises) gemäß der folgenden Anleitung zurücksetzen.

- Wenn Sie Richtlinienprofile verwenden, um die Integration mit EDR Expert (on-premises) zu konfigurieren, können Sie keine untergeordneten Richtlinien verwenden.

Wenn Sie bereits eine Richtlinie in einer früheren Version des Web-Plug-ins konfiguriert haben, müssen Sie die Einstellungen der Komponente Endpoint Detection and Response Expert (on-premises) zurücksetzen, um die Integrationseinstellungen von EDR Expert (on-premises) aus den Richtlinienprofilen auf verwaltete Geräte anzuwenden.

So setzen Sie die Komponenteneinstellungen zurück:

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (On-Premises)**.

5. Ändern Sie den Funktionsmodus von **Endpoint Detection and Response Expert (Version 7.1 oder älter)** zu **Modus für Endpoint Detection and Response Expert (Version 8.0 oder höher)**.

6. Wechseln Sie zurück zu **Endpoint Detection and Response Expert (Version 7.1 oder älter)**.

7. Speichern Sie die vorgenommenen Änderungen.

Endpoint Detection and Response Expert (cloud)

Die Integration von Kaspersky Endpoint Security in Kaspersky Endpoint Detection and Response Expert (cloud) ist vorübergehend nicht verfügbar. Diese Funktionalität wird planmäßig bis Ende 2026 unterstützt. Bitte beachten Sie unsere Versionshinweise. Dort finden Sie aktuelle Informationen über Programm-Upgrades und neue Funktionen.



Kaspersky Endpoint Security unterstützt die Integration in die Lösung Kaspersky Endpoint Detection and Response Expert (cloud). *Kaspersky Endpoint Detection and Response Expert (cloud)* ist eine Cybersicherheitslösung für Unternehmen. Mit den darin enthaltenen Kaspersky-Anwendungen kann sich ein Unternehmen vor den meisten Arten von Cyber-Risiken schützen und die wichtigsten Verbreitungsszenarien für Bedrohungen abdecken. Die Komponenten von EDR Expert (cloud) werden auf der Open Single Management Platform (OSMP) bereitgestellt. Diese Plattform führt plattformübergreifende Szenarien auf einer einzigen Benutzeroberfläche aus und ermöglicht die Integration von Kaspersky-Programmen in Drittersteller-Programme, um ein umfassendes Sicherheitssystem zu gestalten.

Eines der zentralen Elemente dieser Lösung ist *SIEM*. SIEM verfolgt Ereignisse, die von allen Komponenten stammen, und stellt mithilfe von Herstellerregeln und benutzerdefinierten Regeln Zusammenhänge zwischen diesen Ereignissen her. EDR Expert (cloud) analysiert von der Unternehmensinfrastruktur empfangene Protokolle und Telemetriedaten, um Angriffe automatisch zu erkennen, und ermöglicht die Untersuchung von Vorfällen. Dazu dient ein einheitlicher Untersuchungsgraph, der alle in EDR Expert (cloud) erfassten Ereignisse kombiniert, einschließlich der Ereignisse aus Kaspersky-Anwendungen und Drittanbieter-Sicherheitsprodukten.

Zur Reaktion auf komplexe Vorfälle verwendet EDR Expert (cloud) vordefinierte und benutzerdefinierte Szenarien. Sie können auch Reaktionen aus Drittanbieter-Programmen sowie Reaktionsszenarien verwenden, an denen mehrere Programme beteiligt sind.

Threat Intelligence-Tools

Kaspersky Endpoint Detection and Response verwendet die folgenden Threat Intelligence-Tools:

- Integration in Kaspersky Threat Intelligence Portal, das Informationen über die Reputation von Dateien und Webadressen enthält und anzeigt.
- Kaspersky Threats-Datenbank.
- Die Cloud-Service-Infrastruktur von Kaspersky Security Network (im Folgenden auch „KSN“ genannt), die Echtzeitzugriff auf Datei-, Website- und Software-Reputationsinformationen aus der Kaspersky-Wissensdatenbank bietet. Durch die Verwendung von Daten aus Kaspersky Security Network wird die Reaktion der Kaspersky-Programme auf Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem verringert sich das Risiko von Fehlalarmen.

Funktionsweise der Lösung

Kaspersky Endpoint Security wird auf den einzelnen Computern einer IT-Unternehmensinfrastruktur installiert und überwacht kontinuierlich Prozesse, offene Netzwerkverbindungen und geänderte Dateien.

Informationen über Ereignisse auf dem Computer (Telemetrie) werden an den Server von EDR Expert (cloud) gesendet. In diesem Fall sendet Kaspersky Endpoint Security an die Telemetrie-Erfassungsserver auch Informationen über die vom Programm erkannten Bedrohungen sowie Informationen über die Verarbeitungsergebnisse dieser Bedrohungen.

Die Integration von EDR Expert (cloud) wird in der Kaspersky Security Center-Konsole konfiguriert. Anschließend wird der integrierte Agent über Open Single Management Platform (OSMP) verwaltet. Dies bezieht sich beispielsweise auch auf folgende Vorgänge: Aufgaben ausführen, Objekte in der Quarantäne verwalten und Berichte anzeigen.

Integration des integrierten Agenten in EDR Expert (cloud)

Um die Integration in die Lösung Kaspersky Endpoint Detection and Response (cloud) einzurichten, müssen Sie die Komponente Endpoint Detection and Response Expert (cloud) installieren und Kaspersky Endpoint Security konfigurieren.

Die Komponenten Endpoint Detection and Response Optimum, Endpoint Detection and Response Expert (cloud) und Endpoint Detection and Response Expert (on-premises) sind nicht miteinander kompatibel.

Betriebsbedingungen für EDR Expert (Cloud)

Damit EDR Expert (cloud) funktioniert, müssen die folgenden Bedingungen erfüllt sein:

- Die Infrastruktur von Kaspersky Endpoint Detection and Response Expert (cloud) ist in Ihrer Region verfügbar. Informationen zur Verfügbarkeit der Infrastruktur von EDR Expert (cloud) in Ihrer Region erhalten Sie beim Technischen Support.
- OSMP (Open Single Management Platform) ist installiert.
- Kaspersky Endpoint Security im Standardmodus installiert.
- Kaspersky Endpoint Security ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Sie haben die Bedingungen der Vereinbarung zur Datenverarbeitung für Kaspersky Endpoint Detection and Response Expert (cloud) akzeptiert.
- Die Komponente Endpoint Detection and Response Expert (cloud) ist aktiviert.
- Die Anwendungskomponenten, die den Betrieb von EDR Expert (cloud) gewährleisten, sind aktiviert und betriebsbereit:
  - 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.

Schritte zur Integration mit EDR Expert (Cloud)

Die Einrichtung der Integration für EDR Expert (cloud) umfasst die folgenden Schritte:

1. **Installation der Komponente Endpoint Detection and Response Expert (cloud)**

   Sie können die Komponente Endpoint Detection and Response Expert (cloud) während der Installation oder beim Upgrade auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   > Sie müssen Ihren Computer neu starten, um das Upgrade der App mit der neuen Komponente abzuschließen.

2. **Kaspersky Endpoint Detection and Response Expert (cloud) aktivieren**

   Sie müssen eine separate Lizenz für Kaspersky Endpoint Detection and Response Expert (cloud) kaufen.

   Die Funktionalität ist verfügbar, sobald ein separater Schlüssel für Kaspersky Endpoint Detection and Response (cloud) hinzugefügt wurde. Dadurch werden zwei Schlüssel auf dem Computer hinzugefügt: ein Schlüssel für Kaspersky Endpoint Security und ein Schlüssel für Kaspersky Endpoint Detection and Response (cloud).

   Die Lizenzierung der eigenständigen Funktionalität von Endpoint Detection and Response (cloud) entspricht der Lizenzierung von Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die Funktionalität von EDR Expert (cloud) in der Lizenz enthalten ist und in der lokalen Anwendungsoberfläche ausgeführt wird.

3. **Verbindung mit dem Telemetrie-Erfassungsserver und dem Reaktionsserver herstellen**

   Kaspersky Endpoint Detection and Response Expert (cloud) erfordert eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und zwei Servern:

   - Ein *Telemetrie-Erfassungsserver* ist Teil einer SIEM-Lösung, die Informationen über auf dem Computer auftretende Ereignisse sammelt, normalisiert, korreliert, analysiert und speichert.
   - Ein *Reaktionsserver* ist ein Server, der Daten empfängt und sendet, das Verhalten von Objekten analysiert und die Ergebnisse solcher Untersuchungen veröffentlicht.

   So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, mit EDR Expert (cloud) (in der Web Console)

   1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
   2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

      Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
   3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
   4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (Cloud)**.

5. Aktivieren Sie die Komponente mithilfe des Schalters **Endpoint Detection and Response Expert (Cloud) DEAKTIVIERT**.

6. Wenn die aktuelle Richtlinie eine untergeordnete Richtlinie ist und die übergeordnete Richtlinie Änderungen an den Integrationseinstellungen für EDR Expert (cloud) untersagt (geschlossenes „Vorhängeschloss"), können Sie die Vererbung von Einstellungen im Abschnitt **Vererbung** konfigurieren:

   - **Verbindungseinstellungen aus der Richtlinie übernehmen** (Standardwert). Die Verbindungseinstellungen werden von der übergeordneten Richtlinie vererbt. Sie können die Einstellungen nicht ändern.

   - **Benutzerdefinierte Verbindungseinstellungen verwenden**. Sie können die Verbindungseinstellungen manuell konfigurieren.

7. Auf der Registerkarte **Reaktionsserver** werden der vollständig qualifizierte Domänenname und der Port des Reaktionsservers angezeigt, die automatisch abgerufen werden. Wenn die Sicherheitsrichtlinie in Ihrer Infrastruktur keine direkte Verbindung mit Servern von EDR Expert (cloud) zulässt, können Sie eine Verbindung über einen TCP-Tunnel einrichten:

   a. Aktivieren Sie das Kontrollkästchen **TCP-Tunnel für die Reaktion verwenden**.

   b. Geben Sie die Serveradresse (IPv4, IPv6) und den Port für die Tunnelverbindung an.

8. Legen Sie bei Bedarf im Feld **Synchronisierungsanfrage an Server senden alle (Min.)** fest, wie häufig Synchronisierungsanfragen an den Server gesendet werden sollen. Während der Synchronisierung empfängt Kaspersky Endpoint Security Aufgaben zur Reaktion auf Bedrohungen und sendet Aufgabenergebnisse.

9. Gehen Sie zur Registerkarte **Telemetrie-Erfassungsserver**.

10. Konfigurieren Sie die Verbindungseinstellungen für den Server zur Erfassung von Telemetriedaten:

    a. Klicken Sie auf den Link **Ändern**.

    b. Wählen Sie im geöffneten Fenster den Telemetrie-Erfassungsserver aus der Liste aus. Der KUMA-Kollektor dient in EDR Expert (cloud) als Telemetrie-Erfassungsserver. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

    Falls beim Verbinden mit dem Telemetrie-Erfassungsserver ein Fehler auftritt, wählen Sie einen anderen Server aus. Sollte eine Verbindung zum Telemetrie-Erfassungsserver nicht möglich sein, wenden Sie sich bitte an den Technischen Support.

    c. Bei Bedarf können Sie eine Verbindung zum Telemetrie-Erfassungsserver über einen TCP-Tunnel konfigurieren, genauso wie für den Reaktionsserver.

11. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Sie können den Komponentenstatus mithilfe von *Bericht über den Status der Programmkomponenten* überprüfen. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **Endpoint Detection and Response Expert (cloud)** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Telemetrie-Einstellungen für EDR Expert (cloud) konfigurieren

Telemetrie ist eine Liste von Ereignissen, die auf dem geschützten Computer aufgetreten sind. Kaspersky Endpoint Security analysiert Telemetrie-Daten und sendet diese während der Synchronisierung an Telemetrie-Erfassungsserver. Telemetrie-Ereignisse treffen fast kontinuierlich auf dem Server ein. Kaspersky Endpoint Security startet die Synchronisierung mit dem Server, wenn eine der folgenden Bedingungen erfüllt ist:

- Das Synchronisierungsintervall ist abgelaufen.
- Die Anzahl der Ereignisse im Puffer überschreitet die Höchstgrenze.

Dann synchronisiert die App standardmäßig alle 30 Sekunden oder immer, wenn der Puffer 1024 Ereignisse enthält. Sie können das Synchronisierungsverhalten in der Richtlinie von Kaspersky Endpoint Security anpassen und optimale Werte für Ihre Netzwerklast auswählen (siehe Anleitung unten).

Bei fehlender Verbindung zwischen Kaspersky Endpoint Security und dem Server stellt die App neue Ereignisse in die Warteschlange. Sobald die Verbindung wiederhergestellt wird, sendet Kaspersky Endpoint Security die Ereignisse aus der Warteschlange in der richtigen Reihenfolge an den Server. Um eine Überlastung des Servers zu vermeiden, kann Kaspersky Endpoint Security bestimmte Ereignisse überspringen. Diese Option können Sie in den Einstellungen für die Ereignisübertragung optimieren und dafür beispielsweise einen Höchstwert für Ereignisse pro Stunde festlegen (siehe Anleitung unten).

Führen Sie die folgenden Schritte aus, um die Telemetrie-Einstellungen zu konfigurieren:

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **Endpoint Detection and Response Expert (Cloud)**.
5. Wählen Sie im folgenden Fenster die Registerkarte **Einstellungen für die Datenübertragung** aus.
6. Stellen Sie sicher, dass das Kontrollkästchen **Telemetrie-Übertragung AKTIVIERT** aktiviert ist.
7. Aktivieren Sie bei Bedarf die Funktionalität **Telemetrie nur mit IOA senden**. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen. Die Funktionalität ist standardmäßig deaktiviert.
8. Passen Sie bei Bedarf die Einstellungen für die Serversynchronisierung an:

   - **Maximale Verzögerung der Ereignisübertragung (Sek.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
   - **Maximale Anzahl der Ereignispakete**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.
9. Gehen Sie zur Registerkarte **Anforderungsbegrenzung**.

10. Deaktivieren Sie bei Bedarf die Anforderungsbegrenzung mithilfe des Umschalters **Anforderungsbegrenzung AKTIVIERT**.

    Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Diese Option ist standardmäßig aktiviert.

11. Konfigurieren Sie die Optimierungseinstellungen für das Senden von Ereignissen an den Server:

    - **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.

    - **Prozentsatz für die Überschreitung des Ereignislimits (%)**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

12. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Telemetrie-Ausnahmen für EDR Expert (cloud)

Um die Leistung zu verbessern und die Datenübertragung an den Telemetrie-Erfassungsserver zu optimieren, können Sie Telemetrie-Ausnahmen hinzufügen. Sie können beispielsweise festlegen, dass für einzelne Anwendungen keine Netzwerkkommunikationsdaten gesendet werden.

Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des Servers für die Erfassung von Telemetriedaten erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So erstellen Sie eine Telemetrie-Ausnahme (in der Web Console und Cloud Console):

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (Cloud)** aus.
6. Klicken Sie im Block **Allgemeine Ausnahmen** auf **Hinzufügen**.

   Das Fenster **Ausschlussregel hinzufügen** wird geöffnet.

7. Ändern Sie bei Bedarf den Status der Regel. Die Regel ist standardmäßig aktiviert.

8. Geben Sie einen Namen für die Regel ein.

9. Wählen Sie die Aktion aus, die bei Auslösung der Regel ausgeführt werden soll:

   - **Nicht sammeln**. Das gefilterte Ereignis wird aus den zu sendenden Telemetriedaten ausgeschlossen.

   - **IOA ausschließen**. Das Trigger-Ereignis der IOA-Regel wird aus den zu sendenden Telemetriedaten ausgeschlossen.

10. Wenn die Option **IOA ausschließen** ausgewählt ist, geben Sie an, welche IOA-Regeln zu den Ausnahmen hinzugefügt werden sollen:

    - **Alle ausschließen**. Wenn die angegebene Bedingung erfüllt ist, werden die Ereignisse, die basierend auf allen IOA-Regeln generiert wurden, von der Telemetrie ausgeschlossen.

    - **Nach GUID ausschließen**. Geben Sie die GUID der IOA-Regel an. Sie können mehrere GUIDs durch `,` getrennt angeben. Details über die IOA-Regeln finden Sie in der Hilfe zu EDR Expert (cloud).

11. Geben Sie die Filterbedingung an:

    a. Wählen Sie den Namen des Feldes aus, nach dem gefiltert werden soll.

    b. Wählen Sie einen Operator aus (siehe folgende Tabelle) und geben Sie den Wert an, mit dem der Feldwert aus dem Ereignis verglichen werden soll.

Liste der Bedingungsoperatoren

Operator	Beschreibung
<	Wenn der Feldwert kleiner ist als der in der Bedingung angegebene Wert, wird das Ereignis herausgefiltert.
≤	Wenn der Feldwert kleiner oder gleich dem in der Bedingung angegebenen Wert ist, wird das Ereignis herausgefiltert.
=	Wenn der Feldwert mit dem in der Bedingung angegebenen Wert übereinstimmt, wird das Ereignis herausgefiltert.
≥	Wenn der Feldwert größer oder gleich dem in der Bedingung angegebenen Wert ist, wird das Ereignis herausgefiltert.
>	Wenn der Feldwert größer als der in der Bedingung angegebene Wert ist, wird das Ereignis herausgefiltert.
≠	Wenn der Feldwert nicht mit dem in der Bedingung angegebenen Wert übereinstimmt, wird das Ereignis herausgefiltert.
ist ähnlich	Wenn der Feldwert mit der in der Bedingung angegebenen Maske übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen `*` und `?`.
ist nicht ähnlich	Wenn der Feldwert nicht mit der in der Bedingung angegebenen Maske übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen `*` und `?`.
ein Element von	Wenn der Feldwert mit einem der Werte in der Liste übereinstimmt, die in der Bedingung angegeben sind, gilt das Ereignis als gefiltert.
kein Element von	Wenn der Feldwert mit keinem der Werte in der Liste übereinstimmt, die in der Bedingung angegeben sind, gilt das Ereignis als gefiltert.
entspricht einem Element von	Wenn der Feldwert mit einer der in der Bedingung angegebenen Masken übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen * und ?.
entspricht keinem Element von	Wenn der Feldwert mit keiner der in der Bedingung angegebenen Masken übereinstimmt, wird das Ereignis herausgefiltert. Die Anwendung unterstützt bei der Eingabe einer Maske die Zeichen * und ?.
vorhanden	Wenn das in der Bedingung angegebene Feld im Ereignis vorhanden ist, wird das Ereignis herausgefiltert.
nicht vorhanden	Wenn das in der Bedingung angegebene Feld nicht im Ereignis vorhanden ist, wird das Ereignis herausgefiltert.
enthält	Wenn der in der Bedingung angegebene Wert im Feldwert vorhanden ist, wird das Ereignis herausgefiltert.

Operator	Beschreibung
ist gleich	Wenn der Feldwert mit dem in der Bedingung angegebenen Wert übereinstimmt, wird das Ereignis herausgefiltert. Bei der Untersuchung wird die Groß-/Kleinschreibung nicht berücksichtigt.
bitweises UND	Wenn das Ergebnis der bitweisen UND-Operation (&) zwischen dem Feldwert und dem in der Bedingung angegebenen Wert gleich 1 ist, wird das Ereignis herausgefiltert.

12. Bei Bedarf können Sie komplexe Filterkriterien erstellen, indem Sie mehrere Filterbedingungen und Bedingungsgruppen hinzufügen. Sie können einer Bedingungsgruppe auch verschachtelte Bedingungen und Bedingungsgruppen hinzufügen. Sie können die folgenden Operatoren angeben:

    - **UND** bedeutet, dass der Filter die Ereignisse auswählt, die alle angegebenen Bedingungen erfüllen.
    - **ODER** bedeutet, dass der Filter die Ereignisse auswählt, die eine der angegebenen Bedingungen erfüllen.
    - **NICHT** (Um diesen Operator zu verwenden, wählen Sie die Option **Davor NICHT einfügen**) bedeutet, dass der Filter die Ereignisse auswählt, die keine der angegebenen Bedingungen erfüllen.

    Bedingungen und Bedingungsgruppen der ersten Ebene werden mit dem Operator **UND** kombiniert.

13. Um die erstellte Filterregel zu überprüfen, klicken Sie auf **Regel überprüfen**.

    Im nächsten Fenster wird eine Ereignistabelle angezeigt, die nach der erstellten Regel gefiltert wurde. Weitere Informationen finden Sie in der Hilfe zu EDR Expert (cloud).

14. Fügen Sie bei Bedarf unter **Alle Ereignistypen** Telemetrie-Ausnahmen hinzu, die vom Ereignistyp abhängen.

    a. Klicken Sie auf den Namen des Ereignistyps.

    b. Klicken Sie im angezeigten Fenster auf **Manuell einrichten**.

    c. Konfigurieren Sie bei Bedarf die Telemetrie-Übertragung für den ausgewählten Ereignistyp. Verwenden Sie dazu den Schalter **Ereignis senden**. Standardmäßig ist die Telemetrie-Übertragung für alle Ereignistypen aktiviert.

    d. Klicken Sie im Block **Ausschlussregeln** auf **Hinzufügen**.

    Das Fenster **Ausschlussregel hinzufügen** wird geöffnet.

    e. Führen Sie für jede hinzugefügte Regel die in den Schritten 7 bis 13 beschriebenen Aktionen aus.

15. Für einige Ereignistypen können Sie auch Einschlussregeln hinzufügen, um die gesammelten Telemetriedaten zu erweitern:

    a. Klicken Sie im Block **Einschlussregeln** auf **Hinzufügen**.

    Das Fenster **Einschlussregeln hinzufügen** wird geöffnet.

    b. Geben Sie einen Namen für die Regel ein.

    c. Geben Sie unter **Bedingung** die Werte für die angezeigten Felder ein. Der Typ der verfügbaren Felder hängt vom ausgewählten Ereignis ab.

> Ausschlussregeln haben höhere Priorität als Einschlussregeln.

16. Um die Richtlinie auf Computer anzuwenden, vergewissern Sie sich, dass die Vorhängeschlösser geschlossen sind (🔒), und speichern Sie Ihre Änderungen.

So exportieren oder importieren Sie Ereignisfilter für EDR Expert (cloud)

Sie können die Ausnahmeliste in eine json-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Ereignis-IDs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup der Ereignisfilter anzulegen oder die Listen auf einen anderen Server zu migrieren.

Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des Servers für die Erfassung von Telemetriedaten erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So exportieren oder importieren Sie Ereignisfilter (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (Cloud)** aus.
6. So exportieren Sie die Ereignisfilter:

   a. Klicken Sie auf **Exportieren**.

   b. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   c. Speichern Sie die Datei.

   Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.
7. So importieren Sie Ereignisfilter:

   a. Klicken Sie auf **Import**.

   b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.

   c. Wählen Sie aus, auf welche Weise die Regeln für die Ereignisfilterung importiert werden sollen: Regeln zu vorhandenen Regeln hinzufügen oder vorhandene Regeln verwerfen und durch neue ersetzen.

   d. Öffnen Sie die Datei.

8. Um die Richtlinie auf Computer anzuwenden, vergewissern Sie sich, dass die Vorhängeschlösser geschlossen sind (🔒), und speichern Sie Ihre Änderungen.

    1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
    2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

       Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
    3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
    4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
    5. Wählen Sie die Registerkarte **Telemetrie für EDR Expert (Cloud)** aus.
    6. So exportieren Sie die Ereignisfilter:

        a. Klicken Sie auf **Exportieren**.

        b. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

        c. Speichern Sie die Datei.

           Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.
    7. So importieren Sie Ereignisfilter:

        a. Klicken Sie auf **Import**.

        b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.

        c. Wählen Sie aus, auf welche Weise die Regeln für die Ereignisfilterung importiert werden sollen: Regeln zu vorhandenen Regeln hinzufügen oder vorhandene Regeln verwerfen und durch neue ersetzen.

        d. Öffnen Sie die Datei.
    8. Um die Richtlinie auf Computer anzuwenden, vergewissern Sie sich, dass die Vorhängeschlösser geschlossen sind (🔒), und speichern Sie Ihre Änderungen.

Verwalten der 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. Unter Quarantäne stehende Dateien werden in verschlüsselter Form gespeichert und gefährden die Sicherheit des Gerätes nicht. Kaspersky Endpoint Security verwendet die Quarantäne nur dann, wenn das Programm in Kaspersky Detection and Response-Lösungen integriert ist. In anderen Fällen legt Kaspersky Endpoint Security die entsprechende Datei im Backup ab. Ausführliche Informationen zur Verwaltung der Quarantäne als Teil dieser Lösungen finden Sie in der Hilfe zu Kaspersky Sandbox, Hilfe zu Kaspersky Endpoint Detection and Response Optimum, Hilfe zu Kaspersky Endpoint Detection and Response Expert, Hilfe zu Kaspersky Anti Targeted Attack Platform, und Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises).

Kaspersky Endpoint Security verwendet das Systemkonto (SYSTEM), um Dateien unter Quarantäne zu stellen.

Sie können die Quarantäneeinstellungen nur über die Kaspersky Security Center-Konsole konfigurieren. Mit der Kaspersky Security Center-Konsole können Sie auch unter Quarantäne stehende Objekte verwalten (z. B. wiederherstellen, löschen oder hinzufügen). Lokal (auf dem Computer) können Sie das Objekt nur über die Befehlszeile wiederherstellen.

Konfigurieren der maximalen Quarantäne-Größe

Die Größe der Quarantäne ist standardmäßig auf 1024 MB begrenzt. Wenn die maximale Quarantäne-Größe erreicht wird, sendet Kaspersky Endpoint Security keine Dateien mehr und generiert das Ereignis *Zu wenig Platz im Quarantäne-Speicher*. Um zu verhindern, dass die Quarantäne zu viel Speicherplatz einnimmt, können Sie einen Schwellenwert festlegen, ab dem Kaspersky Endpoint Security das Ereignis *Der Quarantäne-Speicher ist fast voll* generiert. Es ist nicht möglich, einen Aufbewahrungszeitraum für Dateien in der Quarantäne festzulegen, damit Dateien automatisch entfernt werden.

Wenn die Lösung Kaspersky Anti Targeted Attack Platform (EDR) in Ihrem Unternehmen bereitgestellt wird, empfehlen wir, die Größe der Quarantäne zu erhöhen. Beim Durchführen eines YARA-Scans kann die Anwendung auf ein großes Speicherabbild stoßen. Wenn die Größe des Speicherauszugs die Größe der Quarantäne überschreitet, wird der YARA-Scan mit einem Fehler beendet und der Speicherauszug wird nicht unter Quarantäne gestellt. Unsere Empfehlung: Legen Sie für die Quarantäne die Größe fest, die der Arbeitsspeicher des Computers hat (z. B. 8 GB), oder deaktivieren Sie die Größenbeschränkung der Quarantäne.

So konfigurieren Sie die maximale Größe der Quarantäne in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Berichte und Speicher** aus.
4. Legen Sie im Block **Quarantäne** die Quarantäne-Größe fest:
   - **Maximale Größe der Quarantäne n MB**. Wenn das Kontrollkästchen aktiviert ist, ist die Quarantäne-Größe auf den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 1024 MB. Wenn die maximale Quarantäne-Größe erreicht wird, sendet Kaspersky Endpoint Security das Ereignis *Zu wenig Platz im Quarantäne-Speicher* an Kaspersky Security Center und veröffentlicht das Ereignis im Windows-Ereignisprotokoll. Die Anwendung stellt vorläufig keine neuen Objekte mehr unter Quarantäne. Sie müssen die Quarantäne manuell leeren.

     Wenn das Kontrollkästchen deaktiviert ist, wird die Quarantäne-Größe durch den auf der Festplatte verfügbaren Speicherplatz begrenzt.

   - **Melden, wenn Quarantäne-Speicher diesen Wert erreicht n Prozent**. Schwellenwert für die Quarantäne. Sie können beispielsweise 50% als Quarantäne-Schwellenwert festlegen. Wenn die Quarantäne den Schwellenwert erreicht, sendet Kaspersky Endpoint Security ein entsprechendes Ereignis an Kaspersky Security Center und veröffentlicht das Ereignis im Windows-Ereignisprotokoll. Die Anwendung stellt weiterhin neue Objekte unter Quarantäne.

     Wenn dieses Kontrollkästchen deaktiviert ist, generiert das Programm keine Ereignisse, falls der Quarantäne-Schwellenwert erreicht wird.
5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die maximale Quarantäne-Größe (in der Web Console und Cloud Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Berichte und Speicher**.
5. Legen Sie im Block **Quarantäne** die Quarantäne-Größe fest:

   - **Maximale Größe der Quarantäne**. Wenn das Kontrollkästchen aktiviert ist, wird die Quarantäne-Größe auf den angegebenen Wert beschränkt. Wenn das Kontrollkästchen deaktiviert ist, wird die Quarantäne-Größe durch den auf der Festplatte verfügbaren Speicherplatz begrenzt. Dies kann für die YARA-Untersuchung erforderlich sein, bei der das Programm möglicherweise eine große Speicherabbilddatei speichert.
   - **Maximale Quarantäne-Größe (MB)**. Wenn das Kontrollkästchen aktiviert ist, ist die Quarantäne-Größe auf den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 1024 MB. Wenn die maximale Quarantäne-Größe erreicht wird, sendet Kaspersky Endpoint Security das Ereignis *Zu wenig Platz im Quarantäne-Speicher* an Kaspersky Security Center und veröffentlicht das Ereignis im Windows-Ereignisprotokoll. Die Anwendung stellt vorläufig keine neuen Objekte mehr unter Quarantäne. Sie müssen die Quarantäne manuell leeren.

     Wenn das Kontrollkästchen deaktiviert ist, wird die Quarantäne-Größe durch den auf der Festplatte verfügbaren Speicherplatz begrenzt.
   - **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 Kaspersky Endpoint Security ein entsprechendes Ereignis an Kaspersky Security Center und veröffentlicht das Ereignis im Windows-Ereignisprotokoll. Die Anwendung stellt weiterhin neue Objekte unter Quarantäne.
6. Speichern Sie die vorgenommenen Änderungen.

Senden von Daten über Quarantäne-Dateien an Kaspersky Security Center

Um Aktionen mit Quarantäne-Objekten in der „Web Console" auszuführen, müssen Sie das Senden von Daten über Quarantäne-Dateien an den Administrationsserver aktivieren. So können Sie z. B. in Web Console eine Datei aus der Quarantäne zur Analyse herunterladen. Dazu muss das Senden von Daten über Quarantäne-Dateien für alle Funktionen von Kaspersky Sandbox und Kaspersky Endpoint Detection and Response aktiviert sein.

So aktivieren Sie die Übertragung von Daten über Quarantäne-Dateien in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Berichte und Speicher** aus.
4. Klicken Sie im Block **Datenübertragung an den Administrationsserver** auf **Einstellungen**.

5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Quarantäne-Dateien**.

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Übertragung von Daten über Quarantäne-Dateien in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen → KSC-Integration**.

5. Aktivieren Sie im Block **Datenübertragung an den Administrationsserver** das Kontrollkästchen **Über Quarantäne-Dateien**.

6. Speichern Sie die vorgenommenen Änderungen.

Als Ergebnis können Sie in der Konsole von Kaspersky Security Center eine Liste der auf Ihrem Computer isolierten Dateien anzeigen. Mit der Kaspersky Security Center-Konsole können Sie unter Quarantäne stehende Objekte auch verwalten (z. B. wiederherstellen, löschen oder hinzufügen). Weitere Informationen über die Arbeit mit der Quarantäne finden Sie in der Hilfe zu Kaspersky Security Center.

Wiederherstellen von Dateien aus der Quarantäne

Kaspersky Endpoint Security stellt Dateien standardmäßig im ursprünglichen Ordner wieder her. Wenn der Zielordner gelöscht wurde oder der Benutzer keine Zugriffsrechte auf diesen Ordner hat, verschiebt die App diese Datei in den Ordner `%DataRoot%\QB\Restored`. Dann müssen Sie die Datei manuell in den Zielordner verschieben.

Um Dateien aus der Quarantäne wiederherzustellen:

1. Klicken Sie im Web Console-Hauptfenster auf **Vorgänge → Datenverwaltung → Quarantäne**.

2. Dadurch wird die Liste der Dateien in der Quarantäne geöffnet. Wählen Sie in dieser Liste die Dateien aus, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.

   Kaspersky Endpoint Security stellt die Datei wieder her. Wenn der Zielordner bereits eine Datei mit diesem Namen enthält, bricht die App die Dateiwiederherstellung ab. Das Programm speichert nach der Wiederherstellung der Datei eine Kopie in der Quarantäne. Um die Datei zu löschen, müssen Sie die Quarantäne manuell leeren.

Überwachung von EDR-Aktionen

Mit Kaspersky Endpoint Security für Windows 12.9 wird das Überwachungscenter für EDR-Aktionen eingeführt. Das *Überwachungscenter für EDR-Aktionen* ist eine Konsole, in der Sie den Threat Response-Verlauf für alle Lösungen von Kaspersky Detection and Response einsehen können. Wenn in Ihrem Unternehmen mehrere Detection and Response-Lösungen bereitgestellt werden (z. B. EDR Optimum und MDR), zeigt Kaspersky Endpoint Security einen Threat Response-Verlauf für alle Lösungen an. Auf diese Weise können Sie die Leistung von Detection and Response-Lösungen auf einem separaten Computer analysieren und die Einstellungen dieser Lösungen optimieren.

Das Überwachungscenter stellt die folgenden Informationen bereit:

- Informationen über Threat Response-Aufgaben (z. B. die Aufgabe *Prozess beenden*)
- Änderungen von Regeln für die Netzwerkisolation und Ausführungsprävention

Wenn bei der Reaktion auf Bedrohungen ein Fehler beim Zugriff auf eine Netzwerkfreigabe erkannt wird, wird dieser Fehler nicht im Threat Response-Verlauf angezeigt.

So gelangen Sie zum Überwachungscenter für EDR-Aktionen:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Assets (Geräte)** aus.
2. Klicken Sie auf den Namen des Computers, auf dem Sie die lokalen Programmeinstellungen anpassen möchten.
   Die Eigenschaften des Computers werden geöffnet.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Klicken Sie auf **Kaspersky Endpoint Security für Windows 14.2**.
   Die lokalen Programmeinstellungen werden geöffnet.
5. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
6. Gehen Sie zu **Detection and Response → Reaktionsverlauf**.

Dadurch wird die Konsole des Überwachungscenter für EDR-Aktionen geöffnet. In der Konsole können Sie den Status von Threat Response-Aufgaben, die Aufgabendauer, Regeländerungen und Details zum Initiator einsehen.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky Endpoint Security für Windows 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. In der KUMA-Konsole werden Ereignisse als Liste ohne Markierungen angezeigt, ähnlich wie im Windows-Ereignisprotokoll.

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.

Integration von Kaspersky Endpoint Security in KUMA

Die Einrichtung der Integration von KES in KUMA umfasst die folgenden Schritte:

1. Fügen Sie in der KUMA-Konsole einen Kollektor hinzu.
2. Konfigurieren Sie in der KUMA-Konsole einen Connector für den Kollektor, um Ereignisse von KES zu empfangen.
3. Aktivieren Sie in der KUMA-Konsole die Zwei-Wege-Authentifizierung (optional).
4. Konfigurieren Sie in der Richtlinie von Kaspersky Endpoint Security für Windows die Einstellungen für die Verbindung von KES mit KUMA.
5. Stellen Sie in der KUMA-Konsole sicher, dass Ereignisse von KES dem richtigen Mandanten zugeordnet und von den richtigen Korrelationsregeln verarbeitet werden.

Vorbereitung auf die Integration von KES mit KUMA

Für die Verwendung von KUMA müssen folgende Bedingungen erfüllt sein:

- Kaspersky Security Center Version 14.2 oder höher. In älteren Versionen von Kaspersky Security Center kann die KUMA-Integrationsfunktionalität nicht aktiviert werden.
- Die Anwendung ist aktiviert und die Funktionalität ist durch die Lizenz abgedeckt.
- Die KUMA-Integrationskomponente ist aktiviert.

Die Vorbereitung auf die Integration von KES mit KUMA umfasst die folgenden Schritte:

1. **Installation der KUMA-Integrationskomponente**

   Sie können die KUMA-Integrationskomponente während der Installation oder beim Upgrade der App auswählen oder die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

   Sie müssen Ihren Computer neu starten, um das Upgrade der App mit der neuen Komponente abzuschließen.

2. **KUMA-Aktivierung**

   Zusätzlich zu einer Lizenz für das Programm Kaspersky Endpoint Security (z. B. Kaspersky Endpoint Security für Unternehmen Standard) benötigen Sie eine separate Lizenz für die Integration von Kaspersky Endpoint Security in KUMA (Add-on für die Integration von Kaspersky Endpoint Security für Windows in KUMA).

   Wenn Sie die App im EDR Agent-Modus installieren, benötigen Sie eine Lizenz für die Integration von Kaspersky Endpoint Security in KUMA, eine Lizenz für die Kaspersky Anti Targeted Attack Platform (KATA) oder eine Lizenz für Kaspersky Managed Detection and Response (MDR). Sie können EDR Agent nicht ausschließlich für KUMA bereitstellen.

   Die Funktionalität ist verfügbar, nachdem der separate KUMA-Schlüssel hinzugefügt wurde. Danach befindet sich auf dem Computer ein weiterer aktiver Schlüssel für die Integration von Kaspersky Endpoint Security in KUMA.

   Die Lizenzverwaltung für die eigenständige KUMA-Funktionalität entspricht der Lizenzverwaltung für Kaspersky Endpoint Security.

   Stellen Sie sicher, dass die KUMA-Funktionalität in der Lizenz enthalten ist und dass sie auf der lokalen App-Oberfläche funktioniert.

Verbinden von KES mit KUMA

So verbinden Sie den Computer, auf dem Kaspersky Endpoint Security installiert ist, mit der KUMA-Lösung:

1. Fügen Sie in der KUMA-Konsole einen Kollektor mit Konnektoren des Typs **tcp**, **udp** oder **http** hinzu und geben Sie die grundlegenden Netzwerkeinstellungen der Verbindung an. Details zur Verwaltung von Konnektoren finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

2. Fügen Sie in der Kaspersky Endpoint Security-Richtlinie die Adressen der KUMA-Kollektoren hinzu und geben Sie die Netzwerkeinstellungen der Verbindung an.

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Verwaltungskonsole (MMC) mit KUMA

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.

3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

4. Wählen Sie im Richtlinienfenster den Punkt **KUMA-Integration** aus.

5. Aktivieren Sie das Kontrollkästchen **KUMA-Integration**.

6. Aktivieren Sie im Block **Integrationseinstellungen** das Kontrollkästchen **Übertragung von Windows-Ereignissen an einen KUMA-Server aktivieren**.

7. Fügen Sie KUMA-Server hinzu:

   a. Klicken Sie auf **Hinzufügen**.

   Dadurch wird ein Formular geöffnet, in dem Sie KUMA-Server hinzufügen können.

   b. Wählen Sie das Protokoll für die Verbindung mit dem KUMA-Server aus: **HTTP/HTTPS**, **TCP**, **UDP**.

   Das Protokoll für die Verbindung mit dem Kollektor in Kaspersky Endpoint Security muss dem Konnektortyp in KUMA entsprechen: **http**, **tcp** oder **udp**.

   > Bei Verwendung des UDP-Protokolls können Daten aufgrund von protokollbedingten Übertragungsverlusten verloren gehen.

   c. Geben Sie die Serveradresse (IPv4, IPv6, FQDN) und den Port für die Verbindung mit dem Server ein (standardmäßig ist Port 443 angegeben).

   Beachten Sie bei der Eingabe der Serveradresse Folgendes:

   - **TCP**:
     - **Ohne TLS**. Sie können entweder die IP-Adresse oder den FQDN des Servers angeben.
     - **Mit TLS**. Sie müssen nur den FQDN des Servers angeben.
   - **HTTP/HTTPS**:
     - **Ohne TLS**. Sie müssen das HTTP-Protokoll explizit in der Serveradresse angeben (z. B. `http://server.com` oder `http://10.10.10.100`).
     - **Mit TLS**. Sie müssen das Protokoll nicht angeben (z. B. `https://server.com` oder `server.com`).
   - **UDP**. Das UDP-Protokoll unterstützt keine TLS-Verschlüsselung. Sie können entweder die IP-Adresse oder den FQDN des Servers angeben.

   Sie können die Serveradresse in den Konnektoreigenschaften in der KUMA-Konsole anzeigen. Weitere Informationen zu KUMA-Konnektoren finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

   d. Klicken Sie auf **OK**.

Kaspersky Endpoint Security verbindet sich mit dem ersten KUMA-Server in der Liste. Wenn die Verbindung fehlschlägt, verbindet sich Kaspersky Endpoint Security mit dem zweiten KUMA-Server in der Liste und so weiter.

8. Konfigurieren Sie, sofern erforderlich, die Einstellung **Maximale Verzögerung der Ereignisübertragung (Sek.)** im Block **Einstellungen für die Datenübertragung**. Wenn die festgelegte Dauer abgelaufen ist, versucht Kaspersky Endpoint Security, eine Verbindung mit demselben Kollektor herzustellen, oder stellt eine Verbindung mit dem nächsten Kollektor in der Liste her, falls es mehrere Kollektoren gibt. Der Standardwert ist 30 Sekunden.

9. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So verbinden Sie einen Computer, auf dem Kaspersky Endpoint Security installiert ist, über die Web Console mit KUMA

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **KUMA-Integration**.

5. Aktivieren Sie den Schalter **KUMA-Integration AKTIVIERT**.

6. Fügen Sie KUMA-Server hinzu:

   a. Klicken Sie auf **Hinzufügen**.

      Dadurch wird ein Formular geöffnet, in dem Sie KUMA-Server hinzufügen können.

   b. Wählen Sie das Protokoll für die Verbindung mit dem KUMA-Server aus: **HTTP/HTTPS**, **TCP**, **UDP**.

      Das Protokoll für die Verbindung mit dem Kollektor in Kaspersky Endpoint Security muss dem Konnektortyp in KUMA entsprechen: **http**, **tcp** oder **udp**.

      > Bei Verwendung des UDP-Protokolls können Daten aufgrund von protokollbedingten Übertragungsverlusten verloren gehen.

   c. Geben Sie die Serveradresse (IPv4, IPv6, FQDN) und den Port für die Verbindung mit dem Server ein (standardmäßig ist Port 443 angegeben).

      Beachten Sie bei der Eingabe der Serveradresse Folgendes:

      - **TCP**:
        - **Ohne TLS**. Sie können entweder die IP-Adresse oder den FQDN des Servers angeben.
        - **Mit TLS**. Sie müssen nur den FQDN des Servers angeben.
      - **HTTP/HTTPS**:
        - **Ohne TLS**. Sie müssen das HTTP-Protokoll explizit in der Serveradresse angeben (z. B. `http://server.com` oder `http://10.10.10.100`).
        - **Mit TLS**. Sie müssen das Protokoll nicht angeben (z. B. `https://server.com` oder `server.com`).
      - **UDP**. Das UDP-Protokoll unterstützt keine TLS-Verschlüsselung. Sie können entweder die IP-Adresse oder den FQDN des Servers angeben.

Sie können die Serveradresse in den Konnektoreigenschaften in der KUMA-Konsole anzeigen. Weitere Informationen zu KUMA-Konnektoren finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform.

d. Klicken Sie auf **OK**.

Kaspersky Endpoint Security verbindet sich mit dem ersten KUMA-Server in der Liste. Wenn die Verbindung fehlschlägt, verbindet sich Kaspersky Endpoint Security mit dem zweiten KUMA-Server in der Liste und so weiter.

7. Konfigurieren Sie, sofern erforderlich, die Einstellung **Maximale Verzögerung beim Versenden von Ereignissen (Sek.)** im Block **Einstellungen der Serververbindung**. Wenn die festgelegte Dauer abgelaufen ist, versucht Kaspersky Endpoint Security, eine Verbindung mit demselben Kollektor herzustellen, oder stellt eine Verbindung mit dem nächsten Kollektor in der Liste her, falls es mehrere Kollektoren gibt. Der Standardwert ist 30 Sekunden.

8. Speichern Sie die vorgenommenen Änderungen.

In der KUMA-Konsole können Sie überprüfen, ob die KUMA-Integration richtig konfiguriert ist (Details finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). Überprüfen Sie den Betriebsstatus der Komponente. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* in der Kaspersky Security Center-Konsole an. Den Betriebsstatus einer Komponente können Sie auch den Berichten in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security entnehmen. Die Komponente **KUMA-Integration** wir zur Liste der Kaspersky Endpoint Security-Komponenten hinzugefügt.

Herstellen einer vertrauenswürdigen Verbindung zwischen KES und KUMA

Sie können eine vertrauenswürdige Verbindung zwischen Kaspersky Endpoint Security und einem KUMA-Kollektor mit einem Konnektor des Typs tcp oder http herstellen. Mit einem Konnektor vom Typ udp kann keine vertrauenswürdige Verbindung hergestellt werden.

Zum Herstellen einer vertrauenswürdigen Verbindung müssen Sie in den Konnektoreinstellungen einen TLS-Modus konfigurieren. Folgende TLS-Modi sind möglich:

- **Disabled**: Verwenden Sie keine TLS-Verschlüsselung. Dieser Status gilt als Standard.
- **Enabled**: Verwenden Sie die TLS-Verschlüsselung, jedoch ohne Zertifikatsüberprüfung.
- **Custom PFX with client authentication**: Verwenden Sie die TLS-Verschlüsselung mit einem PFX-Geheimnis. In diesem Modus wird der Client mit einem Zertifikat authentifiziert.

Kaspersky Endpoint Security unterstützt den TLS-Modus **Custom PFX** nicht. Bei der Integration von KES mit KUMA unter Verwendung von PFX ist eine Benutzerauthentifizierung mit einem Kennwort erforderlich.

Um eine vertrauenswürdige Verbindung zu konfigurieren, benötigen Sie ein TLS-Zertifikat — das *CA-Zertifikat für den Microservice*. Sie können ein TLS-Zertifikat in der KUMA-Konsole abrufen. Details zum Herunterladen von TLS-Zertifikaten finden Sie in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform. Anschließend müssen Sie das TLS-Zertifikat zu Kaspersky Endpoint Security hinzufügen (siehe Anleitung unten).

Um die Verbindung sicherer zu machen, können Sie zusätzlich die Authentifizierung des Computers in KUMA (Zwei-Wege-Authentifizierung) aktivieren. Um eine solche Authentifizierung zu aktivieren, müssen Sie einen Krypto-Container bei einer externen Zertifizierungsstelle erstellen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel im Format PKCS#12. Anschließend müssen Sie in den KUMA-Einstellungen die Zwei-Wege-Authentifizierung aktivieren (TLS-Modus **Custom PFX with client authentication**), die Zwei-Wege-Authentifizierung in Kaspersky Endpoint Security aktivieren und der KUMA-Konsole sowie Kaspersky Endpoint Security ein PFX-Archiv hinzufügen.

So konfigurieren Sie eine vertrauenswürdige Verbindung zwischen KES und KUMA in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster den Punkt **KUMA-Integration** aus.
5. Aktivieren Sie das Kontrollkästchen **KUMA-Integration**.
6. Aktivieren Sie im Block **Einstellungen der Verbindung zu KUMA-Servern** das Kontrollkästchen **TLS-Verschlüsselung verwenden**.
7. Konfigurieren Sie die vertrauenswürdige Verbindung:
   a. Klicken Sie auf **Einstellungen der Verbindung zu KUMA-Servern**.
   b. Konfigurieren Sie die Serververbindung:
      - **Timeout (Sek)**. Die maximale Wartezeit auf eine Antwort vom KUMA-Server (standardmäßig beträgt der Wert 5 Sekunden). Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen KUMA-Server zu verbinden.
      - **TLS-Zertifikat des Servers**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem KUMA-Server. Sie können ein TLS-Zertifikat in der Konsole von Kaspersky Unified Monitoring and Analysis Platform abrufen (siehe Anleitung in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform).

        Um eine vertrauenswürdige Verbindung herzustellen, müssen Sie in der KUMA-Konsole den TLS-Modus **Enabled** auswählen.

- **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen KES und KUMA. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie in der KUMA-Konsole in den Konnektor-Einstellungen den TLS-Modus **Custom PFX with client authentication** auswählen (siehe Konnektor-Einstellungen in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). Anschließend müssen Sie ein Serverzertifikat herunterladen und ein Kennwort zum Schutz des Krypto-Containers festlegen.

  Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

c. Klicken Sie auf **OK**.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie eine vertrauenswürdige Verbindung zwischen KES und KUMA in der Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Konfiguration der integrierten Agenten** → **KUMA-Integration**.
5. Aktivieren Sie den Schalter **KUMA-Integration AKTIVIERT**.
6. Aktivieren Sie unter **Einstellungen der Serververbindung** den Schalter **TLS-Verschlüsselung verwenden**.
7. Konfigurieren Sie die vertrauenswürdige Verbindung:

   a. Klicken Sie auf **Verbindungseinstellungen**.

   b. Konfigurieren Sie die Serververbindung:

   - **Timeout (Sek.)**. Die maximale Wartezeit auf eine Antwort vom KUMA-Server (standardmäßig beträgt der Wert 5 Sekunden). Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen KUMA-Server zu verbinden.
   - **TLS-Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem KUMA-Server. Sie können ein TLS-Zertifikat in der Konsole von Kaspersky Unified Monitoring and Analysis Platform abrufen (siehe Anleitung in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform).

     Um eine vertrauenswürdige Verbindung herzustellen, müssen Sie in der KUMA-Konsole den TLS-Modus **Enabled** auswählen.

- **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen KES und KUMA. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie in der KUMA-Konsole in den Konnektor-Einstellungen den TLS-Modus **Custom PFX with client authentication** auswählen (siehe Konnektor-Einstellungen in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). Anschließend müssen Sie ein Serverzertifikat herunterladen und ein Kennwort zum Schutz des Krypto-Containers festlegen.

  Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.

c. Klicken Sie auf **OK**.

8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Senden von Telemetrie an den KUMA-Server aktivieren

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*.

So aktivieren Sie das Senden von Telemetrie an KUMA in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.
5. Klicken Sie im Block **Telemetrie-Einstellungen → Telemetrie für KUMA** auf **Einstellungen**.
6. Wählen Sie Ereignisprotokolle aus, die Sie als Ereignisquellen verwenden möchten: *Application*, *Security* oder *System*.

   Zusätzlich zu den Standardprotokollen können Sie auch Folgendes angeben: Protokoll eines Drittanbieter-Programms.
7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So aktivieren Sie das Senden von Telemetrie an KUMA in Web Console

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Allgemeine Einstellungen → Telemetrie-Einstellungen**.

5. Wählen Sie die Registerkarte **Telemetrie für KUMA** aus.

6. Wählen Sie Ereignisprotokolle aus, die Sie als Ereignisquellen verwenden möchten: *Application*, *Security* oder *System*.

   Zusätzlich zu den Standardprotokollen können Sie auch Folgendes angeben: Protokoll eines Drittanbieter-Programms.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Filterung von Ereignissen, die an KUMA gesendet werden sollen

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*. Um die Leistung zu verbessern und die Datenübertragung an den KUMA-Server zu optimieren, können Sie einzelne Ereignisse manuell zur Telemetrie hinzufügen oder davon ausschließen. Sie können beispielsweise Sysmon-Ereignisse ausschließen.

So erstellen Sie eine Liste mit Ereignissen, die an KUMA gesendet werden sollen (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.

3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Ausnahmen und Objekttypen** aus.

5. Klicken Sie im Block **Telemetrie-Einstellungen → Telemetrie für KUMA** auf **Einstellungen**.

6. Konfigurieren Sie im folgenden Fenster die Filter für Ereignisse, die an KUMA gesendet werden sollen.

   Sie können die Ereignisfilterung für die Standardprotokolle *Application*, *Security* und *System* konfigurieren oder manuell ein anderes Protokoll hinzufügen:

   a. Öffnen Sie die Protokolleigenschaften, oder klicken Sie auf **Hinzufügen** und geben Sie den Namen des Protokolls ein.

   b. Wählen Sie einen Modus für das Senden von Ereignissen aus:

   - **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.

c. Erstellen Sie Listen mit Ausschlussregeln oder Einschlussregeln für den entsprechenden Ereignisversandmodus.

Um Regeln hinzuzufügen, müssen Sie die Ereignis-ID aus dem Windows-Ereignisprotokoll angeben. Sie können mehrere Ereignis-IDs in einer Regel angeben. Um mehrere Ereignis-IDs anzugeben, verwenden Sie ein Komma (,) als Trennzeichen.

d. Aktivieren Sie bei Bedarf die Ereignisprotokollierung mithilfe des Kontrollkästchens neben dem Protokollnamen.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So erstellen Sie eine Liste mit Ereignissen, die an KUMA gesendet werden sollen (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für KUMA** aus.
6. Konfigurieren Sie im folgenden Fenster die Filter für Ereignisse, die an KUMA gesendet werden sollen.

   Sie können die Ereignisfilterung für die Standardprotokolle *Application*, *Security* und *System* konfigurieren oder manuell ein anderes Protokoll hinzufügen:

   a. Öffnen Sie die Protokolleigenschaften, oder klicken Sie auf **Hinzufügen** und geben Sie den Namen des Protokolls ein.

   b. Wählen Sie einen Modus für das Senden von Ereignissen aus:

   - **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.

   c. Erstellen Sie Listen mit Ausschlussregeln oder Einschlussregeln für den entsprechenden Ereignisversandmodus.

   Um Regeln hinzuzufügen, müssen Sie die Ereignis-ID aus dem Windows-Ereignisprotokoll angeben. Sie können mehrere Ereignis-IDs in einer Regel angeben. Um mehrere Ereignis-IDs anzugeben, verwenden Sie ein Komma (,) als Trennzeichen.

   d. Aktivieren Sie bei Bedarf die Ereignisprotokollierung mithilfe des Schalters neben dem Protokollnamen.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Filter für KUMA-Ereignisse exportieren und importieren

Sie können die Ausnahmeliste in eine json-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Ereignis-IDs hinzuzufügen. Sie können die Export-/Importfunktion auch verwenden, um ein Backup der Ereignisfilter anzulegen oder die Listen auf einen anderen Server zu migrieren.

Wenn zu viele Regeln verwendet werden, kann sich die Auslastung des KUMA-Servers erhöhen und die Computerleistung verringern. Es wird empfohlen, nur erforderlich Regeln hinzuzufügen.

So exportieren und importieren Sie Ereignisfilter (in der Verwaltungskonsole (MMC))

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.
3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
4. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen** → **Ausnahmen und Objekttypen** aus.
5. Klicken Sie im Block **Telemetrie-Einstellungen** → **Telemetrie für KUMA** auf **Einstellungen**.
6. So exportieren Sie die Ereignisfilter:
   a. Wählen Sie die Ereignisprotokolle mit Filtern aus, die Sie exportieren möchten.
   b. Klicken Sie auf die Schaltfläche → **Exportieren**.
   c. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.
   d. Speichern Sie die Datei.
      Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.
7. So importieren Sie Ereignisfilter:
   a. Klicken Sie auf die Schaltfläche → **Importieren**.
   b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.
   c. Öffnen Sie die Datei.
      Falls auf dem Computer bereits Ereignisfilterungsregeln vorhanden sind, ersetzt Kaspersky Endpoint Security während des Importvorgangs.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So exportieren und importieren Sie Ereignisfilter (in der Web Console)

1. Wählen Sie im Web Console-Hauptfenster die Registerkarte **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen** → **Telemetrie-Einstellungen**.
5. Wählen Sie die Registerkarte **Telemetrie für KUMA** aus.
6. So exportieren Sie die Ereignisfilter:

   a. Wählen Sie die Ereignisprotokolle mit Filtern aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche → **Exportieren**.

   c. Geben Sie im folgenden Fenster den Namen der json-Datei an, in die Sie die Ereignisfilter exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   d. Speichern Sie die Datei.

      Kaspersky Endpoint Security exportiert die Ereignisfilter in die json-Datei.
7. So importieren Sie Ereignisfilter:

   a. Klicken Sie auf die Schaltfläche → **Import**.

   b. Wählen Sie im folgenden Fenster die json-Datei aus, aus der Sie die Ereignisfilter importieren möchten.

   c. Öffnen Sie die Datei.

      Falls auf dem Computer bereits Ereignisfilterungsregeln vorhanden sind, ersetzt Kaspersky Endpoint Security während des Importvorgangs.
8. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

Sie können Ereignisfilter auch über die Befehlszeile exportieren oder importieren.

Leitfaden zur Migration von KSWS zu KES

Ab Version 11.8.0 unterstützt Kaspersky Endpoint Security für Windows die grundlegenden Funktionen der Lösung Kaspersky Security für Windows Server (KSWS). *Kaspersky Security für Windows Server* schützt Server, auf denen Microsoft Windows-Betriebssysteme ausgeführt werden, sowie Netzwerkspeicher vor Viren und anderen Sicherheitsrisiken, die Servern und Netzwerkspeichern beim Austausch von Dateien drohen. Ausführliche Informationen zur Funktionsweise der Lösung finden Sie in der Hilfe zu Kaspersky Security für Windows Server. Ab Kaspersky Endpoint Security 11.8.0 können Sie von Kaspersky Security für Windows Server zu Kaspersky Endpoint Security für Windows migrieren und haben damit eine einheitliche Lösung zum Schutz von Workstations und Servern.

Softwarevoraussetzungen

Bevor Sie mit der Migration von KSWS zu KES beginnen, stellen Sie sicher, dass Ihr Server die Hard- und Softwareanforderungen von Kaspersky Endpoint Security für Windows erfüllt. Die Listen der unterstützten Betriebssystemversionen sind für KES und KSWS unterschiedlich. Beispielsweise unterstützt KES keine Server, auf denen Windows Server 2003 ausgeführt wird.

Minimale Softwareanforderungen für die Migration von KSWS zu KES:

- Kaspersky Endpoint Security für Windows 12.0.
- Kaspersky Security 11.0.1 für Windows Server.

  Wenn Sie eine ältere Version von Kaspersky Security für Windows Server installiert haben, empfehlen wir Ihnen, das Programm auf die neueste Version upzugraden. Der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben unterstützt keine älteren Versionen von Kaspersky Security für Windows Server.
- Kaspersky Security Center 14.2

  Wenn Sie eine ältere Version von Kaspersky Security Center installiert haben, aktualisieren Sie diese auf 14.2 oder höher. In dieser Version von Kaspersky Security Center können Sie mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben Richtlinien in ein Profil migrieren, aber nicht in eine Richtlinie. In dieser Version von Kaspersky Security Center können Sie mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben auch eine breitere Palette von Richtlinieneinstellungen migrieren.
- Kaspersky Endpoint Agent 3.10.

  Wenn Sie eine ältere Version von Kaspersky Endpoint Agent installiert haben, empfehlen wir Ihnen, die App auf die neueste Version upzugraden. Kaspersky Endpoint Security unterstützt die Migration einer [KSWS KEA]-Konfiguration zu [KES+built-in agent] ab Kaspersky Endpoint Agent 3.10.

Empfehlungen für die Migration

Beachten Sie bei der Migration von KSWS zu KES die folgenden Empfehlungen:

- Planen Sie vorab einen passenden Zeitpunkt für die Migration von KSWS zu KES. Wählen Sie einen Zeitpunkt aus, zu dem die Server am wenigsten ausgelastet sind, z. B. am Wochenende.
- Aktivieren Sie nach der Migration nicht alle Programmkomponenten auf einmal. Aktivieren Sie beispielsweise zuerst nur die Komponente „Schutz vor bedrohlichen Dateien“, aktivieren Sie dann andere Schutzkomponenten, aktivieren Sie anschließend die Kontrollkomponenten und so weiter. Bei jedem Schritt müssen Sie überprüfen, ob das Programm ordnungsgemäß funktioniert, und Sie müssen die Leistung des Servers überwachen. Die Architektur von KES unterscheidet sich von KSWS, daher kann sich auch das Betriebssystem anders verhalten.
- Führen Sie die Migration Schritt für Schritt durch. Migrieren Sie zuerst einen einzelnen Server, dann mehrere Server und führen Sie anschließend die Migration auf allen Servern des Unternehmens durch.
- Migrieren Sie verschiedene Servertypen separat. Migrieren Sie beispielsweise zuerst Datenbankserver, dann Mailserver und so weiter.
- Bei der Migration auf Servern mit hoher Auslastung müssen spezielle Aspekte berücksichtigt werden.

Schritte der Migration

Die Migration von KSWS zu KES erfolgt halbautomatisch. Dies ist durch Unterschiede in der Programmarchitektur bedingt. Um die Richtlinieneinstellungen zu migrieren, müssen Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (den Migrations-Assistenten) ausführen. Nach der Migration der Richtlinieneinstellungen müssen Sie bestimmte Einstellungen manuell konfigurieren. Dies sind Einstellungen, die der Migrations-Assistent nicht automatisch migrieren kann (z. B. Einstellungen für den Kennwortschutz). Außerdem müssen Sie nach der Migration überprüfen, ob der Migrations-Assistent alle Einstellungen korrekt migriert hat.

Für die Migration von KSWS zu KES gilt folgende Reihenfolge:

1. **Migration von KSWS-Aufgaben und -Richtlinien**

   Nach der Migration der Richtlinien und Aufgaben müssen Sie zusätzliche Konfigurationsschritte ausführen. Außerdem müssen Sie sicherstellen, dass Kaspersky Endpoint Security nach der Migration von KSWS das erforderliche Sicherheitsniveau bietet.

   > Der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben für Kaspersky Security für Windows Server ist nur in der Verwaltungskonsole (MMC) verfügbar. Einstellungen für Richtlinien und Aufgaben können nicht über die Web Console oder Kaspersky Security Center Cloud Console migriert werden.

2. **Installation von Kaspersky Endpoint Security**

Sie können Kaspersky Endpoint Security wie folgt installieren:

- Installation von KES nach dem Entfernen von KSWS (empfohlen).

  Das Dienstprogramm kavremover unterstützt die Verwaltung von KSWS nicht.

- Installation von KES über KSWS.

3. Aktivieren von KES mit einem KSWS-Schlüssel

4. **Überprüfen, ob das Programm nach der Migration funktionsfähig ist**

   Überprüfen Sie nach der Migration von KSWS zu KES, ob das Programm ordnungsgemäß funktioniert. Überprüfen Sie den Status des Servers in der Konsole (erforderlicher Status: *OK*). Stellen Sie sicher, dass keine Fehler für das Programm gemeldet wurden. Überprüfen Sie außerdem den Zeitpunkt der letzten Verbindung zum Administrationsserver, den Zeitpunkt des letzten Datenbanken-Updates und den Status des Serverschutzes.

   Achten Sie insbesondere auf die Migration von Ausnahmelisten, vertrauenswürdigen Apps, vertrauenswürdigen Webadressen und Regeln der „Programmkontrolle“.

Entsprechung von KSWS- und KES-Komponenten

Bei der Migration von KSWS zu KES wird der Komponentensatz nur migriert, wenn das Programm lokal installiert wird.

Entsprechung der Komponenten von „Kaspersky Security für Windows Server“ und „Kaspersky Endpoint Security für Windows“

Komponente von „Kaspersky Security für Windows Server“	Komponente von „Kaspersky Endpoint Security für Windows“
Grundfunktionen	Anwendungskernel
Protokollanalyse	Protokollanalyse
Gerätekontrolle	Gerätekontrolle
Firewall-Verwaltung	*(nicht unterstützt)* Die Funktionen der KSWS-Firewall werden von der Firewall auf Systemebene ausgeführt. In KES gibt es eine eigene Komponente für die Firewall-Funktionalität. Nach der Migration können Sie die Kaspersky Endpoint Security-Firewall konfigurieren.
Überwachung der Datei-Integrität	Überwachung der Systemintegrität
Exploit-Prävention	Exploit-Prävention
Systemfachsymbol	*(nicht unterstützt)* Sie können die Benutzerinteraktion in den Einstellungen der Programmoberfläche konfigurieren.
Integration in Kaspersky Security Center	Administrationsagent-Connector
Endpoint Agent	*(nicht unterstützt)* In Kaspersky Endpoint Security 11.9.0 ist das Verteilungspaket für Kaspersky Endpoint Agent nicht mehr Teil des Verteilungskits für Kaspersky Endpoint Security. Sie müssen das Verteilungspaket für Kaspersky Endpoint Agent separat herunterladen.
Schutz vor Netzwerkbedrohungen	Schutz vor Netzwerkbedrohungen
Schutz vor Verschlüsselung	Verhaltensanalyse
Anti-Cryptor für NetApp	*(nicht unterstützt)*

Komponente von „Kaspersky Security für Windows Server“	Komponente von „Kaspersky Endpoint Security für Windows“
Schutz des Datenverkehrs	Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen Web-Kontrolle
Untersuchung auf Befehl	Anwendungskernel
Schutz von per ICAP-Protokoll verbundenen Netzwerkspeichern	*(nicht unterstützt)* Kaspersky Endpoint Security unterstützt keine Komponenten für den Schutz von netzgebundenen Speichern (NAS, Network Attached Storage). Wenn Sie diese Komponenten benötigen, können Sie Kaspersky Security für Windows Server weiterhin verwenden.
Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern	*(nicht unterstützt)* Kaspersky Endpoint Security unterstützt keine Komponenten für den Schutz von netzgebundenen Speichern (NAS, Network Attached Storage). Wenn Sie diese Komponenten benötigen, können Sie Kaspersky Security für Windows Server weiterhin verwenden.
Echtzeitschutz für Dateien	Schutz vor bedrohlichen Dateien
Skript-Untersuchung	*(nicht unterstützt)* Die „Skript-Untersuchung“ wird von anderen Komponenten übernommen, z. B. von „AMSI-Schutz“.
Verwendung von KSN	Kaspersky Security Network
Kontrolle des Programmstarts	Programmkontrolle
Leistungsindikatoren	*(nicht unterstützt)*

Entsprechung von KSWS- und KES-Einstellungen

Beim Migrieren von Richtlinien und Aufgaben wird KES den KSWS-Einstellungen entsprechend konfiguriert. Einstellungen von Programmkomponenten, die in KSWS nicht vorhanden sind, erhalten Standardwerte.

Programmeinstellungen

Skalierbarkeit, Benutzeroberfläche und Untersuchungseinstellungen

Programmeinstellungen werden in „Kaspersky Endpoint Security für Windows“ nicht unterstützt.

Programmeinstellungen

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Skalierbarkeitseinstellungen	*(wird nicht migriert)* Kaspersky Endpoint Security verwaltet alle Arbeitsprozesse.
Taskleistensymbol anzeigen	*(wird nicht migriert)* Auf einem Client-Computer sind standardmäßig das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an. Sie können die Benutzerinteraktion in den Einstellungen der Programmoberfläche konfigurieren.
Dateiattribute nach der Untersuchung wiederherstellen	*(wird nicht migriert)* Kaspersky Endpoint Security stellt die Dateiattribute nach der Untersuchung einer Datei automatisch wieder her.
CPU-Auslastung für die Thread-Untersuchung beschränken	*(wird nicht migriert)* Kaspersky Endpoint Security beschränkt die CPU-Auslastung bei der Untersuchung nicht. Sie können festlegen, dass die Aufgabe ausgeführt wird, wenn der Computer minimal ausgelastet ist.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Ordner für während der Untersuchung erstellte temporäre Dateien	*(wird nicht migriert)* Kaspersky Endpoint Security legt die temporären Dateien im Ordner `C:\Windows\Temp` ab.
Einstellungen des HSM-Systems	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt keine HSM-Systeme.

Sicherheit und Zuverlässigkeit

Die KSWS-Sicherheitseinstellungen werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitte **Programmeinstellungen** und **Benutzeroberfläche**.

Einstellungen für Programmsicherheit

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Programmprozesse vor externen Bedrohungen schützen	**Selbstschutz aktivieren** (Unterabschnitt **Programmeinstellungen**)
Kennwortschutz verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security hat eine integrierte Kennwortschutz-Funktion (siehe Unterabschnitt **Benutzeroberfläche**).
Wiederherstellen von Aufgaben ausführen	*(wird nicht migriert)* Kaspersky Endpoint Security stellt nur die Aufgaben *Schadsoftware-Untersuchung* automatisch wieder her. Andere Aufgaben werden von Kaspersky Endpoint Security nach einem Zeitplan ausgeführt.
Aufgaben zur Untersuchung nach Zeitplan nicht starten	**Geplante Aufgaben bei Akkubetrieb aufschieben** (Unterabschnitt **Programmeinstellungen**)
Laufende Untersuchungsaufgaben anhalten	*(wird nicht migriert)* Wenn der Computer von einer unterbrechungsfreien Stromversorgung versorgt wird, hält Kaspersky Endpoint Security bereits laufende Untersuchungsaufgaben nicht an.

Verbindungseinstellungen

Die Einstellungen für die Interaktion mit dem Administrationsserver werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitte **Netzwerkeinstellungen** und **Programmeinstellungen**.

Einstellungen für die Interaktion mit dem Administrationsserver

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Proxyserver-Einstellungen	**Proxyserver-Einstellungen** (Unterabschnitt **Netzwerkeinstellungen**)
Für lokale Adressen keinen Proxyserver verwenden	**Einen Proxyserver für lokale Adressen umgehen** (Unterabschnitt **Netzwerkeinstellungen**)
Einstellungen für die Authentifizierung auf dem Proxyserver	**Proxyserver-Authentifizierung verwenden** (Unterabschnitt **Netzwerkeinstellungen**) Das Kennwort für die Proxyserver-Authentifizierung wird nicht migriert. Nachdem eine Richtlinie migriert wurde, muss das Kennwort manuell eingegeben werden.
Kaspersky Security Center als Proxyserver für die Programmaktivierung verwenden	**Kaspersky Security Center als Proxyserver für die Aktivierung verwenden** (Unterabschnitt **Programmeinstellungen**)

Start von lokalen Systemaufgaben

Kaspersky Endpoint Security ignoriert die Einstellungen für laufende lokale Systemaufgaben von Kaspersky Security für Windows Server. Die Verwendung lokaler KES-Aufgaben können Sie unter **Lokale Aufgaben**, **Aufgabenverwaltung** konfigurieren. Außerdem können Sie einen Zeitplan für den Start der Aufgaben *Schadsoftware-Untersuchung* und *Update der Datenbanken und Programm-Module* in den Eigenschaften der jeweiligen Aufgaben konfigurieren.

Zusätzlich

Vertrauenswürdige Zone

Die KSWS-Einstellungen für die vertrauenswürdige Zone werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitt **Ausnahmen**.

Einstellungen der vertrauenswürdigen Zone

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Zu untersuchendes Objekt (Ausnahmen)	**Untersuchungsausnahmen** (Untersuchungsausnahmen) Die von KSWS und KES verwendeten Methoden zur Auswahl von Objekten unterscheiden sich. Bei der Migration unterstützt KES Ausnahmen, die als einzelne Dateien oder Pfade für Dateien bzw. Ordner definiert sind. Ausnahmen, die KSWS als vordefinierten Bereich oder als Skript-URL konfiguriert hat, werden nicht migriert. Solche Ausnahmen müssen Sie nach der Migration manuell hinzufügen. Ausnahmen in Form vordefinierter Bereiche müssen in den Einstellungen der Aufgabe *Schadsoftware-Untersuchung* konfiguriert werden. Ausnahmen in Form von Skript-Webadressen müssen zu den vertrauenswürdigen Webadressen für den „Schutz vor Web-Bedrohungen“ hinzugefügt werden.
Auch für Unterordner übernehmen (Ausnahmen)	**Unterordner einschließen** (Untersuchungsausnahmen)
Zu erkennende Objekte (Ausnahmen)	**Typ des erkannten Objekts** (Untersuchungsausnahmen)
Gültigkeitsbereich der Ausnahme (Ausnahmen)	**Schutzkomponenten** (Untersuchungsausnahmen) Wenn in KSWS mindestens eine Komponente ausgewählt ist, wendet KES die Ausnahmen auf alle Programmkomponenten an.
Kommentar (Ausnahmen)	**Kommentar** (Untersuchungsausnahmen)
Vertrauenswürdiger Prozess (Vertrauenswürdiger Prozess)	**Vertrauenswürdige Programme** Die Auswahlmethoden für vertrauenswürdige Prozesse bzw. Programme unterscheiden sich in KSWS und KES. Bei der Migration unterstützt KES vertrauenswürdige Programme, die als Pfad der ausführbaren Datei oder als Maske konfiguriert sind. Vertrauenswürdige Prozesse, die KSWS als Datei-Hash konfiguriert hat, werden nicht migriert. Solche vertrauenswürdigen Prozesse müssen Sie nach der Migration manuell hinzufügen.
Datei-Aktivität beim Erstellen eines Backups nicht untersuchen (Vertrauenswürdiger Prozess)	**Programmaktivität nicht überwachen** (Vertrauenswürdige Programme)

Untersuchung von Wechseldatenträgern

Einstellungen für die Untersuchung von Wechseldatenträgern werden migriert in den Abschnitt **Lokale Aufgaben**, Unterabschnitt **Untersuchung von Wechseldatenträgern**.

Einstellungen für die Untersuchung von Wechseldatenträgern

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Wechseldatenträger beim Anschließen über USB untersuchen	**Aktion bei Verbindung eines Wechseldatenträgers**
Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)	**Maximale Größe des Wechseldatenträgers**

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Untersuchung mit folgender Sicherheitsstufe starten: • **Maximale Sicherheit** • **Empfohlen** • **Maximale Leistung**	**Aktion bei Verbindung eines Wechseldatenträgers**: • **Maximaler Schutz**. • **Empfohlen**. Die KSWS-Sicherheitsstufen entsprechen den folgenden KES-Untersuchungsmodi: • Maximaler Schutz – Maximaler Schutz • Empfohlen – Empfohlen • Maximale Leistung – Empfohlen

Benutzerberechtigungen für die Programmverwaltung

Die Zuweisung von Benutzerzugriffsberechtigungen für die Programmverwaltung und die Verwaltung von Programmdiensten werden von Kaspersky Endpoint Security nicht unterstützt. Die Zugriffseinstellungen für Benutzer und Benutzergruppen für die Verwaltung des Programms können Sie in Kaspersky Security Center konfigurieren.

Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service

Die Zuweisung von Benutzerzugriffsberechtigungen für die Programmverwaltung und die Verwaltung von Programmdiensten werden von Kaspersky Endpoint Security nicht unterstützt. Die Zugriffseinstellungen für Benutzer und Benutzergruppen für die Verwaltung des Programms können Sie in Kaspersky Security Center konfigurieren.

Speicher

KSWS-Speichereinstellungen werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitt **Berichte und Speicher**, und in den Abschnitt **Basisschutz**, Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

Speichereinstellungen

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Backup-Ordner	*(wird nicht migriert)* Kaspersky Endpoint Security speichert Backup-Kopien von Dateien im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximale Größe des Backups (MB)	**Maximale Größe des Backups n MB** (**Allgemeine Einstellungen** → Abschnitt **Berichte und Speicher**)
Grenzwert für verfügbaren Speicherplatz (MB)	*(wird nicht migriert)* Kaspersky Endpoint Security protokolliert das Ereignis *Der Quarantäne-Speicher ist fast voll*, wenn die 50%-Schwelle erreicht wird.
Ordner für die Wiederherstellung von Objekten	*(wird nicht migriert)* Kaspersky Endpoint Security stellt Dateien im ursprünglichen Ordner wieder her.
Quarantäneordner	*(wird nicht migriert)* Kaspersky Endpoint Security speichert Backup-Kopien von Dateien im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.
Maximale Größe der Quarantäne (MB)	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet das Backup, um möglicherweise infizierte Objekte zu speichern. Bei der Migration berücksichtigt Kaspersky Endpoint Security die Quarantäne-Einstellungen nicht.
Grenzwert für verfügbaren Speicherplatz (MB)	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet das Backup, um möglicherweise infizierte Objekte zu speichern. Bei der Migration berücksichtigt Kaspersky Endpoint Security die Quarantäne-Einstellungen nicht.
Ordner für die Wiederherstellung von Objekten	*(wird nicht migriert)* Kaspersky Endpoint Security stellt Dateien im ursprünglichen Ordner wieder her.
Automatisch entsperren nach n	**Angreifende Geräte sperren für n Min** (**Basisschutz** → Abschnitt **Schutz vor Netzwerkbedrohungen**)

Echtzeitschutz für Server

Echtzeitschutz für Dateien

KSWS-Einstellungen für den Echtzeitschutz von Dateien werden migriert in den Abschnitt **Basisschutz**, Unterabschnitt **Schutz vor bedrohlichen Dateien**.

Einstellungen für den Echtzeitschutz für Dateien

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Schutzmodus für Objekte: • **Intelligent** • **Beim Ausführen** • **Bei Zugriff** • **Bei Zugriff und Veränderungen**	**Untersuchungsmodus**: • **Intelligenter Modus**. • **Bei Ausführung**. • **Bei Zugriff**. • **Bei Zugriff und Veränderungen**.
Tiefere Analyse startender Prozesse	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt nur einen Analysemodus, und zwar den Modus Optimal.
Heuristische Analyse: • **Oberflächlich** • **Mittel** • **Tief**	**Heuristische Analyse**: • **Oberflächlich**. • **Mittel**. • **Tief**.
Vertrauenswürdige Zone anwenden	*(wird nicht migriert)* Kaspersky Endpoint Security wendet die vertrauenswürdige Zone auf alle Komponenten an. Ausnahmen können Sie in den Einstellungen der vertrauenswürdigen Zone konfigurieren.
KSN zum Schutz verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet KSN für alle Programmkomponenten.
Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen	*(wird nicht migriert)* Standardmäßig blockiert Kaspersky Endpoint Security den Zugriff auf gemeinsam genutzte Netzwerkressourcen für Hosts, die bösartige Aktivitäten zeigen.
Untersuchung wichtiger Bereiche starten, wenn eine aktive Infektion erkannt wird	*(wird nicht migriert)* Kaspersky Endpoint Security startet die Aufgabe zur Untersuchung wichtiger Bereiche nicht, wenn eine aktive Infektion erkannt wird.
Kaspersky Sandbox zum Schutz verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security sendet Objekte standardmäßig zur Untersuchung an „Kaspersky Sandbox“.
Schutzbereich	**Schutzbereich**
Zeitplan-Einstellungen	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet einen eigenen Zeitplan zum Anhalten des „Schutzes vor bedrohlichen Dateien“.

Verwendung von KSN

KSWS-Einstellungen für Kaspersky Security Network werden migriert in den Abschnitt **Erweiterter Schutz**, Unterabschnitt **Kaspersky Security Network**.

Einstellungen für „Kaspersky Security Network“

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Ich bestätige, dass ich die Bedingungen zur Teilnahme an KSN vollständig gelesen habe, und sie verstehe und akzeptiere.	**Erklärung zu Kaspersky Security Network** In folgenden Fällen fordert Kaspersky Endpoint Security auf, die Erklärung zu Kaspersky Security Network zu akzeptieren: Wenn das Programm installiert, eine neue Richtlinie erstellt oder die Nutzung von Kaspersky Security Network aktiviert wird.
Daten über untersuchte Dateien senden	*(wird nicht migriert)* Kaspersky Endpoint Security sendet automatisch Daten über untersuchte Dateien, wenn KSN aktiviert ist.
Daten über angeforderte URLs senden	*(wird nicht migriert)* Kaspersky Endpoint Security sendet automatisch Daten über angeforderte URLs, wenn KSN aktiviert ist.
Statistiken an Kaspersky Security Network senden	**Erweiterten KSN-Modus aktivieren**
Bedingungen der Erklärung zu Kaspersky Managed Protection akzeptieren	*(wird nicht migriert)* Der KMP-Dienst ist nicht in Kaspersky Endpoint Security enthalten.
Aktion für Objekte, die laut KSN nicht vertrauenswürdig sind	*(wird nicht migriert)* Die Aktion beim Fund einer Bedrohung können Sie in den Einstellungen der Schutzkomponente und in den Einstellungen der Untersuchungsaufgabe konfigurieren.
Keine Prüfsumme für den Versand an KSN berechnen für Dateien, die größer sind als n MB	*(wird nicht migriert)* Die Beschränkungen für die Untersuchung großer Dateien können Sie in den Einstellungen der Schutzkomponente und in den Einstellungen der Untersuchungsaufgabe konfigurieren.
Kaspersky Security Center als KSN-Proxyserver verwenden	**Administrationsserver als KSN-Proxyserver verwenden**
Zeitplan-Einstellungen	*(wird nicht migriert)* Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

Schutz des Datenverkehrs

KSWS-Einstellungen für den Schutz des Datenverkehrs werden migriert in den Abschnitt **Basisschutz**, Unterabschnitte **Schutz vor Web-Bedrohungen** und **Schutz vor E-Mail-Bedrohungen**, Abschnitt **Sicherheitskontrolle**, Unterabschnitt **Web-Kontrolle**, Abschnitt **Allgemeine Einstellungen**, Unterabschnitt **Netzwerkeinstellungen**.

Einstellungen für den Schutz des Datenverkehrs

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
URL-basierte Regeln übernehmen	**Web-Kontrolle** (Unterabschnitt **Web-Kontrolle**) URL-basierte Regeln werden in separate Regeln in Kaspersky Endpoint Security migriert.
Zertifikatsbasierte Regeln übernehmen	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt keine zertifikatsbasierten Regeln.
Regeln zur Überwachung von Kategorien des Web-Datenverkehrs anwenden	**Web-Kontrolle** (Unterabschnitt **Web-Kontrolle**) Die Sperr-Regeln für die Kontrolle von Kategorien des Web-Datenverkehrs werden in Kaspersky Endpoint Security in eine einzige Sperr-Regel migriert. Kaspersky Endpoint Security ignoriert Erlaubnisregeln für die Kategoriekontrolle. Die Entsprechung der KSWS- und KES-Kategorien ist unten aufgeführt.
Zugriff erlauben, wenn die Webseite nicht kategorisiert werden kann	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt den Zugriff, wenn die Webseite nicht kategorisiert werden kann.
Zugriff auf legitime Webressourcen erlauben, die zur Schädigung eines geschützten Geräts verwendet werden können	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt den Zugriff auf legitime Webressourcen, mit denen das geschützte Gerät beschädigt werden kann.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Zugriff auf legitime Werbung erlauben	*(wird nicht migriert)* Den Zugriff auf legitime Werbung können Sie mithilfe der Webressourcen-Kategorie *Banner* in den Einstellungen der „Web-Kontrolle“ verwalten.
Ausführungsmodus: • **Treiber-Interceptor** • **Redirector** • **Externer Proxyserver**	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt nur den Treiber-Interceptor-Modus.
Einstellungen für die Verbindung mit dem ICAP-Dienst	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt den Schutz von per ICAP verbundenen Netzwerkspeichern nicht.
Sichere Verbindungen über das HTTPS-Protokoll überprüfen	Modus **Verschlüsselte Verbindungen untersuchen** / **Verschlüsselte Verbindungen immer untersuchen** (Unterabschnitt **Netzwerkeinstellungen**)
TLS-Protokollversion verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security untersucht den verschlüsselten Netzwerkverkehr, der über die folgenden Protokolle übertragen wird: • SSL 3.0; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. SSL 2.0-Verbindungen können zusätzlich in Einstellungen für die Untersuchung verschlüsselter Verbindungen blockiert werden.
Webservern mit falschem Zertifikat nicht vertrauen	**Adresse** (Unterabschnitt **Netzwerkeinstellungen**)
Ports abfangen (Interception-Bereich)	**Überwachte Ports** (Unterabschnitt **Netzwerkeinstellungen**) Während der Migration deaktiviert KES die Kontrollkästchen **Alle Ports für Programme überwachen, die auf der von Kaspersky empfohlenen Liste stehen** und **Alle Ports für die angegebenen Programme überwachen**.
Ports ausschließen (Interception-Bereich)	*(wird nicht migriert)*
IP-Adressen ausschließen (Interception-Bereich)	**Vertrauenswürdige Adressen konfigurieren** (Unterabschnitt **Netzwerkeinstellungen**)
Prozesse ausschließen (Interception-Bereich)	**Vertrauenswürdige Programme konfigurieren** (Unterabschnitt **Netzwerkeinstellungen**) Während der Migration konfiguriert KES die folgenden Einstellungen für das vertrauenswürdige Programm: • Das Kontrollkästchen **Netzwerkverkehr nicht untersuchen** ist aktiviert. KES scannt den Netzwerkverkehr nicht auf Remote-IP-Adressen und Ports. • Die anderen Kontrollkästchen in den Einstellungen für vertrauenswürdige Programme sind deaktiviert.
Sicherheitsport	*(wird nicht migriert)*
Weblinks mittels Datenbank für bösartige Links untersuchen	**Webadresse mit der Datenbank für bösartige Webadressen untersuchen** (Unterabschnitt **Schutz vor Web-Bedrohungen**)
Websites mittels Anti-Phishing-Datenbank untersuchen	**Webadresse mit der Datenbank für Phishing-Webadressen untersuchen** (Unterabschnitt **Schutz vor Web-Bedrohungen**)
KSN zum Schutz verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet KSN für alle Programmkomponenten.
Vertrauenswürdige Zone verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security wendet die vertrauenswürdige Zone auf alle Komponenten an. Ausnahmen können Sie in den Einstellungen der vertrauenswürdigen Zone konfigurieren.
Heuristische Analyse verwenden	**Heuristische Analyse verwenden** (Unterabschnitte **Schutz vor Web-Bedrohungen** und **Schutz vor E-Mail-Bedrohungen**)
Sicherheitsstufe	*(wird nicht migriert)* Kaspersky Endpoint Security verfügt über eigene Sicherheitsstufen für die Komponenten „Schutz vor Web-Bedrohungen“ und „Schutz vor E-Mail-Bedrohungen“. Kaspersky Endpoint Security legt standardmäßig die empfohlene Sicherheitsstufe fest.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Schutz vor E-Mail-Bedrohungen aktivieren	**Schutz vor E-Mail-Bedrohungen** (Unterabschnitt **Schutz vor E-Mail-Bedrohungen**) **Erweiterung für Microsoft Outlook verbinden** **Nur eingehende Nachrichten** (Schutzbereich) **Beim Empfang untersuchen** (E-Mail-Schutz)
Zeitplan-Einstellungen	*(wird nicht migriert)* Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

Exploit-Prävention

Die KSWS-Einstellungen für die „Exploit-Prävention“ werden migriert in den Abschnitt **Erweiterter Schutz**, Unterabschnitt **Exploit-Prävention**.

Einstellungen zur Exploit-Prävention

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Exploit von Prozessen mit Schwachstellen verhindern: • **Bei Exploit beenden** • **Nur informieren**	**Wenn ein Exploit erkannt wird**: • **Verbieten**. • **Informieren**.
Mittels Terminaldienst über missbräuchlich verwendete Prozesse benachrichtigen	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt keine Terminaldienste.
Exploit von Prozessen mit Schwachstellen auch verhindern, wenn Kaspersky Security Service deaktiviert ist	*(wird nicht migriert)* Kaspersky Endpoint Security verhindert permanent Angriffe auf anfällige Prozesse.
Geschützte Prozesse	**Schutz für den Arbeitsspeicher von Systemprozessen aktivieren** Kaspersky Endpoint Security unterstützt die Auswahl geschützter Prozesse nicht. Sie können nur den Speicherschutz für Systemprozesse aktivieren.
Verfahren zur Exploit-Prävention: • **Alle verfügbaren Methoden zur Exploit-Prävention anwenden** • **Folgende Verfahren zur Exploit-Prävention anwenden**	*(wird nicht migriert)* Kaspersky Endpoint Security wendet alle verfügbaren Methoden für die Exploit-Prävention an.

Schutz vor Netzwerkbedrohungen

Die KSWS-Einstellungen für den „Schutz vor Netzwerkbedrohungen“ werden migriert in den Abschnitt **Basisschutz**, Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

Einstellungen für den „Schutz vor Netzwerkbedrohungen“

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Ausführungsmodus: • **Pass-through** • **Über Netzwerkangriffe nur informieren** • **Verbindungen bei erkanntem Angriff blockieren**	**Schutz vor Netzwerkbedrohungen** Wenn der **Pass-Through**-Modus ausgewählt wurde, ist der „Schutz vor Netzwerkbedrohungen“ deaktiviert. Wenn der Modus **Über Netzwerkangriffe nur informieren** oder der Modus **Verbindungen bei erkanntem Angriff blockieren** ausgewählt wurde, ist der „Schutz vor Netzwerkbedrohungen“ aktiviert. Kaspersky Endpoint Security funktioniert immer im Modus **Verbindungen blockieren, wenn ein Angriff erkannt wird**.
Datenverkehrsanalyse nicht stoppen, wenn die Aufgabe nicht ausgeführt wird	*(wird nicht migriert)* Kaspersky Endpoint Security analysiert den Datenverkehr permanent, wenn die Komponente aktiviert ist.
Ausgeschlossene IP-Adressen nicht kontrollieren	**Ausnahmen**
Zeitplan-Einstellungen	*(wird nicht migriert)* Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

Skript-Untersuchung

Kaspersky Endpoint Security unterstützt die Komponente „Skript-Untersuchung“ nicht. Die „Skript-Untersuchung“ wird von anderen Komponenten übernommen, z. B. von „AMSI-Schutz“.

Website-Kategorien

Kaspersky Endpoint Security unterstützt nicht alle Kategorien von „Kaspersky Security für Windows Server“. Kategorien, die in Kaspersky Endpoint Security nicht vorhanden sind, werden nicht migriert. Darum werden Klassifizierungsregeln für Webressourcen mit nicht unterstützten Kategorien nicht migriert.

Website-Kategorien

Kategorien von „Kaspersky Security für Windows Server“	Kategorien von „Kaspersky Endpoint Security für Windows“
Kriegsspiele	Videospiele
Abtreibungen	*(wird nicht migriert)*
Lotterien (erweitert)	Glücksspiel, Lotterien, Wetten
Alkohol	Alkohol, Tabak, Betäubungsmittel
Anonyme Proxyserver	Anonyme Proxyserver
Werbung für Diäten und Gewichtsverlust	*(wird nicht migriert)*
Vermietungen für Immobilien	*(wird nicht migriert)*
Audio, Video und Software	Software, Audio, Video
Banken	Banken
Blogs	Blogs
Militär	Waffen, Sprengstoff, militärische Inhalte
Für Kinder	*(wird nicht migriert)*
Diskriminierung	Gewalt, Intoleranz
Familie und Zuhause	*(wird nicht migriert)*
Hosting und Domänendienste	Kommunikation im Internet
Tiere und Haustiere	*(wird nicht migriert)*
Recht und Politik	Verboten gemäß den regionalen Gesetzen
Unterliegt Einschränkungen durch Roskomnadzor (Russland)	Verboten gemäß den Gesetzen der Russischen Föderation
Unterliegt Einschränkungen durch das föderale Gesetz 436 (Russland)	Verboten gemäß den Gesetzen der Russischen Föderation
Unterliegt Einschränkungen durch russische Gesetzgebung	Verboten gemäß den Gesetzen der Russischen Föderation
Unterliegt Einschränkungen durch globale Gesetzgebung	Verboten gemäß den regionalen Gesetzen
Partnersuche für Erwachsene	Inhalte für Erwachsene
Internetdienstleistungen	*(wird nicht migriert)*
Sexshops	Inhalte für Erwachsene
Informationstechnologie	*(wird nicht migriert)*
Casinos, Kartenspiele	Glücksspiel, Lotterien, Wetten
Bücher und Literatur	*(wird nicht migriert)*
Computerspiele	Videospiele
Gesundheit und Schönheit	*(wird nicht migriert)*
Kultur und Gesellschaft	*(wird nicht migriert)*
LGBT	Inhalte für Erwachsene
Lotterien	Glücksspiel, Lotterien, Wetten
Medizin	*(wird nicht migriert)*

Kategorien von „Kaspersky Security für Windows Server“	Kategorien von „Kaspersky Endpoint Security für Windows“
Mode	*(wird nicht migriert)*
Musik	*(wird nicht migriert)*
Betäubungsmittel	Alkohol, Tabak, Betäubungsmittel
Gewalt	Gewalt, Intoleranz
Unmut	*(wird nicht migriert)*
Illegale Drogen	Alkohol, Tabak, Betäubungsmittel
Hass und Diskriminierung	Gewalt, Intoleranz
Obszönes Vokabular	Obszönität
Dessous	Inhalte für Erwachsene
News	Nachrichtenportale
Nudismus	Inhalte für Erwachsene
Bildung	*(wird nicht migriert)*
Online-Shopping	Online-Shops
Alle Kommunikationsmittel	Kommunikation im Internet
Zahlung mit Kreditkarten	Zahlungssysteme
Online-Shopping (eigenes Zahlungssystem)	Online-Shops
Online-Enzyklopädien	*(wird nicht migriert)*
Online-Banking	Banken
Waffen	Waffen, Sprengstoff, militärische Inhalte
Jagd und Fischerei	*(wird nicht migriert)*
Zahlungssysteme	Zahlungssysteme
Karriere-Netzwerk	Karriere-Netzwerk
Suchmaschinen	*(wird nicht migriert)*
Polizeibeschlüsse (JP)	Verboten gemäß der japanischen Polizei
Laut KPSN vertrauenswürdig	*(wird nicht migriert)*
Laut KPSN nicht vertrauenswürdig	*(wird nicht migriert)*
Pornografie	Inhalte für Erwachsene
Medien-Hosting und Streaming	Nachrichtenportale
Webmail	Web-E-Mail
Reisen	*(wird nicht migriert)*
TV und Radio	Nachrichtenportale
Teaser und Werbedienste	Banner
Religion	Konfessionen, religiöse Vereinigungen
Restaurants, Cafés und Essen	*(wird nicht migriert)*
Partnerbörsen	Partnerbörsen
Sexualerziehung	Inhalte für Erwachsene
Soziale Netzwerke	Soziale Netzwerke
Sport	*(wird nicht migriert)*
Wetten	Glücksspiel, Lotterien, Wetten
Suizid	Gewalt, Intoleranz
Tabak	Alkohol, Tabak, Betäubungsmittel

Kategorien von „Kaspersky Security für Windows Server“	Kategorien von „Kaspersky Endpoint Security für Windows“
Torrents	Torrents
Aufgenommen in die Föderale Liste der Extremisten (Russland)	Verboten gemäß den Gesetzen der Russischen Föderation
Filehosting-Anbieter	Filehosting-Anbieter
Pharmazie	*(wird nicht migriert)*
Hobby und Unterhaltung	*(wird nicht migriert)*
Chats und Foren	Chats, Foren, IM
Seiten von Schulen und Universitäten	*(wird nicht migriert)*
Astrologie und Esoterik	*(wird nicht migriert)*
Extremismus und Rassismus	Gewalt, Intoleranz
E-Commerce	Online-Shops
Erotik	Inhalte für Erwachsene
Humor	*(wird nicht migriert)*

Überwachung der Desktop-Aktivitäten

Kontrolle des Programmstarts

Die KSWS-Einstellungen für die „Programmkontrolle“ werden migriert in den Abschnitt **Sicherheitskontrolle**, Unterabschnitt **Programmkontrolle**.

Einstellungen der Kontrolle des Programmstarts

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Ausführungsmodus: • **Nur Statistik** • **Aktiv**	**Aktion** (Programmkontrolle): • **Regeln testen**. • **Regeln anwenden**.
Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten	*(wird nicht migriert)* Kaspersky Endpoint Security untersucht das Programm bei jedem Startversuch.
Den Start von Befehlsinterpretern verbieten, wenn kein ausführbarer Befehl vorhanden ist	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt die Ausführung von Befehlsinterpretern, wenn sie nicht von der „Programmkontrolle“ verboten sind.
Regeln	**Regeln der Programmkontrolle** *(mit Einschränkungen unterstützt)* Kaspersky Endpoint Security 11.11.0 führt die Unterstützung für die Migration von Regeln für die Kontrolle des Programmstarts ein. Die Migrationsfunktion für die Regel zur Kontrolle des Programmstarts weist einige Einschränkungen auf. Standardmäßig enthält die KSWS-Kontrolle des Programmstarts zwei Regeln: • **Start von Skripten und MSI-Paketen, deren Zertifikate im OS als vertrauenswürdig eingestuft sind, erlauben** • **Ausführbare Datei durch vom Betriebssystem vertrauenswürdiges Zertifikat zulassen** Wenn mindestens eine KSWS-Regel den Typ **Erlauben** hat, erstellt KES während der Migration eine neue Erlaubnisregel, **Programme mit vertrauenswürdigen Stammzertifikaten**. Das heißt, die KES Programmkontrolle verwendet eine einzige Regel, um die Ausführung vertrauenswürdiger Skripts, MSI-Pakete und ausführbarer Dateien zuzulassen. Wenn beide Quell-KSWS-Regeln den Typ **Verbieten** haben, fügt KES keine Regeln für die Verwaltung von Programmen mit vertrauenswürdigen Stammzertifikaten hinzu.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Regeln für ausführbare Dateien verwenden	*(wird nicht migriert)* Der Anwendungsbereich der Regel kann nicht in den KES Programmkontroll-Einstellungen konfiguriert werden. Die KES Programmkontrolle wendet Regeln auf alle Dateitypen an: ausführbare Dateien, Skripte und MSI-Pakete. Wenn alle Dateitypen im Anwendungsbereich der Regel in KSWS enthalten sind, übernimmt KES während der Migration die KSWS-Regeln. Wenn ein Dateityp aus dem Anwendungsbereich der Regelanwendung in KSWS ausgeschlossen ist, übernimmt KES während der Migration auch die KSWS-Regeln, aber **Regeln testen** ist als Aktion zur Programmkontrolle ausgewählt.
Laden von DLL-Modulen überwachen	**Laden von DLL-Modulen überwachen (führt zu erheblich erhöhter Systemauslastung)**
Regeln für Skripte und MSI-Pakete verwenden	*(wird nicht migriert)* Der Anwendungsbereich der Regel kann nicht in den KES Programmkontroll-Einstellungen konfiguriert werden. Die KES Programmkontrolle wendet Regeln auf alle Dateitypen an: ausführbare Dateien, Skripte und MSI-Pakete. Wenn alle Dateitypen im Anwendungsbereich der Regel in KSWS enthalten sind, übernimmt KES während der Migration die KSWS-Regeln. Wenn ein Dateityp aus dem Anwendungsbereich der Regel in KSWS ausgeschlossen ist, übernimmt KES während der Migration die KSWS-Regeln, aber **Regeln testen** ist als Aktion zur Programmkontrolle ausgewählt.
Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten	*(wird nicht migriert)* Kaspersky Endpoint Security berücksichtigt die Reputation von Programmen nicht, sondern erlaubt oder verweigert die Ausführung von Programmen gemäß den Regeln.
Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben	Während der Migration fügt KES eine neue Erlaubnisregel hinzu. Die KL-Kategorie **Andere Programme\Programme, die laut KSN-Reputation vertrauenswürdig sind** ist als Auslösebedingung der Regel angegeben.
Benutzer und / oder Benutzergruppen, denen der Start von laut KSN vertrauenswürdigen Programmen erlaubt ist	**Benutzer und deren Rechte** in einer Erlaubnisregel der Programmkontrolle, die die KL-Kategorie **Andere Programme\Programme, die laut KSN-Reputation vertrauenswürdig sind** enthält.
Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben	Die Softwareverteilungssteuerung in KSWS und KES funktioniert unterschiedlich. Während der Migration fügt KES neue Erlaubnisregeln für Programme hinzu, für die die automatische Softwareverteilung zugelassen ist. Als regelauslösende Bedingung wird der Datei-Hash angegeben.
Verteilung von Programmen mittels Windows Installer immer erlauben	Die Softwareverteilungssteuerung in KSWS und KES funktioniert unterschiedlich. Während der Migration fügt KES neue Erlaubnisregeln für Programme hinzu, für die die automatische Softwareverteilung zugelassen ist (**Erlaubte Programme und Pakete für die Software-Verteilung**). Als regelauslösende Bedingung wird der Datei-Hash angegeben. In den Kontoeigenschaften ist das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen** aktiviert.
Verteilung von Programmen mittels SCCM unter Verwendung des Background Intelligent Transfer Service (BITS) immer erlauben	*(wird nicht migriert)*
Liste der erlaubten Programme und Installationspakete	Die Softwareverteilungssteuerung in KSWS und KES funktioniert unterschiedlich. Während der Migration fügt KES neue Erlaubnisregeln für Programme hinzu, für die die automatische Softwareverteilung zugelassen ist. Als regelauslösende Bedingung wird der Datei-Hash angegeben. In den Kontoeigenschaften ist das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen** aktiviert.
Zeitplan-Einstellungen	*(wird nicht migriert)* Wenn in den KSWS-Einstellungen ein Zeitplan für die Komponente konfiguriert ist, wird die Komponente „Programmkontrolle“ bei der Migration aktiviert. Wenn in den KSWS-Einstellungen kein Zeitplan für die Komponente konfiguriert ist, wird die Komponente „Programmkontrolle“ bei der Migration deaktiviert. Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

Gerätekontrolle

Die KSWS-Einstellungen für die „Gerätekontrolle“ werden migriert in den Abschnitt **Sicherheitskontrolle**, Unterabschnitt **Gerätekontrolle**.

Einstellungen der „Gerätekontrolle“

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Ausführungsmodus: • **Aktiv** • **Nur Statistik**	*(wird nicht migriert)* Die „Programmkontrolle“ läuft im Modus *Aktiv*. Das Audit stellt kontinuierlich eine Verbindungsstatistik der Geräte bereit.
Die Verwendung aller externen Geräte erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird	*(wird nicht migriert)* Die „Gerätekontrolle“ ist immer aktiviert, während Kaspersky Endpoint Security ausgeführt wird.
Regeln für die Gerätekontrolle	**Vertrauenswürdige Geräte** Während der Migration ignoriert Kaspersky Endpoint Security deaktivierte KSWS-Regeln.
Zeitplan-Einstellungen	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet einen eigenen Zeitplan für den Zugriff auf bestimmte Gerätetypen.

Schutz von ins Netzwerk eingebundenen Speichern

Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern

Kaspersky Endpoint Security unterstützt keine Komponenten für den Schutz von netzgebundenen Speichern (NAS, Network Attached Storage). Wenn Sie diese Komponenten benötigen, können Sie Kaspersky Security für Windows Server weiterhin verwenden.

Schutz von per ICAP-Protokoll verbundenen Netzwerkspeichern

Kaspersky Endpoint Security unterstützt keine Komponenten für den Schutz von netzgebundenen Speichern (NAS, Network Attached Storage). Wenn Sie diese Komponenten benötigen, können Sie Kaspersky Security für Windows Server weiterhin verwenden.

Anti-Cryptor für NetApp

Kaspersky Endpoint Security unterstützt Anti-Cryptor für NetApp nicht. Die Funktionalität von Anti-Cryptor wird durch andere Programmkomponenten gewährleistet, beispielsweise durch die Verhaltensanalyse.

Netzwerküberwachung

Firewall-Verwaltung

Die KSWS-Firewall-Verwaltung wird von Kaspersky Endpoint Security nicht unterstützt. Die Funktionen der KSWS-Firewall werden von der Firewall auf Systemebene ausgeführt. Nach der Migration können Sie die Kaspersky Endpoint Security-Firewall konfigurieren.

Schutz vor Verschlüsselung

Die Network Anti-Cryptor-Einstellungen werden migriert in den Abschnitt **Erweiterter Schutz**, Unterabschnitt **Verhaltensanalyse**.

Anti-Cryptor-Einstellungen

KSWS-Einstellungen	KES-Einstellungen
Ausführungsmodus: • **Nur Statistik** • **Aktiv**	**Wenn eine externe Verschlüsselung freigegebener Ordner erkannt wird**: • **Informieren**. • **Verbieten**.

KSWS-Einstellungen	KES-Einstellungen
Heuristische Analyse	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet keine heuristische Analyse für die „Verhaltensanalyse“.
Konfiguration des Schutzbereichs: • **Alle freigegeben Netzwerkordner auf dem geschützten Gerät** • **Nur die angegebenen freigegebenen Ordner**	*(wird nicht migriert)* Kaspersky Endpoint Security verhindert eine Verschlüsselung aller freigegebenen Netzwerkordner des geschützten Computers.
Ausnahmen	*(wird nicht migriert)* Kaspersky Endpoint Security verfügt über eigene Ausnahmen für die Komponente „Verhaltensanalyse“. Nach der Migration können Sie manuell Ausnahmen hinzufügen.
Zeitplan-Einstellungen	*(wird nicht migriert)* Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

System-Diagnose

Überwachung der Datei-Integrität

Die Einstellungen für die „Überwachung der Datei-Integrität“ werden von KSWS migriert in den Abschnitt **Sicherheitskontrolle**, Unterabschnitt **Überwachung der Systemintegrität**.

Einstellungen Überwachung der Datei-Integrität

KSWS-Einstellungen	KES-Einstellungen
Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden	*(wird nicht migriert)* Kaspersky Endpoint Security protokolliert keine Ereignisse für Dateioperationen, die während der Unterbrechung der Überwachung durchgeführt wurden.
Versuche zur Kompromittierung des USN-Protokolls blockieren	*(wird nicht migriert)* Kaspersky Endpoint Security blockiert keine Versuche, das USN-Protokoll zu manipulieren.
Überwachungsbereich	**Überwachungsbereich → Datei** *(mit Einschränkungen unterstützt)* Deaktivierte Datensätze zum Überwachungsbereich werden nicht zu KES migriert. Kaspersky Endpoint Security fügt dem Überwachungsbereich nur aktivierte Datensätze hinzu.
Vertrauenswürdige Benutzer	**Vertrauenswürdige Benutzer und/oder Benutzergruppen**
Datei-Operations-Marker	**Markierungen für Dateivorgänge**
Berechnen Sie die Prüfsumme für die Datei, wenn möglich	**Hashing**
Ausnahmen	**Ausnahmen → Datei**

Protokollanalyse

Die KSWS-Einstellungen für die „Protokollanalyse“ werden migriert in den Abschnitt **Sicherheitskontrolle**, Unterabschnitt **Protokollanalyse**.

Protokollanalyseeinstellungen

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Benutzerdefinierte Regeln für die Protokollanalyse verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security wendet alle aktivierten benutzerdefinierten Regeln an.
Manuell festgelegte Regeln	**Benutzerdefinierte Regeln** Die vordefinierte Regel **Ein Dienst wurde im System installiert (für Server 2003 OS)** ist nicht in KES migriert.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Vorkonfigurierte Regeln für die Protokollanalyse verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security wendet alle aktivierten vordefinierten Regeln an.
Vorkonfigurierte Regeln	**Vordefinierte Regeln**
Passwort-Brute-Force-Erkennung	**Erkennung von Brute-Force-Angriffen**
Netzwerk-Anmeldungserkennung	**Erkennung von Netzwerkanmeldungen**
Ausnahmen (IP-Adressen)	**Ausnahmen** (IP-Adresse)
Ausnahmen (Benutzer)	**Ausnahmen** (Benutzer)
Zeitplan-Einstellungen	*(wird nicht migriert)* Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

Protokolle und Benachrichtigungen

Protokolle der Aufgabenausführung

KSWS-Einstellungen für Protokolle werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitte **Benutzeroberfläche** und **Berichte und Speicher**.

Einstellungen für Protokolle

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Ereignisse protokollieren	**Meldungen** (Unterabschnitt **Benutzeroberfläche**)
Ordner für Protokolle	*(wird nicht migriert)* Kaspersky Endpoint Security speichert Berichte im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\Report`.
Protokolle der Aufgabenausführung löschen, wenn älter als n Tag(e)	*(wird nicht migriert)* Die Speicherdauer für KES-Berichte können Sie unter **Allgemeine Einstellungen**, **Berichte und Speicher** konfigurieren.
Ereignisse aus dem Systemaudit-Protokoll löschen n Tag(e)	*(wird nicht migriert)* Kaspersky Endpoint Security beschränkt die Speicherung aller Berichte, einschließlich Systemaudit-Berichten.
SIEM-Integration	*(wird nicht migriert)* Die SIEM-Integration können Sie in Kaspersky Security Center konfigurieren.

Ereignisbenachrichtigungen

Die KSWS-Benachrichtigungseinstellungen werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitt **Benutzeroberfläche**.

Benachrichtigungseinstellungen

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Meldungen	**Meldungen**
Benachrichtigung für die Benutzer: • **Mittels Terminaldienst** • **Mittels Windows Messenger Dienst**	*(wird nicht migriert)* Kaspersky Endpoint Security unterstützt das Ändern des Benachrichtigungstextes nicht. Kaspersky Endpoint Security zeigt Standardbenachrichtigungen an.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Benachrichtigung für die Administratoren: • **Mittels Windows Messenger Dienst** • **Ausführbare Datei starten** • **Per E-Mail**	Nur die Einstellungen für E-Mail-Benachrichtigungen werden in Kaspersky Endpoint Security migriert – **E-Mail-Benachrichtigungseinstellungen** (Block **Meldungen**). Andere Methoden zur Benachrichtigung von Administratoren werden nicht unterstützt.
Programm-Datenbanken sind veraltet	**Benachrichtigung „Datenbanken sind veraltet“ senden, wenn die Datenbanken nicht aktualisiert wurden seit**
Programm-Datenbanken sind stark veraltet	**Benachrichtigung „Datenbanken sind stark veraltet“ senden, wenn die Datenbanken nicht aktualisiert wurden seit**
Untersuchung wichtiger Bereiche des Computers wurde lange nicht durchgeführt	*(wird nicht migriert)* Kaspersky Endpoint Security generiert nach drei Tagen ein Ereignis über die versäumte „Untersuchung wichtiger Bereiche“.

Interaktion mit Administrationsserver

Die Einstellungen für die Interaktion mit dem Administrationsserver werden migriert in den Abschnitt **Allgemeine Einstellungen**, Unterabschnitt **Berichte und Speicher**.

Einstellungen für die Interaktion mit dem Administrationsserver

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Dateien in Quarantäne	**Quarantäne-Dateien**
Dateien im Backup	**Backup-Dateien**
Blockierte Hosts	*(wird nicht migriert)* Kaspersky Endpoint Security sendet automatisch Daten über blockierte Hosts.

Aufgaben

Programm aktivieren

Die Aufgabe *Programm aktivieren* (KSWS) wird von Kaspersky Endpoint Security nicht unterstützt. Sie können eine Aufgabe *Schlüssel hinzufügen* (KES) erstellen, dem Installationspaket einen Lizenzschlüssel hinzufügen oder die automatische Lizenzschlüsselverteilung aktivieren.

Update-Verteilung

Die Einstellungen der Aufgabe *Update-Verteilung* (KSWS) werden in die Aufgabe *Update der Datenbanken und Programm-Module* (KES) migriert.

Einstellungen der Aufgabe „Update-Verteilung“

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Update-Quelle: • **Administrationsserver von Kaspersky Security Center** • **Kaspersky-Update-Server** • **Andere HTTP-/ FTP-Server oder Netzwerkressourcen**	**Update-Quelle**: • **Kaspersky Security Center**. • **Kaspersky-Update-Server**. • **Benutzerdefiniert**.
Kaspersky-Update-Server verwenden, wenn die angegebenen Server nicht verfügbar sind	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt die Auswahl mehrerer Update-Quellen, einschließlich der Kaspersky-Update-Server. Wenn die erste Update-Quelle nicht verfügbar ist, können Sie mit Kaspersky Endpoint Security Updates von einer anderen Quelle aus der Liste beziehen.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Update-Servern verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den Proxyserver für alle Komponenten. Sie können die Proxyserver-Verbindung in den Netzwerkoptionen des Programms konfigurieren.
Proxyserver-Einstellungen für die Verbindung zu anderen Servern verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den Proxyserver für alle Komponenten. Sie können die Proxyserver-Verbindung in den Netzwerkoptionen des Programms konfigurieren.
Einstellungen für die Update-Verteilung: • **Updates der Programm-Datenbanken verteilen** • **Wichtige Updates der Programm-Module verteilen** • **Updates der Programm-Datenbanken und wichtige Updates der Programm-Module verteilen**	*(wird nicht migriert)* Kaspersky Endpoint Security kopiert Datenbank-Updates und kritische Updates von Programmmodulen als ein einziges Paket.
Ordner für die lokale Speicherung kopierter Updates	**Updates in folgenden Ordner kopieren**

Überwachung der Baseline-Integrität

Die Einstellungen der Aufgabe *Baseline-Überwachung der Datei-Integrität* (KSWS) werden in den Aufgabe *Prüfung der Systemintegrität* und in den Richtlinienabschnitt **Sicherheitskontrolle**, Unterabschnitt **Überwachung der Systemintegrität** migriert.

Einstellungen der Aufgabe zur Baseline-Überwachung der Datei-Integrität

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Algorithmus zur Hash-Berechnung: • **MD5** • **SHA256**.	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den SHA256-Algorithmus zur Berechnung der Prüfsumme.
Untersuchungsbereich	**Überwachungsbereich** (Unterabschnitt **Überwachung der Systemintegrität**)

Datenbanken-Update

Die Einstellungen der Aufgabe *Datenbanken-Update* (KSWS) werden in die Aufgabe *Update der Datenbanken und Programm-Module* (KES) migriert.

Einstellungen der Aufgabe zum Update der Datenbanken

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Update-Quelle: • **Administrationsserver von Kaspersky Security Center** • **Kaspersky-Update-Server** • **Andere HTTP-/ FTP-Server oder Netzwerkressourcen**	**Update-Quelle**: • **Kaspersky Security Center**. • **Kaspersky-Update-Server**. • **Benutzerdefiniert**.
Kaspersky-Update-Server verwenden, wenn die angegebenen Server nicht verfügbar sind	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt die Auswahl mehrerer Update-Quellen, einschließlich der Kaspersky-Update-Server. Wenn die erste Update-Quelle nicht verfügbar ist, können Sie mit Kaspersky Endpoint Security Updates von einer anderen Quelle aus der Liste beziehen.
Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Update-Servern verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den Proxyserver für alle Komponenten. Sie können die Proxyserver-Verbindung in den Netzwerkoptionen des Programms konfigurieren.
Proxyserver-Einstellungen für die Verbindung zu anderen Servern verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den Proxyserver für alle Komponenten. Sie können die Proxyserver-Verbindung in den Netzwerkoptionen des Programms konfigurieren.
Belastung des Festplatten-Subsystems verringern	*(wird nicht migriert)*

Update der Programm-Module

Die Einstellungen der Aufgabe *Update der Programm-Module* (KSWS) werden in die Aufgabe *Update der Datenbanken und Programm-Module* (KES) migriert.

Einstellungen der Aufgabe „Update der Programm-Module“

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Update-Quelle: • **Administrationsserver von Kaspersky Security Center** • **Kaspersky-Update-Server** • **Andere HTTP-/ FTP-Server oder Netzwerkressourcen**	**Update-Quelle**: • **Kaspersky Security Center**. • **Kaspersky-Update-Server**. • **Benutzerdefiniert**.
Kaspersky-Update-Server verwenden, wenn die angegebenen Server nicht verfügbar sind	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt die Auswahl mehrerer Update-Quellen, einschließlich der Kaspersky-Update-Server. Wenn die erste Update-Quelle nicht verfügbar ist, können Sie mit Kaspersky Endpoint Security Updates von einer anderen Quelle aus der Liste beziehen.
Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Update-Servern verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den Proxyserver für alle Komponenten. Sie können die Proxyserver-Verbindung in den Netzwerkoptionen des Programms konfigurieren.
Proxyserver-Einstellungen für die Verbindung zu anderen Servern verwenden	*(wird nicht migriert)* Kaspersky Endpoint Security verwendet den Proxyserver für alle Komponenten. Sie können die Proxyserver-Verbindung in den Netzwerkoptionen des Programms konfigurieren.
Wichtige Updates der Programm-Module verteilen und installieren	**Kritische und bestätigte Updates installieren**
Nur auf wichtige Updates der Programm-Module überprüfen	*(wird nicht migriert)* Kaspersky Endpoint Security prüft laufend die Verfügbarkeit von kritischen Updates für Programm-Module.
Neustart des Betriebssystems zulassen	*(wird nicht migriert)* Kaspersky Endpoint Security fragt den Benutzer nach Erlaubnis, den Computer neu zu starten.
Über verfügbare planmäßige Updates der Programm-Module informieren	*(wird nicht migriert)* Kaspersky Endpoint Security zeigt Benachrichtigungen über Programm-Modul-Updates an.

Rollback des Updates der Programm-Datenbanken

Die Einstellungen der Aufgabe *Rollback des Updates der Programm-Datenbanken* (KSWS) werden in die Aufgabe *Update-Rollback* (KES) migriert. Die neue Aufgabe *Update-Rollback* (KES) hat einen Zeitplan für den Aufgabenstart – *Manuell*.

Untersuchung auf Befehl

Die Einstellungen der Aufgabe *Untersuchung auf Befehl* (KSWS) werden in die Aufgabe *Schadsoftware-Untersuchung* (KES) migriert.

Einstellungen der Aufgabe „Untersuchung auf Viren“

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Untersuchungsbereich	**Untersuchungsbereich**
Sicherheitsstufe: • **Maximale Sicherheit** • **Empfohlen** • **Maximale Leistung**	**Sicherheitsstufe**: • **Hoch**. • **Empfohlen**. • **Niedrig**. Die Einstellungen der Sicherheitsstufen sind in KSWS und KES unterschiedlich.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Untersuchungsobjekte: • Alle Objekte • Objekte, die nach Format untersucht werden • Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden • Objekte, die nach angegebener Erweiterungsliste untersucht werden	Dateitypen: • **Alle Dateien**. • **Dateien nach Format untersuchen**. • **Dateien nach Erweiterung untersuchen**. In Kaspersky Endpoint Security kann keine benutzerdefinierte Liste mit Erweiterungen erstellt werden. Kaspersky Endpoint Security ersetzt den Wert **Objekte, die nach angegebener Erweiterungsliste untersucht werden** durch den Wert **Dateien nach Erweiterung untersuchen**.
Untergeordnete Ordner	Unterordner einschließen
Untergeordnete Dateien	*(wird nicht migriert)*
Bootsektoren und MBR untersuchen	*(wird nicht migriert)*
Alternative NTFS-Ströme untersuchen	*(wird nicht migriert)*
Nur neue und veränderte Dateien untersuchen	Nur neue und veränderte Dateien untersuchen
Zusammengesetzte Objekte untersuchen: • Alle Archive • Alle SFX-Archive • Alle E-Mail-Datenbanken • Alle gepackten Objekte • Alle E-Mails im Nur-Text-Format • Alle eingebetteten OLE-Objekte	Untersuchung von zusammengesetzten Dateien: • **Archive untersuchen**. • **Kennwortgeschützte Archive untersuchen**. • **Programmpakete untersuchen**. • **Dateien in E-Mail-Formaten untersuchen**. • **Dateien in Microsoft Office-Formaten untersuchen**.
Aktion für infizierte und andere Objekte: • Desinfizieren • Desinfizieren. Entfernen, falls Desinfektion fehlschlägt • Löschen • Empfohlene Aktion ausführen • Nur informieren	Aktion beim Fund einer Bedrohung: • **Desinfizieren – Löschen, wenn Desinfektion fehlschlägt**. • **Desinfizieren – Informieren, wenn Desinfektion fehlschlägt**. • **Informieren**.
Aktion für möglicherweise infizierte Objekte: • Quarantäne • Löschen • Empfohlene Aktion ausführen • Nur informieren	*(wird nicht migriert)* Kaspersky Endpoint Security wendet die Aktion an, wenn eine Bedrohung erkannt wird.
Aktionen je nach Typ des erkannten Objekts ausführen	*(wird nicht migriert)*
Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann	*(wird nicht migriert)*
Dateien ausschließen	*(wird nicht migriert)* Kaspersky Endpoint Security wendet die vertrauenswürdige Zone auf alle Komponenten an. Ausnahmen können Sie in den Einstellungen der vertrauenswürdigen Zone konfigurieren.
Nicht erkennen	*(wird nicht migriert)*
Untersuchung beenden, wenn sie länger dauert als n Sekunden	Dateien überspringen, wenn Untersuchung länger dauert als N Sek
Zusammengesetzte Objekte nicht untersuchen, wenn größer als n MB	Große zusammengesetzte Dateien nicht entpacken
iSwift-Technologie verwenden	iSwift-Technologie
iChecker-Technologie verwenden	iChecker-Technologie
Aktionen für ausgelagerte Dateien: • Nicht untersuchen • Nur den residenten Teil einer Datei untersuchen • Datei vollständig untersuchen • Nur, wenn auf die Datei innerhalb des angegebenen Zeitraums zugegriffen wurde (Tage) • Datei, wenn möglich, nicht auf die lokale Festplatte kopieren	*(wird nicht migriert)* Kaspersky Endpoint Security untersucht ausgelagerte Dateien vollständig.

Integritätsprüfung für Anwendungen

Die Einstellungen der Aufgabe *Integritätsprüfung für Programme* (KSWS) werden in die Aufgabe *Prüfung der Anwendungsintegrität* (KES) migriert.

Erstellen von Regeln für die Kontrolle des Programmstarts

Kaspersky Endpoint Security unterstützt die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* nicht. Sie können Regeln in den Einstellungen der „Programmkontrolle“ generieren.

Erstellen von Regeln für die Gerätekontrolle

Kaspersky Endpoint Security unterstützt die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* nicht. Sie können Regeln in den Einstellungen der „Gerätekontrolle“ generieren.

Migration von KSWS-Komponenten

Vor der lokalen Installation überprüft Kaspersky Endpoint Security, ob andere Kaspersky-Programme auf dem Computer vorhanden sind. Wenn Kaspersky Security für Windows Server auf dem Computer installiert ist, erkennt KES die installierten KSWS-Komponenten und wählt die gleichen Komponenten zur Installation aus.

KES-Komponenten, die in KSWS nicht vorhanden sind, werden wie folgt installiert:

- „AMSI-Schutz“, „Programm-Überwachung“ und „Rollback von schädlichen Aktionen“ werden mit Standardeinstellungen installiert.
- Die Komponenten „Schutz vor modifizierten USB-Geräten“, „Adaptive Kontrolle von Anomalien“, „Datenverschlüsselung“ und „Detection und Response“ werden ignoriert.

Bei einer Remote-Installation wird die Auswahl der installierten KSWS-Komponenten vom Programm KES ignoriert. Das Installationsprogramm installiert die Komponenten, die Sie in den Eigenschaften des Installationspakets auswählen. Nach der Installation von Kaspersky Endpoint Security und der Migration von Richtlinien und Aufgaben werden die KES-Einstellungen gemäß den KSWS-Einstellungen konfiguriert.

Migration von KSWS-Aufgaben und -Richtlinien

Sie können Einstellungen für KSWS-Richtlinien und -Aufgaben wie folgt migrieren:

- Mithilfe des Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (im Folgenden auch „Migrations-Assistent“ genannt).

  > Der Migrations-Assistent für KSWS ist nur in der Verwaltungskonsole (MMC) verfügbar. Richtlinien- und Aufgabeneinstellungen können nicht über die Web Console oder Cloud Console migriert werden.

  Der Assistent für das Massenkonvertieren funktioniert für verschiedene Versionen von Kaspersky Security Center unterschiedlich. Wir empfehlen ein Upgrade der Lösung auf Version 14.2 oder höher. In dieser Version von Kaspersky Security Center können Sie mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben Richtlinien in ein Profil migrieren, aber nicht in eine Richtlinie. In dieser Version von Kaspersky Security Center können Sie mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben auch eine breitere Palette von Richtlinieneinstellungen migrieren.

- Mit dem Assistenten zum Erstellen einer Richtlinie von Kaspersky Endpoint Security für Windows

  Mit dem „Assistenten für das Erstellen einer Richtlinie“ können Sie auf Basis einer KSWS-Richtlinie eine KES-Richtlinie erstellen

Die Verfahren zur Migration der KSWS-Richtlinie unterscheiden sich je nachdem, ob der Migrations-Assistent oder der Assistent für das Erstellen einer Richtlinie verwendet wird.

Assistent für das Massenkonvertieren von Richtlinien und Aufgaben

Anstelle von KES-Richtlinieneinstellungen überträgt der Migrations-Assistent die KSWS-Richtlinieneinstellungen in das Richtlinienprofil. Das *Richtlinienprofil* ist eine Auswahl von Richtlinieneinstellungen, die auf einem Computer aktiviert werden, wenn der Computer die konfigurierten Aktivierungsregeln erfüllt. Das Geräte-Tag `UpgradedFromKSWS` ist als Auslösekriterium für das Richtlinienprofil ausgewählt. Kaspersky Security Center fügt automatisch das Tag `UpgradedFromKSWS` auf allen Computern hinzu, auf denen Sie KES mithilfe der Aufgabe zur Remote-Installation über KSWS installieren. Wenn Sie eine andere Installationsmethode gewählt haben, können Sie das Tag den Geräten manuell zuweisen.

Um einem Gerät ein Tag hinzuzufügen:

1. Erstellen Sie ein neues Tag für Server – `UpgradedFromKSWS`.

   Weitere Informationen über das Erstellen von Tags für Geräte finden Sie in der Hilfe zu Kaspersky Security Center.

2. Erstellen Sie eine neue Administrationsgruppe in der Kaspersky Security Center-Konsole und fügen Sie dieser Gruppe die Server hinzu, denen Sie das Tag zuweisen möchten.

   Sie können die Server mit dem Auswahlwerkzeug gruppieren. Weitere Informationen über die Arbeit mit Auswahlen finden Sie in der Hilfe zu Kaspersky Security Center.

3. Wählen Sie alle Server der Administrationsgruppe in der Kaspersky Security Center-Konsole aus, öffnen Sie die Eigenschaften der ausgewählten Server und weisen Sie das Tag zu.

Wenn Sie mehrere KSWS-Richtlinien migrieren, wird jede Richtlinie in ein Profil innerhalb einer übergeordneten Richtlinie umgewandelt. Wenn die KSWS-Richtlinie bereits Profile enthält, werden diese Profile ebenfalls als Profile migriert. Auf diese Weise erhalten Sie eine einzige Richtlinie, die Profile enthält, die den jeweiligen KSWS-Richtlinien entsprechen.

So verwenden Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben, um KSWS-Richtlinieneinstellungen zu migrieren

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus und öffnen Sie durch Rechtsklick das Kontextmenü.

2. Wählen Sie die Option **Alle Aufgaben → Assistent für das Massenkonvertieren von Richtlinien und Aufgaben** aus.

Der „Assistent für das Massenkonvertieren von Richtlinien und Aufgaben“ wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Auswahl des Programms, für das Sie Richtlinien und Aufgaben konvertieren müssen

Bei diesem Schritt müssen Sie Kaspersky Endpoint Security für Windows auswählen. Weiter zum nächsten Schritt

Schritt 2. Konvertieren von Richtlinien

Der Migrations-Assistent erstellt KSWS-Richtlinienprofile innerhalb einer KES-Richtlinie. Wählen Sie die Richtlinien für Kaspersky Security für Windows Server aus, die Sie in Richtlinienprofile konvertieren möchten. Weiter zum nächsten Schritt

Der Migrations-Assistent beginnt mit der Richtlinienkonvertierung. Die Namen der neuen Richtlinienprofile entsprechen den ursprünglichen KSWS-Richtlinien.

Schritt 3. Bericht über die Richtlinien-Migration

Der Migrations-Assistent erstellt einen Bericht über die Richtlinien-Migration. Der Bericht über die Richtlinien-Migration enthält den Zeitpunkt (Datum und Uhrzeit) der Richtlinienkonvertierung, den Namen der ursprünglichen KSWS-Richtlinie, den Namen der KES-Zielrichtlinie und den Namen des neuen Richtlinienprofils.

Schritt 4. Konvertieren von Aufgaben

Der Migrations-Assistent erstellt neue Aufgaben für Kaspersky Endpoint Security für Windows. Wählen Sie in der Aufgabenliste die KSWS-Aufgaben aus, die Sie für Kaspersky Endpoint Security erstellen möchten. Die neuen Aufgaben erhalten den Namen *<Name der KSWS-Aufgabe> (konvertiert)*. Weiter zum nächsten Schritt

Schritt 5. Assistent abschließen

Schließen Sie den Assistenten ab. Als Ergebnis geht der Assistent wie folgt vor:

- Der Kaspersky Endpoint Security-Richtlinie werden neue Richtlinienprofile hinzugefügt.

  Die Richtlinie enthält Profile mit den Einstellungen von Kaspersky Security für Windows Server. Die neue Richtlinie hat den Status *Aktiv*. Der Assistent verändert die KSWS-Richtlinien nicht.

- Er erstellt Aufgaben für Kaspersky Endpoint Security.

  Die neuen Aufgaben sind Kopien von KSWS-Aufgaben. Der Assistent verändert die KSWS-Aufgaben nicht.

Das neue Richtlinienprofil mit den KSWS-Einstellungen erhält den Namen *UpgradedFromKSWS<Name der Richtlinie für Kaspersky Security für Windows Server>*. In den Profileigenschaften wählt der Migrations-Assistent automatisch das Geräte-Tag `UpgradedFromKSWS` als Auslösekriterium aus. Dadurch werden die Einstellungen aus dem Richtlinienprofil automatisch auf die Server angewendet.

Assistent zum Erstellen einer Richtlinie, die auf einer KSWS-Richtlinie basiert

Wenn eine KES-Richtlinie auf Basis einer KSWS-Richtlinie erstellt wird, überträgt der Assistent die Einstellungen dementsprechend in die neue Richtlinie. Eine KES-Richtlinie entspricht also einer KSWS-Richtlinie. Der Assistent konvertiert die Richtlinie nicht in ein Profil.

So verwenden Sie den „Assistenten für das Erstellen einer Richtlinie“, um die KSWS-Richtlinieneinstellungen zu migrieren

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe aus, zu der die entsprechenden Client-Computer gehören.
3. Wählen Sie im Arbeitsbereich die Registerkarte **Richtlinien** aus.
4. Klicken Sie auf **Neue Richtlinie**.

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

Schritt 1.

Wählen Sie das Programm **Kaspersky Endpoint Security für Windows (14.2)** aus.

Schritt 2.

Geben Sie einen Namen für die Gruppenrichtlinie ein, z. B. *Büro-Richtlinie*.

Aktivieren Sie das Kontrollkästchen **Richtlinieneinstellungen für eine frühere Version der Anwendung verwenden**. Klicken Sie auf **Durchsuchen** und wählen Sie die KSWS-Richtlinie aus.

Schritt 3. Text der Erklärung zu Kaspersky Security Network anzeigen

Bitte lesen und akzeptieren Sie die Erklärung zu Kaspersky Security Network (KSN).

Schritt 4.

Wählen Sie den Punkt **Standardmodus für den Schutz von Hosts**. Kaspersky Endpoint Security bietet eine gemeinsame Richtlinie für alle Programm-Modi und Betriebssystemtypen.

Es wird empfohlen, für die einzelnen Modi und Betriebssystemtypen unterschiedliche Richtlinien zu verwenden.

Schritt 5. Einstellungen importieren

Dieser Schritt ist verfügbar, wenn Sie bei Schritt 4 die manuelle Richtlinienkonfiguration ausgewählt haben.

Sie können eine Richtlinie auf Basis von Einstellungen für Kaspersky Endpoint Security aus einer CFG-Konfigurationsdatei erstellen. Der Assistent für neue Richtlinien unterstützt keine verschlüsselten Konfigurationsdateien. Überspringen Sie beim Exportieren der Konfigurationsdatei den Schritt zur Dateiverschlüsselung.

Beim Importieren einer CFG-Konfigurationsdatei des Programms stehen im Assistenten nicht alle Richtlinieneinstellungen zur Verfügung. In den Programmeinstellungen fehlen beispielsweise Richtlinienprofile. Wenn Sie alle Einstellungen und Profile in die Richtlinie übertragen möchten, können Sie eine andere Richtlinie aus einer KLP-Datei importieren.

Wenn eine Konfigurationsdatei importiert wird, überträgt Kaspersky Endpoint Security keine Kennwörter für Krypto-Container. Wenn Sie für die Verbindung mit Servern die Zwei-Wege-Authentifizierung verwenden, müssen Sie die Kennwörter für Krypto-Container völlig neu angeben.

Schritt 6 bis 10. Richtlinieneinstellungen konfigurieren

Dieser Schritt ist verfügbar, wenn Sie bei Schritt 4 die manuelle Richtlinienkonfiguration ausgewählt haben.

Folgen Sie den Schritten, um die Richtlinieneinstellungen zu anzupassen.

Schritt 11. Vertrauenswürdige Zone konfigurieren

Vertrauenswürdige Zone konfigurieren Sie können vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme hinzufügen. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme sind auch praktisch, um Kaspersky Endpoint Security im Light Agent-Modus in virtuellen Citrix- und VMware-Umgebungen schnell zu konfigurieren.

Schritt 12. Status der Richtlinie auswählen

- **Aktiv**. Die Richtlinie wird auf diesem Computer nach der nächsten Synchronisierung als aktive Richtlinie verwendet.

  Die Einstellungen einer aktiven Richtlinie werden bei der Synchronisierung auf den Client-Computern gespeichert. Für einen Computer dürfen nicht mehrere Richtlinien gleichzeitig gelten, deshalb kann in jeder Gruppe nur eine Richtlinie aktiv sein.

- **Inaktiv**. Ersatzrichtlinie. Eine inaktive Richtlinie kann erforderlichenfalls aktiviert werden.

  Sie können unbeschränkt viele inaktive Richtlinien erstellen. Eine inaktive Richtlinie beeinflusst die Programmeinstellungen auf den Computern im Netzwerk nicht. Inaktive Richtlinien erlauben eine schnelle Reaktion auf Extremsituationen wie beispielsweise Virenangriffe. Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. Dabei wird die aktive Richtlinie automatisch inaktiv.

- **Mobil**. Die Richtlinie wird nur wirksam, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.

Schließen Sie den Assistenten ab.

Zusätzliche Konfiguration von Richtlinien und Aufgaben nach der Migration

KSWS und KES haben eine unterschiedliche Auswahl von Komponenten und Richtlinieneinstellungen, daher müssen Sie nach der Migration überprüfen, ob die Richtlinieneinstellungen den Sicherheitsanforderungen Ihres Unternehmens entsprechen.

Überprüfen Sie die folgenden grundlegenden Richtlinieneinstellungen:

- Kennwortschutz. Die Einstellungen für den KSWS-Kennwortschutz werden nicht migriert. Kaspersky Endpoint Security verfügt über eine integrierte Funktion für den Kennwortschutz. Aktivieren Sie bei Bedarf den Kennwortschutz und legen Sie ein Kennwort fest.

- Vertrauenswürdige Zone. Die von KSWS und KES verwendeten Methoden zur Auswahl von Objekten unterscheiden sich. Bei der Migration unterstützt KES Ausnahmen, die als einzelne Dateien oder Pfade für Dateien bzw. Ordner definiert sind. Ausnahmen, die KSWS als vordefinierten Bereich oder als Skript-URL konfiguriert hat, werden nicht migriert. Solche Ausnahmen müssen Sie nach der Migration manuell hinzufügen.

  Um das korrekte Funktionieren von Kaspersky Endpoint Security auf den Servern sicherzustellen, wird empfohlen, Dateien, die für das Funktionieren von Servern wichtig sind, der vertrauenswürdigen Zone hinzuzufügen. Für SQL-Server müssen Sie MDF- und LDF-Datenbankdateien hinzufügen. Für Microsoft Exchange-Server müssen Sie CHK-, EDB-, JRS-, LOG- und JSL-Dateien hinzufügen. Sie können Masken verwenden, z. B. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

  Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen.

- Firewall. Die Funktionen der KSWS-Firewall werden von der Firewall auf Systemebene ausgeführt. In KES gibt es eine eigene Komponente für die Firewall-Funktionalität. Nach der Migration können Sie die Kaspersky Endpoint Security-Firewall konfigurieren.

- Kaspersky Security Network In Kaspersky Endpoint Security kann KSN nicht für einzelne Komponenten konfiguriert werden. Kaspersky Endpoint Security verwendet KSN für alle Programmkomponenten. Um KSN nutzen zu können, müssen Sie den neuen Nutzungsbedingungen der Kaspersky Security Network-Erklärung zustimmen.

- Web-Kontrolle Die Sperr-Regeln für die Kontrolle von Kategorien des Web-Datenverkehrs werden in Kaspersky Endpoint Security in eine einzige Sperr-Regel migriert. Kaspersky Endpoint Security ignoriert Erlaubnisregeln für die Kategoriekontrolle. Kaspersky Endpoint Security unterstützt nicht alle Kategorien von „Kaspersky Security für Windows Server". Kategorien, die in Kaspersky Endpoint Security nicht vorhanden sind, werden nicht migriert. Darum werden Klassifizierungsregeln für Webressourcen mit nicht unterstützten Kategorien nicht migriert. Fügen Sie bei Bedarf Regeln für die „Web-Kontrolle" hinzu.

- Proxyserver. Das Kennwort für die Verbindung zum Proxyserver wird nicht migriert. Geben Sie das Kennwort für die Verbindung zum Proxyserver manuell ein.

- Zeitpläne für die einzelnen Komponenten. In Kaspersky Endpoint Security können keine Zeitpläne für einzelne Komponenten konfiguriert werden. Die Komponenten sind immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

- Auswahl der Komponenten. Die Auswahl der für Kaspersky Endpoint Security verfügbaren Funktionen ist vom Typ des Betriebssystems abhängig: Workstation oder Server. Auf Servern ist beispielsweise nur die BitLocker-Laufwerkverschlüsselung verfügbar.

- Attribut. Der Zustand des Attributs wird nicht migriert. Das Attribut hat den Standardwert. Standardmäßig gilt für fast alle Einstellungen in der neuen Richtlinie ein Verbot, Einstellungen in untergeordneten Richtlinien und in der lokalen Programmschnittstelle zu ändern. Für Richtlinieneinstellungen im Abschnitt **Managed Detection and Response (Industrial CyberSecurity)** und in der Einstellungsgruppe **Support für Benutzer** (Abschnitt **Benutzeroberfläche**) hat das Attribut hat den Wert . Bei Bedarf können Sie die Vererbung von Einstellungen aus der übergeordneten Richtlinie konfigurieren.

- Arbeit mit aktiven Bedrohungen. Die „Aktive Desinfektion" funktioniert auf Workstations und Servern in unterschiedlicher Weise. Die aktive Desinfektion können Sie in den Einstellungen der Aufgabe *Schadsoftware-Untersuchung* und in den Programmeinstellungen anpassen.

- Programm-Upgrade. Um wichtige Updates und Patches ohne Neustart zu installieren, müssen Sie den Modus für Programm-Upgrades ändern. Standardmäßig ist die Funktion „Programm-Updates ohne Neustart installieren" deaktiviert.

- Kaspersky Endpoint Agent. Kaspersky Endpoint Security verfügt über einen integrierten Agenten für die Verwendung von Detection and Response-Lösungen. Übertragen Sie bei Bedarf die Richtlinieneinstellungen von Kaspersky Endpoint Agent in die Richtlinie von Kaspersky Endpoint Security.

- Aufgaben zur *Update der Datenbanken und Programm-Module*. Überprüfen Sie, ob die Einstellungen der Aufgabe *Update der Datenbanken und Programm-Module* korrekt migriert wurden. Anstelle von drei KSWS-Aufgaben verwendet KES eine einzelne KES-Aufgabe. Sie können die *Update der Datenbanken und Programm-Module*-Aufgaben optimieren und überflüssige Aufgaben entfernen.

- Sonstige Aufgaben. Die Komponenten „Programmkontrolle", „Gerätekontrolle" und „Überwachung der Datei-Integrität" funktionieren in KSWS und KES unterschiedlich. Die folgenden Aufgaben werden von KES nicht verwendet: *Überwachung der Baseline-Integrität*, *Erstellen von Regeln für die Kontrolle des Programmstarts*, *Erstellen von Regeln für die Gerätekontrolle*. Darum werden diese Aufgaben nicht migriert. Nach der Migration können Sie die Komponenten „Überwachung der Datei-Integrität", Programmkontrolle und Gerätekontrolle konfigurieren.

Migration der vertrauenswürdigen Zone für KSWS

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Endpoint Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt. Sie können Objekte der vertrauenswürdigen Zone von KSWS nach KES migrieren und dazu den *Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben* oder den *Assistenten zum Erstellen einer neuen KES-Richtlinie, die auf der KSWS-Richtlinie basiert* verwenden. KSWS und KES haben eine unterschiedliche Auswahl von Komponenten und Funktionen, daher müssen Sie nach der Migration überprüfen, ob die Ausnahmen den Sicherheitsanforderungen Ihres Unternehmens entsprechen. Auch die Methoden, mit denen Ausnahmen zur vertrauenswürdigen Zone hinzugefügt werden, sind für KES und KSWS unterschiedlich. Der Migrations-Assistent bietet keine Tools zur Migration aller KSWS-Ausnahmen. Das bedeutet, dass Sie nach der Migration einige KSWS-Ausnahmen manuell hinzufügen müssen.

Um das korrekte Funktionieren von Kaspersky Endpoint Security auf den Servern sicherzustellen, wird empfohlen, Dateien, die für das Funktionieren von Servern wichtig sind, der vertrauenswürdigen Zone hinzuzufügen. Für SQL-Server müssen Sie MDF- und LDF-Datenbankdateien hinzufügen. Für Microsoft Exchange-Server müssen Sie CHK-, EDB-, JRS-, LOG- und JSL-Dateien hinzufügen. Sie können Masken verwenden, z. B. `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen.

Methoden zum Erstellen der vertrauenswürdige Zone für KES und KSWS.

KSWS		KES
Untersuchungsobjekt		
• Vordefinierter Bereich	*(wird nicht migriert)*	
• Datenträger, Ordner oder Netzwerkpfad	→	**Datei oder Ordner**
• Datei	→	**Datei oder Ordner**
• Skriptdatei oder Webadresse	*(wird nicht migriert)*	
Erkanntes Objekt	→	**Typ des erkannten Objekts**
Vertrauenswürdige Prozesse	→	**Vertrauenswürdige Programme**

Migration untersuchter Objekte

KSWS-Ausnahmen, in deren Eigenschaften die Methode **Untersuchungsobjekt** ausgewählt ist, werden mit gewissen Einschränkungen in KES-Ausnahmen migriert, in deren Eigenschaften die Methode **Datei oder Ordner** ausgewählt ist. Die Migration einer Ausnahme ist von der Methode zur Objektauswahl abhängig:

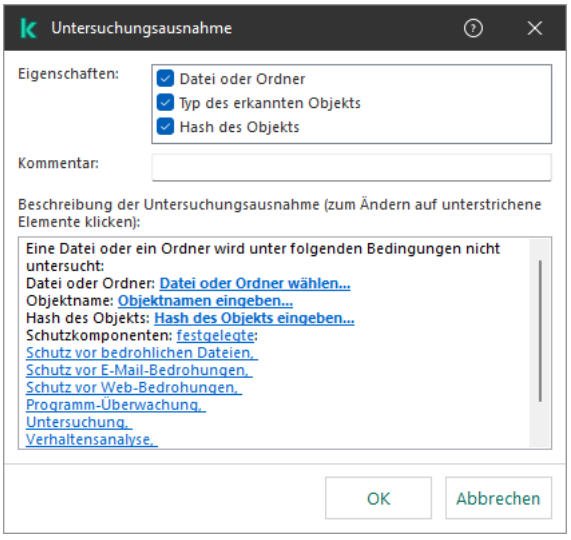
- Vordefinierter Bereich – *nicht migrieren*.

  Solche Ausnahmen müssen Sie nach der Migration manuell hinzufügen. Ausnahmen in Form vordefinierter Bereiche müssen in den Einstellungen der Aufgabe *Schadsoftware-Untersuchung* konfiguriert werden.

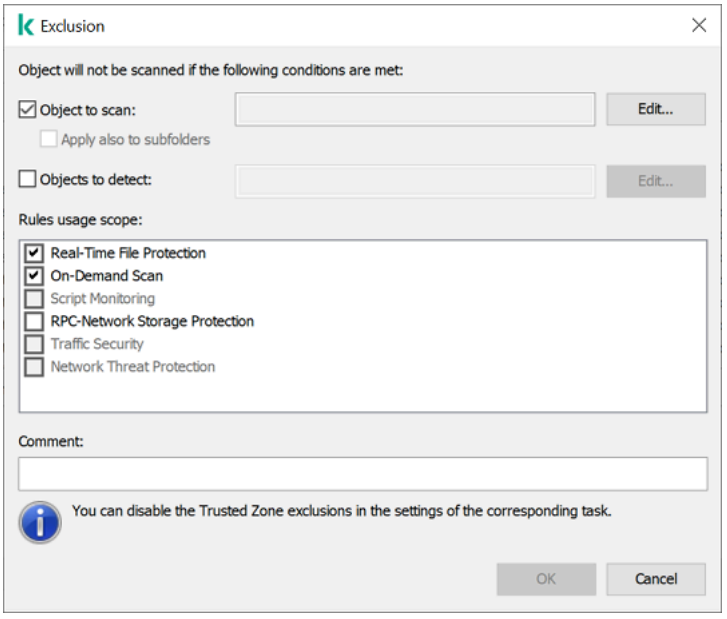
- Datenträger, Ordner oder Netzwerkpfad – in KES-Ausnahmen migrieren, in deren Eigenschaften die Methode „Datei oder Ordner“ ausgewählt ist.
- Datei – in KES-Ausnahmen migrieren, in deren Eigenschaften die Methode „Datei oder Ordner“ ausgewählt ist.
- Skriptdatei oder Webadresse – *nicht migrieren*.

  Solche Ausnahmen müssen Sie nach der Migration manuell hinzufügen. Ausnahmen in Form von Skript-Webadressen müssen zu den vertrauenswürdigen Webadressen für den „Schutz vor Web-Bedrohungen“ hinzugefügt werden.

Wenn das Kontrollkästchen **Auch für Unterordner übernehm** für das untersuchte Objekt aktiviert ist, wird diese Einstellung in die KES-Ausnahme migriert (Kontrollkästchen **Unterordner einschließen**).



Einstellungen der KES-Ausnahme



Einstellungen der KSWS-Ausnahme

Migration erkannter Objekte

KSWS-Ausnahmen, in deren Eigenschaften die Methode **Erkanntes Objekt** ausgewählt ist, werden in KES-Ausnahmen migriert, in deren Eigenschaften die Methode **Typ des erkannten Objekts** ausgewählt ist. Der Name des erkannten Objekts entspricht der Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`). Kaspersky Endpoint Security unterstützt Masken mit einem Fragezeichen `?` (Platzhalter für ein beliebiges einzelnes Zeichen) und dem Sternchen `*` (Platzhalter für eine Zeichenfolge).

Migration des Verwendungsbereichs einer Ausnahme

Der Verwendungsbereich einer Ausnahme ist eine Auswahl von Komponenten, für welche die Ausnahme gilt. KES und KSWS verfügen über eine unterschiedliche Auswahl von Komponenten. Deshalb kann der Migrations-Assistent den Verwendungsbereich einer Ausnahme nicht migrieren. Wenn also im KSWS-Verwendungsbereich mindestens eine Komponente ausgewählt ist, wendet KES die Ausnahme auf alle App-Komponenten an.

Einen KSWS-Verwendungsbereich können Sie in den Einstellungen der vertrauenswürdigen Zone sowie in den Einstellungen der KSWS-Schutzkomponenten konfigurieren. Aktivieren oder deaktivieren Sie dazu das Kontrollkästchen **Vertrauenswürdige Zone anwenden** im entsprechenden Abschnitt der Richtlinie. In den Einstellungen der KES-Schutzkomponenten gibt es dieses Kontrollkästchen nicht. Das bedeutet, dass der Status der vertrauenswürdigen Zone in individuellen Komponenteneinstellungen bei der Migration verloren geht. Wählen Sie nach Abschluss der Migration die Komponenten aus, für welche die Ausnahme in den Einstellungen der vertrauenswürdigen Zone in der KES-Richtlinie gilt.

Kommentare zur Migration

Kommentare aus der vertrauenswürdigen Zone für KSWS werden unverändert in Kommentare einer KES-Ausnahme migriert.

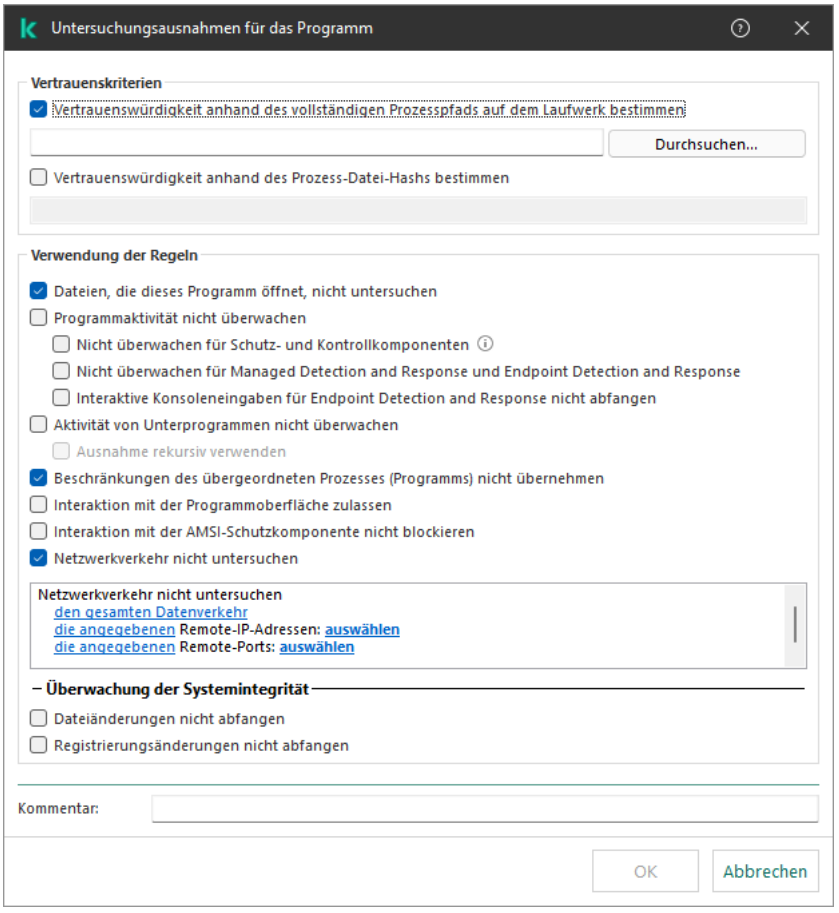
Vertrauenswürdige Prozesse migrieren

Vertrauenswürdige Prozesse von KSWS werden ohne Einschränkungen in vertrauenswürdige Prozesse von KES migriert. Die Migration von vertrauenswürdigen Prozessen ist von der Methode zur Objektauswahl abhängig:

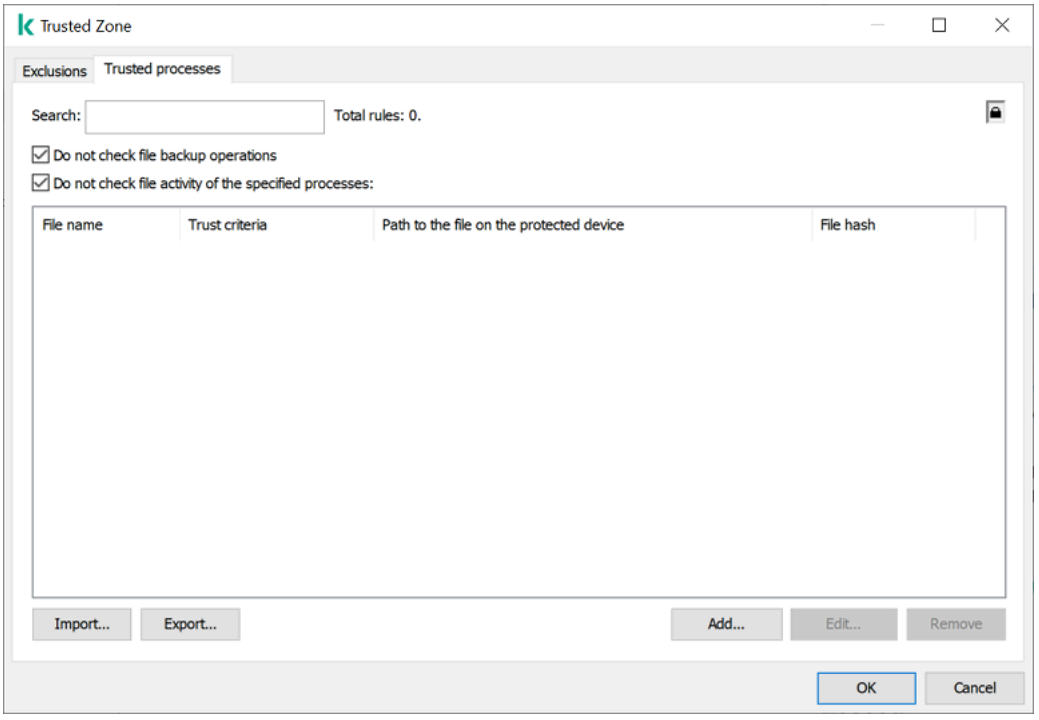
- Pfad der Datei auf dem geschützten Gerät – in die vertrauenswürdigen Anwendungen für KES migrieren.
- Datei-Hash – *nicht migrieren*.

Vertrauenswürdige Prozesse, die KSWS als Datei-Hash konfiguriert hat, werden nicht migriert. Solche vertrauenswürdigen Prozesse müssen Sie nach der Migration manuell hinzufügen.

Wenn das Kontrollkästchen **Datei-Aktivität beim Erstellen eines Backups nicht untersuchen** in den Einstellungen des vertrauenswürdigen Prozesses aktiviert ist, wird diese Einstellung in die vertrauenswürdigen Anwendungen von KES migriert (Kontrollkästchen **Programmaktivität nicht überwachen**).



Einstellungen für vertrauenswürdige Anwendungen für KES



Einstellungen für vertrauenswürdige Prozesse für KSWS

Regeln für die KSWS-Kontrolle des Programmstarts migrieren

Die Standardaktion der KSWS-Kontrolle des Programmstarts ist Blockieren. Das heißt, die Kontrolle des Programmstarts blockiert automatisch alle Programme, die in den Regeln nicht als erlaubte Programme angegeben sind. Daher legt der Migrations-Assistent für die KES-Programmkontrolle automatisch den Kontrollmodus **Allow-Liste** fest, was dem standardmäßigen Blockieren entspricht.

Sie können Regeln von KSWS nach KES migrieren und dazu den *Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben* oder den *Assistenten zum Erstellen einer neuen KES-Richtlinie, die auf der KSWS-Richtlinie basiert* verwenden.

Modus der Kontrolle des Programmstarts migrieren

Der Modus der KSWS-Kontrolle des Programmstarts wird wie folgt zur KES-Kontrolle des Programmstarts migriert:

- **Nur Statistik → Regeln testen**
- **Aktiv → Regeln anwenden**

Vordefinierte Regeln der KSWS-Kontrolle des Programmstarts migrieren

Standardmäßig enthält die KSWS-Kontrolle des Programmstarts zwei Regeln:

- **Start von Skripten und MSI-Paketen, deren Zertifikate im OS als vertrauenswürdig eingestuft sind, erlauben**
- **Ausführbare Datei durch vom Betriebssystem vertrauenswürdiges Zertifikat zulassen**

Vordefinierte Regeln erlauben das Ausführen von *Skripten*, *MSI-Paketen* und *ausführbaren Dateien*, die mit einem vertrauenswürdigen Stammzertifikat signiert sind. Wenn mindestens eine vordefinierte KSWS-Regel den Typ **Erlauben** hat, erstellt der Migrations-Assistent eine neue Erlaubnisregel, **Programme mit vertrauenswürdigen Stammzertifikaten**. Das heißt, die KES Programmkontrolle verwendet eine einzige Regel, um die Ausführung vertrauenswürdiger Skripts, MSI-Pakete und ausführbarer Dateien zuzulassen.

Wenn beide vordefinierten KSWS-Regeln den Typ **Verweigern** haben, ignoriert KES die vordefinierten Regeln.

Benutzerdefinierte Regeln für die KSWS-Kontrolle des Programmstarts migrieren

Die Regeln für die KSWS-Kontrolle des Programmstarts regeln die Ausführung von Dateien nach den folgenden Kriterien:

- Signatur mit digitalem Zertifikat
- SHA256-Hash
- Dateipfad

Regeln werden in KSWS und KES unterschiedlich erstellt, daher erstellt der Migrations-Assistent *Programmkategorien*, die Bedingungen und Ausnahmen von KSWS-Regeln enthalten, und fügt diese Programmkategorien den KES-Regeln hinzu. Der Assistent verwendet in den Programmkategorien die Bedingungen **Zertifikat**, **Ordnerpfad** und **Datei-Hash**. In der Kaspersky Security Center-Verwaltungskonsole im Abschnitt **Programmverwaltung → Programmkategorien** sind neue Programmkategorien verfügbar.

Der Migrations-Assistent gruppiert KSWS-Regeln nach Typ und Benutzer. Danach erstellt der Assistent Programmkategorien, die Bedingungen und Ausnahmen von KSWS-Regeln enthalten, und fügt die Programmkategorien den neuen KES-Regeln hinzu. Der Assistent gibt die Namen der KSWS-Regeln im Feld **Beschreibung** der KES-Regeln an.

Erweiterte Einstellungen der KSWS-Kontrolle des Programmstarts migrieren

Die KSWS-Programmkontrolle und die KES-Programmkontrolle funktionieren unterschiedlich. Daher kann der Migrations-Assistent nur einen Teil der Einstellungen migrieren.

Einstellungen der Kontrolle des Programmstarts

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten	*(wird nicht migriert)* Kaspersky Endpoint Security untersucht das Programm bei jedem Startversuch.
Den Start von Befehlsinterpretern verbieten, wenn kein ausführbarer Befehl vorhanden ist	*(wird nicht migriert)* Kaspersky Endpoint Security erlaubt die Ausführung von Befehlsinterpretern, wenn sie nicht von der „Programmkontrolle“ verboten sind.
Regeln für ausführbare Dateien verwenden	*(wird nicht migriert)* Der Anwendungsbereich der Regel kann nicht in den KES Programmkontroll-Einstellungen konfiguriert werden. Die KES Programmkontrolle wendet Regeln auf alle Dateitypen an: ausführbare Dateien, Skripte und MSI-Pakete. Wenn alle Dateitypen im Anwendungsbereich der Regel in KSWS enthalten sind, übernimmt KES während der Migration die KSWS-Regeln. Wenn ein Dateityp aus dem Anwendungsbereich der Regelanwendung in KSWS ausgeschlossen ist, übernimmt KES während der Migration auch die KSWS-Regeln, aber **Regeln testen** ist als Aktion zur Programmkontrolle ausgewählt.
Laden von DLL-Modulen überwachen	**Laden von DLL-Modulen überwachen (führt zu erheblich erhöhter Systemauslastung)**
Regeln für Skripte und MSI-Pakete verwenden	*(wird nicht migriert)* Der Anwendungsbereich der Regel kann nicht in den KES Programmkontroll-Einstellungen konfiguriert werden. Die KES Programmkontrolle wendet Regeln auf alle Dateitypen an: ausführbare Dateien, Skripte und MSI-Pakete. Wenn alle Dateitypen im Anwendungsbereich der Regel in KSWS enthalten sind, übernimmt KES während der Migration die KSWS-Regeln. Wenn ein Dateityp aus dem Anwendungsbereich der Regel in KSWS ausgeschlossen ist, übernimmt KES während der Migration die KSWS-Regeln, aber **Regeln testen** ist als Aktion zur Programmkontrolle ausgewählt.

Einstellungen für „Kaspersky Security für Windows Server“	Einstellungen für „Kaspersky Endpoint Security für Windows“
Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten	*(wird nicht migriert)* Kaspersky Endpoint Security berücksichtigt die Reputation von Programmen nicht, sondern erlaubt oder verweigert die Ausführung von Programmen gemäß den Regeln.
Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben	Während der Migration fügt KES eine neue Erlaubnisregel hinzu. Die KL-Kategorie **Andere Programme\Programme, die laut KSN-Reputation vertrauenswürdig sind** ist als Auslösebedingung der Regel angegeben.
Benutzer und / oder Benutzergruppen, denen der Start von laut KSN vertrauenswürdigen Programmen erlaubt ist	**Benutzer und deren Rechte** in einer Erlaubnisregel der Programmkontrolle, die die KL-Kategorie **Andere Programme\Programme, die laut KSN-Reputation vertrauenswürdig sind** enthält.
Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben	Die Softwareverteilungssteuerung in KSWS und KES funktioniert unterschiedlich. Während der Migration fügt KES neue Erlaubnisregeln für Programme hinzu, für die die automatische Softwareverteilung zugelassen ist. Als regelauslösende Bedingung wird der Datei-Hash angegeben.
Verteilung von Programmen mittels Windows Installer immer erlauben	Die Softwareverteilungssteuerung in KSWS und KES funktioniert unterschiedlich. Während der Migration fügt KES neue Erlaubnisregeln für Programme hinzu, für die die automatische Softwareverteilung zugelassen ist (**Erlaubte Programme und Pakete für die Software-Verteilung**). Als regelauslösende Bedingung wird der Datei-Hash angegeben. In den Kontoeigenschaften ist das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen** aktiviert.
Verteilung von Programmen mittels SCCM unter Verwendung des Background Intelligent Transfer Service (BITS) immer erlauben	*(wird nicht migriert)*
Liste der erlaubten Programme und Installationspakete	Die Softwareverteilungssteuerung in KSWS und KES funktioniert unterschiedlich. Während der Migration fügt KES neue Erlaubnisregeln für Programme hinzu, für die die automatische Softwareverteilung zugelassen ist. Als regelauslösende Bedingung wird der Datei-Hash angegeben. In den Kontoeigenschaften ist das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen** aktiviert.
Zeitplan-Einstellungen	*(wird nicht migriert)* Wenn in den KSWS-Einstellungen ein Zeitplan für die Komponente konfiguriert ist, wird die Komponente „Programmkontrolle“ bei der Migration aktiviert. Wenn in den KSWS-Einstellungen kein Zeitplan für die Komponente konfiguriert ist, wird die Komponente „Programmkontrolle“ bei der Migration deaktiviert. Es kann kein separater Zeitplan für die Komponente konfiguriert werden. Die Komponente ist immer aktiviert, während Kaspersky Endpoint Security in Betrieb ist.

Installation von KES anstelle von KSWS

Sie können Kaspersky Endpoint Security wie folgt installieren:

- Installation von KES nach dem Entfernen von KSWS (empfohlen).
- Installation von KES über KSWS.

Deinstallation von Kaspersky Security für Windows Server

Sie können das Programm entweder per Fernzugriff mithilfe der Aufgabe *Remote-Deinstallation einer Anwendung* oder lokal auf dem Server entfernen. Möglicherweise müssen Sie den Server neu starten, nachdem KSWS entfernt wurde. Wenn Sie Kaspersky Endpoint Security ohne Neustart installieren möchten, stellen Sie sicher, dass Kaspersky Security für Windows Server vollständig entfernt wurde. Wenn das Programm nicht vollständig entfernt wird, kann die Installation von Kaspersky Endpoint Security zu Fehlern auf den Servern führen. Auch bei Verwendung des Dienstprogramms kavremover muss nachgeprüft werden, ob das Programm vollständig entfernt wurde. Das Dienstprogramm kavremover unterstützt die Verwaltung von KSWS nicht.

> Wenn der Kennwortschutz aktiviert ist, um den Zugriff auf KSWS einzuschränken, geben Sie das Deinstallationskennwort in den Einstellungen des KES-Installationspakets ein.

Nachdem Sie KSWS entfernt haben, installieren Sie Kaspersky Endpoint Security für Windows mithilfe einer der verfügbaren Methoden.

Kaspersky Endpoint Security installieren

Wenn Sie KES aus der Ferne installieren, werden die Komponenten, die Sie in den Eigenschaften des Installationspakets ausgewählt haben, auf dem Server installiert. Wir empfehlen, die Standardkomponenten in den Eigenschaften des Installationspakets auszuwählen. Wenn KES über KSWS installiert wird, ist kein Neustart erforderlich.

Vor der lokalen Installation überprüft Kaspersky Endpoint Security, ob andere Kaspersky-Programme auf dem Computer vorhanden sind. Wenn Kaspersky Security für Windows Server auf dem Computer installiert ist, erkennt KES die installierten KSWS-Komponenten und wählt die gleichen Komponenten zur Installation aus. Wenn KES über KSWS installiert wird, ist kein Neustart erforderlich.

> Sollte die Installation von KES über KSWS fehlschlagen, können Sie die Installation rückgängig machen. Nachdem die Installation zurückgesetzt wurde, müssen Sie den Server neu starten. Danach können Sie den Versuch wiederholen.

KSWS-Einstellungen und -Aufgaben werden bei der Installation von „Kaspersky Endpoint Security für Windows“ nicht migriert. Um Einstellungen und Aufgaben zu migrieren, führen Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben aus.

Die Liste der installierten Komponenten können Sie wie folgt überprüfen: im Abschnitt **Sicherheit** auf der Benutzeroberfläche des Programms, mithilfe des Befehls `status` oder in der Kaspersky Security Center-Konsole in den Computereigenschaften. Nach der Installation können Sie die Komponentenauswahl ändern, indem Sie die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Migration der Konfiguration [KSWS+KEA] zur Konfiguration [KES+built-in agent]

Zur Unterstützung von Kaspersky Endpoint Security für Windows als Teil von EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA und MDR wurde dem Programm ein integrierter Agent hinzugefügt. Das separate Programm „Kaspersky Endpoint Agent“ ist nicht mehr erforderlich, um diese Lösungen zu nutzen.

Bei der Migration von KSWS zu KES funktionieren die Lösungen EDR (KATA), EDR Optimum, EDR Expert, Kaspersky Sandbox, KUMA und MDR weiterhin mit den integrierten Agents von Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt.

Die Migration der Konfiguration [KSWS+KEA] zu [KES+built-in agent] umfasst die folgenden Schritte:

1. **Migration von KSWS zu KES**

   Die Migration von KSWS zu KES beinhaltet die Installation von Kaspersky Endpoint Security anstelle von Kaspersky Security für Windows Server.

   Gewöhnlich aktivieren Administratoren den Kennwortschutz, um den Zugriff auf KSWS und KEA einzuschränken. Ab Kaspersky Security Center Linux 15.1 können Sie das Kennwort für die Deinstallation des Programms in den Einstellungen der Aufgabe *Remote-Installation einer Anwendung* eingeben. Für die Aufgabe kann nur ein einziges Deinstallationskennwort eingegeben werden. Wenn für KSWS und KEA dasselbe Kennwort festgelegt wurde, werden die Anwendungen KSWS und KEA erfolgreich entfernt. Wenn sich die Kennwörter unterscheiden, schlägt das Entfernen einer dieser Anwendungen wegen eines Zugriffsfehlers fehl. Um die Migration abzuschließen, müssen Sie den Kennwortschutz für die Anwendung deaktivieren, deren Kennwort Sie nicht in den Einstellungen der Aufgabe *Remote-Installation einer Anwendung* eingeben konnten.

   Um die Migration durchzuführen, müssen Sie die Komponenten auswählen, die zur Unterstützung der Detection and Response-Lösungen als Teil von Kaspersky Endpoint Security erforderlich sind. Nach der Installation des Programms wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

2. **Migration der Richtlinie und der Aufgaben**

   Die Migration der Richtlinien und Aufgaben von [KSWS+KEA] zu [KES+built-in agent] umfasst die folgenden Schritte:

   1. Migrieren von Richtlinien und Aufgaben von KSWS zu KES mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (nur in der Verwaltungskonsole (MMC) verfügbar).

      Dadurch wird ein Richtlinienprofil mit dem Namen *UpgradedFromKSWS <Name der Richtlinie von Kaspersky Security für Windows Server>* zu der KES-Richtlinie hinzugefügt. Außerdem werden neue KES-Aufgaben mit den Namen *<Name der KSWS-Aufgabe> (umgewandelt)* erstellt.

   2. Migrieren von Richtlinien und Aufgaben von KEA zu KES mit dem Assistenten für die Migration von Kaspersky Endpoint Agent (nur in Web Console und Cloud Console verfügbar).

      Dadurch wird eine neue Richtlinie mit dem Namen *<Name der Kaspersky Endpoint Security-Richtlinie> & <Name der Kaspersky Endpoint Agent-Richtlinie>* erstellt. Außerdem werden neue Aufgaben und KES-Aufgaben erstellt.

3 Lizenzverwaltung

Wenn Sie eine gewöhnliche Lizenz für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security zur Aktivierung von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Agent verwenden, wird die Funktionalität „EDR Optimum“ nach dem Upgrade des Programms auf Version 11.7.0 automatisch aktiviert. Sie müssen keine zusätzlichen Aktionen ausführen.

Wenn Sie eine eigenständige Lizenz für das Kaspersky Endpoint Detection and Response Optimum-Add-on zur Aktivierung der EDR Optimum-Funktionalität verwenden, müssen Sie sicherstellen, dass der Schlüssel für das EDR Optimum-Add-on zur Kaspersky Security Center-Datenverwaltung hinzugefügt wird und dass die Funktionalität zur automatischen Verteilung von Lizenzschlüsseln aktiviert ist. Nach dem Upgrade des Programms auf Version 11.7.0 wird die Funktionalität „EDR Optimum“ automatisch aktiviert.

Wenn Sie Kaspersky Endpoint Agent mit einer Lizenz für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security aktivieren und eine andere Lizenz zur Aktivierung von Kaspersky Endpoint Security für Windows verwenden, müssen Sie den Schlüssel für Kaspersky Endpoint Security für Windows mit dem gewöhnlichen Schlüssel für Kaspersky Endpoint Detection and Response Optimum oder Kaspersky Optimum Security ersetzen. Sie können den Schlüssel mithilfe der Aufgabe *Schlüssel hinzufügen* ersetzen.

Die Funktionalität „Kaspersky Sandbox“ muss nicht aktiviert werden. Kaspersky Sandbox ist sofort nach dem Upgrade und der Aktivierung von Kaspersky Endpoint Security für Windows verfügbar.

Zum Aktivieren von Kaspersky Endpoint Security als Teil der Kaspersky Anti Targeted Attack Platform-Lösung kann nur die Lizenz von Kaspersky Anti Targeted Attack Platform verwendet werden. Nach dem Upgrade der App auf Version 12.1 wird die Funktionalität EDR (KATA) automatisch aktiviert. Sie müssen keine zusätzlichen Aktionen ausführen.

4 Status von Kaspersky Endpoint Detection and Response Optimum und Kaspersky Sandbox überprüfen

Falls der Computer nach dem Upgrade in der Kaspersky Security Center-Konsole den Status *Kritisch* hat:

- Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
- Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*.
- Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

Stellen Sie mithilfe der Option *Bericht über den Status der Programmkomponenten* sicher, dass die EDR Optimum-Funktionalität aktiviert ist. Wird für eine Komponente der Status *Nicht durch Lizenz abgedeckt* angezeigt wird, stellen Sie sicher, dass die Funktionalität zur automatischen Verteilung von Lizenzschlüsseln in EDR Optimum aktiviert ist.

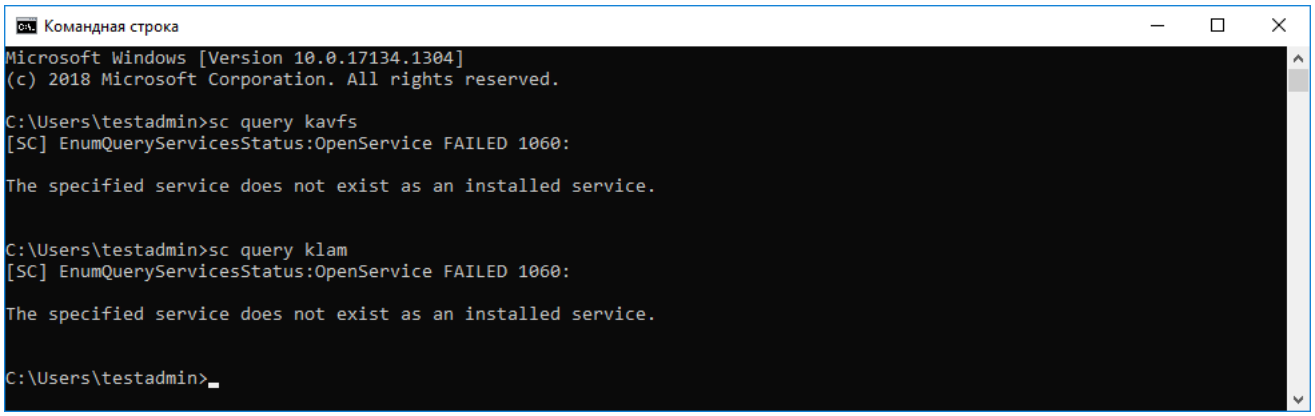
Überprüfen, ob Kaspersky Security für Windows Server erfolgreich entfernt wurde

Vergewissern Sie sich, dass Kaspersky Security für Windows Server vollständig entfernt wurde:

- Der Ordner `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` ist nicht vorhanden.
- Die folgenden Dienste werden nicht vorhanden:
  - Kaspersky Security Service (KAVFS)
  - Dienst Kaspersky Security Management (KAVFSGT)
  - Dienst Kaspersky Security Exploit Prevention (KAVFSSLP)
  - Dienst Kaspersky Security Script Checker (KAVFSSCS)

  Sie können die ausgeführten Dienste im Task-Manager oder mithilfe des Befehls `sc query` überprüfen (siehe Abbildung unten).
- Die folgenden Treiber werden nicht vorhanden:
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys
  - klips.sys
  - klids.sys
  - klwtpee

Sie können die installierten Treiber im Ordner `C:\Windows\System32\drivers` nachsehen oder mithilfe des Befehls `sc query` überprüfen. Wenn ein Dienst oder Treiber fehlt, erhalten Sie die folgende Antwort:



Überprüfen, ob die Dienste und Treiber von Kaspersky Security für Windows Server erfolgreich entfernt wurden

Wenn Programm- oder Treiberdateien auf dem Server verblieben sind, löschen Sie die entsprechenden Dateien manuell. Wenn immer noch Dienste von Kaspersky Security für Windows Server auf dem Server ausgeführt werden, beenden (`sc stop`) und löschen (`sc delete`) Sie die Dienste manuell. Um den Treiber klam.sys driver zu stoppen, können Sie den Befehl `fltmc unload klam` verwenden.

Aktivieren von KES mit einem KSWS-Schlüssel

Nach der Installation des Programms können Sie „Kaspersky Endpoint Security für Windows“ (KES) mit einem Lizenzschlüssel für „Kaspersky Security für Windows Server“ (KSWS) aktivieren. Der Aktivierungsvorgang nach der Migration hängt von der KSWS-Aktivierungsmethode ab (siehe Tabelle unten).

Die *Lizenz für Kaspersky Security for Storage* wird von Kaspersky Endpoint Security nicht unterstützt. Um mit dieser Lizenz zu arbeiten, müssen Sie Kaspersky Security für Windows Server verwenden.

Um KES mit dem KSWS-Schlüssel zu aktivieren, können Sie nur den Aktivierungscode verwenden. Wenn Sie eine Schlüsseldatei zur Programmaktivierung verwenden, müssen Sie den Technischen Support kontaktieren und eine Schlüsseldatei für Kaspersky Endpoint Security anfordern.

Aktivieren von „Kaspersky Endpoint Security für Windows“ mit einem Schlüssel für „Kaspersky Security für Windows Server“

Aktivierungsmethode für „Kaspersky Security für Windows Server“	Migration des Schlüssels für Kaspersky Endpoint Security für Windows.
Automatische Verteilung des KSWS-Lizenzschlüssels an andere Computer.	Ist die automatische Schlüsselverteilung in den Eigenschaften des KSWS-Lizenzschlüssels aktiviert, so wird KES automatisch mit dem KSWS-Schlüssel aktiviert.
Der KSWS-Schlüssel wird mithilfe einer Aufgabe hinzugefügt.	Wird KSWS über die Aufgabe aktiviert, so wird der KSWS-Lizenzschlüssel während der Migration aus KSWS gelöscht. Sie müssen das Programm erneut aktivieren. Sie können zum Beispiel einen Lizenzschlüssel zum Installationspaket für „Kaspersky Endpoint Security für Windows“ hinzufügen.
Der KSWS-Schlüssel wird lokal über die Programmoberfläche hinzugefügt.	Wird KSWS lokal über den Assistenten zur Programmaktivierung aktiviert, so wird der KSWS-Lizenzschlüssel während der Migration aus KSWS gelöscht. Sie müssen das Programm erneut aktivieren. Sie können zum Beispiel einen Lizenzschlüssel zum Installationspaket für „Kaspersky Endpoint Security für Windows“ hinzufügen.
Der KSWS-Schlüssel wird dem Installationspaket hinzugefügt.	Wird KSWS mithilfe des Schlüssels aus dem Installationspaket aktiviert, so wird der KSWS-Lizenzschlüssel während der Migration aus KSWS gelöscht. Sie müssen das Programm erneut aktivieren. Sie können zum Beispiel einen Lizenzschlüssel zum Installationspaket für „Kaspersky Endpoint Security für Windows“ hinzufügen.

Aktivierungsmethode für „Kaspersky Security für Windows Server“	Migration des Schlüssels für Kaspersky Endpoint Security für Windows.
Kostenpflichtiges Image einer virtuellen Maschine (Amazon Machine Image – AMI) bei Amazon Web Services (AWS).	Wenn Sie Kaspersky Security Center als kostenpflichtiges Image einer virtuellen Maschine (Amazon Machine Image – AMI) bei Amazon Web Services (AWS) erworben haben, muss KES nicht aktiviert werden. In diesem Fall verwendet Kaspersky Security Center das AVS-Abonnement, das bereits zum Programm hinzugefügt wurde.
Vorgefertigtes kostenloses Kaspersky Security Center-Image mit Verwendung Ihrer eigenen Lizenz (Bring Your Own License – BYOL-Modell).	Wenn Sie ein sofort einsatzbereites kostenloses Kaspersky Security Center-Image mit Ihrer eigenen Lizenz in einer Cloud-Umgebung verwenden (Bring Your Own License – BYOL-Modell), müssen Sie die App aktivieren. Dazu können Sie eine beliebige verfügbare Methode verwenden. Sie benötigen eine Lizenz für Kaspersky Hybrid Cloud Security.

Spezielle Aspekte für die Migration von Servern mit hoher Auslastung

Auf Servern mit hoher Auslastung ist es besonders wichtig, die Leistung zu überwachen und Störungen zu vermeiden. Nach der Migration zu Kaspersky Endpoint Security für Windows empfehlen wir, jene Programmkomponenten, die die Serverressourcen relativ stark beanspruchen, vorübergehend zu deaktivieren. Nachdem Sie sichergestellt haben, dass der Server ordnungsgemäß funktioniert, können Sie die Programmkomponenten wieder aktivieren.

Für die Migration von Servern mit hoher Auslastung empfehlen wir folgendes Vorgehen:

1. Erstellen Sie eine Richtlinie für Kaspersky Endpoint Security mit den Standardeinstellungen.

   Die Standardeinstellungen gelten als optimal. Diese Einstellungen werden von den Kaspersky-Experten empfohlen. Die Standardeinstellungen bieten das empfohlene Schutzniveau und eine optimale Ressourcennutzung.

2. Deaktivieren Sie in den Richtlinieneinstellungen die folgenden Komponenten: Schutz vor Netzwerkbedrohungen, Verhaltensanalyse, Exploit-Prävention, Rollback von schädlichen Aktionen, Programmkontrolle.

   Wenn in Ihrem Unternehmen die Lösung Kaspersky Managed Detection and Response (MDR) bereitgestellt wird, laden Sie die BLOB-Konfigurationsdatei in die Richtlinie von Kaspersky Endpoint Security hoch.

3. Entfernen Sie Kaspersky Security für Windows Server vom Server.

4. Installieren Sie Kaspersky Endpoint Security für Windows mit den Standardkomponenten.

   Wenn in Ihrem Unternehmen Detection and Response-Lösungen bereitgestellt werden, wählen Sie die entsprechenden Komponenten in den Eigenschaften des Installationspakets aus.

5. Überprüfen Sie die Standardeinstellungen des Programms:

   - Das Programm wird mit dem KSWS-Lizenzschlüssel aktiviert.
   - Die neue Richtlinie wird angewendet. Zuvor ausgewählte Komponenten werden deaktiviert.

6. Stellen Sie sicher, dass der Server funktioniert. Stellen Sie sicher, dass Kaspersky Endpoint Security für Windows maximal 1 % der Serverressourcen verwendet.

7. Führen Sie bei Bedarf die folgenden Aktionen aus: Untersuchungsausnahmen erstellen, vertrauenswürdige Apps hinzufügen, eine Liste mit vertrauenswürdigen Webadressen erstellen.

8. Aktivieren Sie die Komponenten „Verhaltensanalyse“, „Exploit-Prävention“ und „Rollback von schädlichen Aktionen“. Stellen Sie sicher, dass Kaspersky Endpoint Security für Windows maximal 1 % der Serverressourcen verwendet.

9. Aktivieren Sie die Komponente „Schutz vor Netzwerkbedrohungen“. Stellen Sie sicher, dass Kaspersky Endpoint Security für Windows maximal 2 % der Serverressourcen verwendet.

10. Aktivieren Sie die Komponente „Programmkontrolle“ im Regeltest-Modus.

11. Stellen Sie sicher, dass die „Programmkontrolle“ funktioniert. Fügen Sie bei Bedarf neue Regeln für die „Programmkontrolle“ hinzu und deaktivieren Sie den Regeltest-Modus, nachdem Sie sichergestellt haben, dass die „Programmkontrolle“ funktioniert.

Überprüfen Sie nach der Migration von KSWS zu KES, ob das Programm ordnungsgemäß funktioniert. Überprüfen Sie den Status des Servers in der Konsole (erforderlicher Status: *OK*). Stellen Sie sicher, dass keine Fehler für das Programm gemeldet wurden. Überprüfen Sie außerdem den Zeitpunkt der letzten Verbindung zum Administrationsserver, den Zeitpunkt des letzten Datenbanken-Updates und den Status des Serverschutzes.

Verwaltung der App auf einem Server im Server Core-Modus

Ein Server im Server Core-Modus hat keine Benutzeroberfläche. Sie können die Anwendung also nur per Fernzugriff über die Kaspersky Security Center-Konsole oder lokal über die Befehlszeile verwalten.

Verwaltung der Anwendung über die Kaspersky Security Center-Konsole

Die Installation der Anwendung über die Kaspersky Security Center-Konsole unterscheidet sich nicht von der gewöhnlichen Installation. Wenn Sie ein Installationspaket erstellen, können Sie einen Lizenzschlüssel hinzufügen, um die Anwendung zu aktivieren. Sie können einen Schlüssel für Kaspersky Endpoint Security für Windows oder einen Schlüssel für Kaspersky Security für Windows Server verwenden.

> Auf einem Server im Server Core-Modus sind die folgenden App-Komponenten nicht verfügbar: Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Web-Kontrolle, Schutz vor modifizierten USB-Geräten, Verschlüsselung von Dateien (FLE), Kaspersky-Festplattenverschlüsselung (FDE).

Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein. Die Anwendung kann kein Fenster anzeigen, das den Benutzer zum Neustart des Servers auffordert. Ob ein Neustart des Servers erforderlich ist, können Sie den Berichten in der Kaspersky Security Center-Konsole entnehmen.

Die Verwaltung der App auf einem Server im Server Core-Modus unterscheidet sich nicht von der Verwaltung auf einem Computer. Sie können Richtlinien und Aufgaben verwenden, um die Anwendung zu konfigurieren.

Für die Verwaltung der App auf einem Server im Server Core-Modus sind folgende Aspekte zu berücksichtigen:

- Der Server im Server Core-Modus hat keine Benutzeroberfläche. Deshalb zeigt Kaspersky Endpoint Security keine Warnung an, die den Benutzer über eine notwendige erweiterte Desinfektion informiert. 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*. Dann müssen Sie eine Aufgabe *Schadsoftware-Untersuchung* starten.

- Die BitLocker-Laufwerkverschlüsselung ist nur mit einem Trusted Platform Module (TPM) verfügbar. Für die Verschlüsselung kann keine PIN bzw. kein Passwort verwendet werden, da das Programm das Kennwortabfragefenster für die Preboot-Authentifizierung nicht anzeigen kann. Wenn für das Betriebssystem der FIPS-Kompatibilitätsmodus (Federal Information Processing Standard) aktiviert ist, verbinden Sie einen Wechseldatenträger zum Speichern des Chiffrierschlüssels, bevor Sie mit der Verschlüsselung des Laufwerks beginnen.

Programm über die Befehlszeile verwalten

Wenn keine Benutzeroberfläche verfügbar ist, können Sie Kaspersky Endpoint Security über die Befehlszeile verwalten.

Um die App auf einem Server im Server Core-Modus zu installieren, führen Sie den folgenden Befehl aus:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

Um die Anwendung zu aktivieren, führen Sie den folgenden Befehl aus:

```
avp.com license /add <activation code or key file>
```

Um die Statuswerte des Anwendungsprofils zu überprüfen, führen Sie den folgenden Befehl aus:

```
avp.com status
```

Um eine Liste der Befehle für die Anwendungsverwaltung anzuzeigen, führen Sie den folgenden Befehl aus:

```
avp.com help
```

Migration von [KSWS+KEA] zu [KES+built-in agent]

Bei der Migration von Kaspersky Security für Windows Server (KSWS) zu Kaspersky Endpoint Security (KES) können Sie wie folgt den Serverschutz konfigurieren und die Leistung optimieren. Hier sehen wir uns ein Migrationsbeispiel für ein einzelnes Unternehmen an.

Infrastruktur des Unternehmens

Das Unternehmen setzt die folgenden Komponenten ein:

- Kaspersky Security Center 14.2

  Der Administrator verwaltet Kaspersky-Lösungen über die Verwaltungskonsole (MMC). Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) ist ebenfalls bereitgestellt.

  In Kaspersky Security Center werden drei Administrationsgruppen erstellt, die die Server des Unternehmens enthalten: zwei Administrationsgruppen für SQL-Server und eine Administrationsgruppe für Microsoft Exchange-Server. Jede Administrationsgruppe wird durch eine eigene Richtlinie verwaltet. Die Aufgaben *Datenbanken-Update* und *Untersuchung auf Befehl* werden für alle Server des Unternehmens erstellt.

  Der KSWS-Aktivierungsschlüssel wird zu Kaspersky Security Center hinzugefügt. Die automatische Schlüsselverteilung ist aktiviert.

- SQL-Server, auf denen Kaspersky Security für Windows Server 11.0.1 und Kaspersky Endpoint Agent 3.11 installiert sind. Die SQL-Server werden in zwei Cluster zusammengefasst.

  KSWS wird durch die Richtlinien *SQL_Policy(1)* und *SQL_Policy(2)* verwaltet. Die Aufgaben *Datenbanken-Update* und *Untersuchung auf Befehl* werden erstellt.

- Ein Microsoft Exchange-Server, auf dem Kaspersky Security für Windows Server 11.0.1 und Kaspersky Endpoint Agent 3.11 installiert sind.

  KSWS wird durch die Richtlinie *Exchange_Policy* verwaltet. Die Aufgaben *Datenbanken-Update* und *Untersuchung auf Befehl* werden erstellt.

Planung der Migration

Die Migration umfasst die folgenden Schritte:

1. Migration der KSWS-Aufgaben und -Richtlinien über den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben.
2. Migration der Kaspersky Endpoint Agent-Richtlinie über den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben.
3. Verwenden von Tags zum Aktivieren von Richtlinienprofilen in den Eigenschaften der neuen Richtlinie.
4. Installation von KES anstelle von KSWS.
5. Aktivierung von EDR Optimum.
6. Überprüfen, ob KES funktioniert.

Das Migrationsszenario wird zunächst auf einem der Cluster für SQL-Server durchgeführt. Dann wird das Migrationsszenario auf dem anderen Cluster für SQL-Server durchgeführt. Anschließend wird das Migrationsszenario auf dem Microsoft Exchange durchgeführt.

Migration der KSWS-Aufgaben und -Richtlinien mithilfe des Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben

Zur Migration von KSWS-Aufgaben können Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben verwenden. Dadurch erhalten Sie anstatt der Richtlinien *SQL_Policy(1)*, *SQL_Policy(2)* und *Exchange_Policy* eine einzige Richtlinie mit drei Profilen für SQL- bzw. Microsoft Exchange-Server. Das neue Richtlinienprofil mit den KSWS-Einstellungen erhält den Namen *UpgradedFromKSWS<Name der Richtlinie für Kaspersky Security für Windows Server>*. In den Profileigenschaften wählt der Migrations-Assistent automatisch das Geräte-Tag `UpgradedFromKSWS` als Auslösekriterium aus. Dadurch werden die Einstellungen aus dem Richtlinienprofil automatisch auf die Server angewendet.

Migration der Kaspersky Endpoint Agent-Richtlinie über den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben

Zur Migrieren von Kaspersky Endpoint Agent-Richtlinien können Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben verwenden. Der Migrations-Assistent für Richtlinien und Aufgaben für Kaspersky Endpoint Agent ist nur in der Web Console verfügbar.

Verwenden von Tags zum Aktivieren von Richtlinienprofilen in den Eigenschaften der neuen Richtlinie

Wählen Sie das Geräte-Tag aus, das Sie zuvor als die Aktivierungsbedingung für das Profil zugewiesen haben. Öffnen Sie die Richtlinieneigenschaften und wählen Sie sie *Allgemeinen Regeln zur Aktivierung von Richtlinienprofilen* als Bedingung für die Profilaktivierung aus.

Installation von KES anstelle von KSWS

Vor der Installation von KES müssen Sie den Kennwortschutz in den KSWS-Richtlinieneigenschaften deaktivieren.

Die Installation von KES umfasst die folgenden Schritte:

1. Bereiten Sie das Installationspaket vor. Wählen Sie in den Eigenschaften des Installationspakets das Programmpaket für Kaspersky Endpoint Security für Windows 12.0 und die Standardauswahl der Komponenten aus.
2. Erstellen Sie eine Aufgabe *Remote-Installation einer Anwendung* für eine der SQL Server-Administrationsgruppen.
3. Wählen Sie in den Aufgabeneigenschaften das Installationspaket und die Lizenzschlüsseldatei aus.
4. Warten Sie, bis die Aufgabe erfolgreich abgeschlossen wurde.
5. Wiederholen Sie die KES-Installation für die übrigen Administrationsgruppen.

Nachdem die KES-Installation abgeschlossen wurde, fügt Kaspersky Security Center automatisch das Tag `UpgradedFromKSWS` zu den Namen von Computern auf der Konsole hinzu.

Die KES-Installation können Sie anhand des *Berichts über die Bereitstellung des Schutzes* überprüfen. Außerdem können Sie den Gerätestatus überprüfen. Die Programmaktivierung können Sie anhand des *Berichts über die Lizenzschlüsselnutzung* überprüfen.

Aktivierung von EDR Optimum

Sie können die Funktionalität von EDR Optimum mit einer eigenständigen Add-on-Lizenz für Kaspersky Endpoint Detection and Response Optimum aktivieren. Sie müssen überprüfen, ob der EDR Optimum-Schlüssel zur Kaspersky Security Center-Datenverwaltung hinzugefügt wurde und ob die Funktionalität zur automatischen Lizenzschlüsselverteilung aktiviert ist.

Die Aktivierung von EDR Optimum können Sie anhand des *Bericht über den Status der Programmkomponenten* überprüfen.

Überprüfen, ob KES funktioniert

Um die korrekte Funktion von KES zu überprüfen, sehen Sie nach, ob keine Fehler gemeldet werden. Erforderlicher Gerätestatus: *OK*. Update- und Untersuchungsaufgaben wurden erfolgreich abgeschlossen.

Light Agent-Modus zum Schutz virtueller Maschinen

Ab Version 12.8 können Sie Kaspersky Endpoint Security für Windows als Teil von Kaspersky Security for Virtualization Light Agent verwenden. *Kaspersky Security for Virtualization Light Agent* ist eine integrierte Lösung. Sie schützt virtuelle Maschinen umfassend vor verschiedenen Bedrohungen der Informationssicherheit, Netzwerkangriffen und Phishing-Angriffen. Um diese Lösung zu verwenden, müssen Sie das Programm im Light Agent-Modus installieren.

Die Installation von Kaspersky Endpoint Security im Light Agent-Modus auf Arm-basierten virtuellen Maschinen wird nicht unterstützt.

Sie können Kaspersky Endpoint Security im Light Agent-Modus als Teil von Kaspersky Security for Virtualization Light Agent ab Version 6.2 verwenden.

Wenn Sie Light Agent starten, stellt Light Agent eine Verbindung zu der virtuellen Maschine SVM (Secure Virtual Machine) her und hält die Verbindung aufrecht. Auf der SVM wird ein Schutzserver bereitgestellt. Die *Schutzserver* ist eine Komponente der Lösung Kaspersky Security for Virtualization Light Agent. Sie untersucht Dateien auf Viren und andere Schadsoftware, aktualisiert die Antiviren-Datenbanken und verwaltet die Lizenzschlüssel. Light Agent sendet Dateien oder deren Fragmente, die untersucht werden müssen, an die SVM. Die Untersuchungsergebnisse sind für alle virtuellen Maschinen verfügbar, auf denen Light Agent installiert ist (SharedCache-Technologie). Diese Technologie erhöht die Effizienz der Lösung und ermöglicht eine schnellere Reaktion auf Bedrohungen.

In der Infrastruktur des Unternehmens kann es viele virtuelle Maschinen mit installiertem Light Agent und viele SVMs geben. Der Integrationsserver verwaltet die Interaktion zwischen virtuellen Maschinen und SVMs. Der *Integrationsserver* ist eine Komponente der Lösung Kaspersky Security for Virtualization Light Agent, die eine Liste der verfügbaren SVMs erstellt und diese Daten an Light Agents überträgt, an der Erkennung von SVMs durch Light Agents beteiligt ist, die Verbindung zwischen Light Agents und SVMs schützt und weitere Funktionen ausführt.

Besonderheiten für den Light Agent-Modus

Sie können Kaspersky Endpoint Security im Standard-Modus und Light Agent-Modus mithilfe der Richtlinien und Aufgaben von Kaspersky Endpoint Security verwalten. Im Light Agent-Modus sind einige Komponenten und Funktionen des Programms nicht verfügbar.

Update der Datenbanken und Programm-Module

Kaspersky Endpoint Security verwendet im Light Agent-Modus spezielle Malware-Datenbanken. Diese Datenbanken sind für die Ausführung des Programms im Rahmen von Kaspersky Security for Virtualization Light Agent erforderlich. Kaspersky Endpoint Security erhält vom Schutzserver Updates für die Datenbanken und Programm-Module.

Die Datenbanken und Module auf geschützten virtuellen Maschinen werden mithilfe einer speziellen Update-Aufgabe zum *Update der Datenbanken und Programm-Module* aktualisiert, bei der ein Ordner auf der SVM als Update-Quelle angegeben wird. Light Agent führt die Aufgabe *Update der Datenbanken und Programm-Module* automatisch aus. Sie können keine andere Update-Quelle auswählen, den Aufgabenzeitplan nicht konfigurieren oder die Aufgabe nicht entfernen.

Auch das Rollback des neuesten Updates der Malware-Datenbanken auf dem Schutzserver durchgeführt. Nach dem Rollback eines Updates der Datenbanken und Programm-Module auf der SVM wird auf der geschützten virtuellen Maschine eine spezielle lokale Aufgabe *Update der Datenbanken und Programm-Module* gestartet. Dadurch kehrt der Light Agent zur Verwendung der vorherigen Auswahl der Malware-Datenbanken zurück.

Im Light Agent-Modus wird die Aufgabe *Update-Rollback* von Kaspersky Endpoint Security nicht unterstützt.

Light Agent aktivieren

Zur Aktivierung des Programms müssen Sie der SVM, mit der der Light Agent verbunden ist, einen Lizenzschlüssel hinzufügen. Sie müssen das Programm nicht separat aktivieren.

Weitere Besonderheiten für den Light Agent-Modus

- Wenn Sie eine Richtlinie für das Programm erstellen, sollten Sie den Light Agent-Modus auswählen. In diesem Modus fordert Sie der Assistent für neue Richtlinien auf, die SVM-Verbindung zu konfigurieren. Diese Einstellungen sind erforderlich, damit das Programm im Light Agent-Modus funktioniert.
- Im Light Agent-Modus können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht installieren. Die Auswahl der Komponenten ist vom Typ des Gastbetriebssystems abhängig: Workstation oder Server.
- Light Agent unterstützt die Integration mit den Lösungen Kaspersky Endpoint Detection and Response Expert und Kaspersky Endpoint Detection and Response Expert (Cloud) nicht.
- Sie können Light Agent über die Verwaltungskonsole (MMC) und die Kaspersky Security Center Web Console verwalten. Light Agent kann nicht im Programm Kaspersky Security Center Cloud Console verwaltet werden.
- Das Ändern der Auswahl der Programmkomponenten auf virtuellen VDI-Maschinen wird nicht unterstützt.
- Kaspersky Endpoint Security kommuniziert über den KSN-Proxyserver mit den KSN-Servern. Die direkte Interaktion mit KSN wird nicht unterstützt.
- Der Cloud-Modus von Kaspersky Security Network wird nicht unterstützt.
- Die Verwendung des Proxyservers des Programms beim Herstellen einer Verbindung mit dem Integrationsserver (VIIS), dem Schutzserver (SVM) und den KSN-Servern wird nicht unterstützt.

Vorherige Konfiguration der virtuellen Maschine

Sie können Kaspersky Endpoint Security auf einer virtuellen Maschine installieren, die eine Technologie für virtuelle Plattformen verwendet. Kaspersky Endpoint Security unterstützt virtuelle Plattformen von VMware, Microsoft Hyper-V und Citrix. Vor der Installation müssen Sie die virtuellen Maschinen zuerst konfigurieren.

Kompatibilität mit der Citrix App Layering-Technologie

Wenn Sie beabsichtigen, Full User Layer zu verwenden, um den Status der temporären virtuellen Maschinen zu speichern, müssen Sie vor der Installation auf der Vorlage für virtuelle Maschinen folgende Aktionen ausführen:

1. Erstellen Sie die Datei C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt und fügen Sie dieser die folgenden Ausnahmen hinzu:

   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. Erstellen Sie in der Registrierung des Betriebssystems im Schlüssel HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr einen neuen DWORD-Wert mit dem Namen MiniFilterBypass und setzen Sie diesen auf 1.

3. Erstellen Sie in der Registrierung des Betriebssystems im Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd einen neuen MULTI_SZ-Wert mit dem Namen ExcludeKey und setzen Sie diesen auf \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. Starten Sie die virtuelle Maschine neu.

Für die Installation auf virtuellen Maschinen in einer Infrastruktur, die Citrix App Layering verwendet, gehen Sie wie folgt vor:

1. Installieren Sie den Kaspersky Security Center-Administrationsagenten und Kaspersky Endpoint Security für Windows auf der Vorlage der virtuellen Maschine in der Anwendungsebene.

2. Erstellen Sie ein Image einer virtuellen Maschine, das aus mehreren Ebenen besteht.

3. Stellen Sie das erstellte Image auf den Hypervisoren bereit, die die Citrix App Layering-Lösung unterstützen.

4. Konfigurieren Sie die Erstellung temporärer virtueller Maschinen aus dem erstellten Image.

Einzelheiten zur Installation von Antiviren-Software zusammen mit Citrix App Layering finden Sie in der Dokumentation zu Citrix App Layering.

Kompatibilität mit der Citrix Provisioning-Technologie (Citrix Provisioning Services)

So überprüfen Sie, ob die App mit der Citrix Provisioning-Technologie (Citrix Provisioning Services) kompatibel ist:

- Wenn die Software Citrix Provisioning-Zielgeräte auf der virtuellen Maschine installiert ist, müssen Sie diese Software vor der Installation von Kaspersky Endpoint Security entfernen (Details finden Sie auf der Website des technischen Supports von Citrix). Nach der Installation der Anwendung müssen Sie Citrix Provisioning-Zielgeräte erneut installieren. Außerdem müssen Sie bei der Wiederherstellung des Programms das Citrix Provisioning-Zielgerät neu installieren, auch bei einem Upgrade des Betriebssystems.

  Das Upgrade des Betriebssystems umfasst die folgenden Schritte:

  1. Löschen Sie das Citrix Provisioning-Zielgerät.
  2. Führen Sie ein Upgrade des Betriebssystems durch.
  3. Stellen Sie nach dem Start der virtuellen Maschine sicher, dass Kaspersky Endpoint Security ausgeführt wird und ordnungsgemäß funktioniert.
  4. Installieren Sie das Citrix Provisioning-Zielgerät neu.

- Wenn Sie die App mithilfe des Setup-Assistenten oder per Fernzugriff mithilfe von Kaspersky Security Center installieren, müssen Sie das Kontrollkästchen **Kompatibilität mit Citrix PVS gewährleisten** aktivieren.

Kompatibilität mit der Omnissa App Volumes-Technologie

Vor der Installation auf der Vorlage für virtuelle Maschinen müssen Sie die Datei %SVAgent%\Config\Custom\snapvol.cfg erstellen und dieser Datei die folgenden Ausnahmen hinzufügen:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_path=\Program Files\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`

- exclude_process_path=\Program Files\Kaspersky Lab
- exclude_process_name=avp.exe
- exclude_process_name=klnagent.exe
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon

Details finden Sie in der Dokumentation zu Omnissa.

Light Agent installieren

Die Installation von Kaspersky Endpoint Security im Light Agent-Modus auf Arm-basierten virtuellen Maschinen wird nicht unterstützt.

Die Installation des Programms im Light Agent-Modus erfolgt auf gleiche Weise wie im Standard-Modus. Bevor Sie Light Agent auf einer virtuellen Maschine installieren, müssen Sie sicherstellen, dass der Administrationsagent von Kaspersky Security Center installiert ist. Der *Administrationsagent* gewährleistet die Interaktion zwischen dem Administrationsserver und einer virtuellen Maschine.

Für die Installation von Light Agent auf einer virtuellen Maschine gibt es die folgenden Möglichkeiten:

- per Fernzugriff mithilfe von Kaspersky Security Center.
- Lokal mithilfe des Installationsassistenten.
- Lokal über die Befehlszeile.

Um Light Agent zu installieren, müssen Sie in den Einstellungen des Installationspakets oder im Setup-Assistenten die passende Konfiguration auswählen.

Wenn Light Agent auf einem Server installiert wird, werden die Komponenten des erweiterten Schutzes (Verhaltensanalyse, Exploit-Prävention, Rollback von schädlichen Aktionen) aus der Standardkonfiguration des Programms ausgeschlossen. Die standardmäßigen Programmeinstellungen bieten die empfohlene Schutzstufe und eine optimale Nutzung der Server-Ressourcen. Wenn Light Agent auf einer Workstation installiert wird, sind die Komponenten des erweiterten Schutzes in der Standardkonfiguration des Programms enthalten.

Es wird empfohlen, bei der Installation von Light Agent vordefinierte Ausnahmen und vertrauenswürdige Programme für die jeweilige virtuelle Umgebung auszuwählen. Mithilfe von vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie das Programm schnell einrichten und Kompatibilitätsprobleme mit virtuellen Umgebungen vermeiden. Sie können die Konfiguration vordefinierter Untersuchungsausnahmen und vertrauenswürdiger Programme auch nach der Installation in der Richtlinie vornehmen.

So installieren Sie Light Agent mithilfe des Setup-Assistenten

1. Kopieren Sie den Ordner mit den Programmdateien auf die virtuelle Maschine.
2. Führen Sie setup_kes.exe aus.

   Der Setup-Assistent wird gestartet.

Konfiguration von Kaspersky Endpoint Security



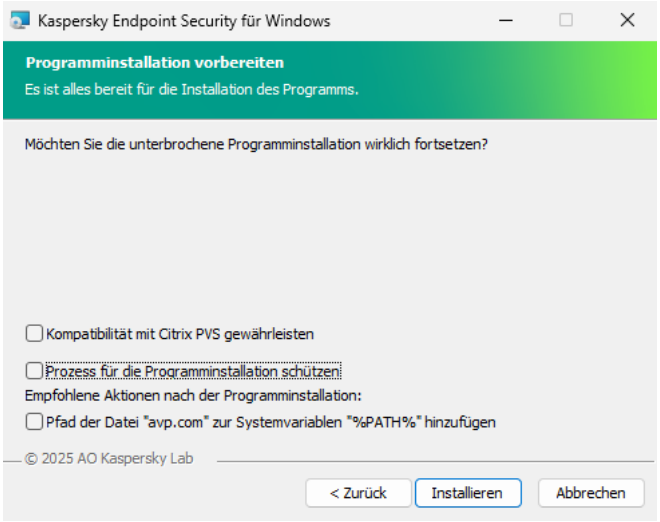
Programmkonfiguration auswählen

Wählen Sie die Konfiguration **Light Agent für den Schutz virtueller Umgebungen** aus. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.

Komponenten von Kaspersky Endpoint Security

Wählen Sie die Komponenten aus, die Sie installieren möchten (siehe folgende Abbildung). Nach der Programminstallation können Sie die Auswahl der Komponenten ändern. Dazu müssen Sie den Installationsassistenten erneut starten und den Vorgang zur Änderung der Komponentenauswahl auswählen.

Erweiterte Einstellungen



Erweiterte Installationseinstellungen für das Programm

Prozess für die Programminstallation schützen. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Endpoint Security und Sperrung des Zugriffs auf den Registrierungsschlüssel mit den Programmschlüsseln. Es wird empfohlen, den Schutz für den Installationsvorgang zu deaktivieren, falls die Programminstallation andernfalls nicht möglich ist (Dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein).

Kompatibilität mit Citrix PVS gewährleisten. Sie können die Unterstützung von Citrix Provisioning Services aktivieren, um Kaspersky Endpoint Security auf einer virtuellen Maschine zu installieren.

Pfad der Datei "avp.com" zur Systemvariablen "%PATH%" hinzufügen. Sie können den Installationspfad der Variablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen.

So installieren Sie Light Agent über die Befehlszeile

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
   ```

   oder

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
   ```

   Die Option `VDI` aktiviert den Modus zum Schutz der VDI-Infrastruktur (Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss. Der Modus zum Schutz der VDI-Infrastruktur ist standardmäßig deaktiviert.

Daraufhin wird Light Agent mit den Standardkomponenten auf der virtuellen Maschine installiert. Mithilfe der Datei setup.ini können Sie die Komponentenauswahl bearbeiten und erweiterte Einstellungen festlegen. Sie können die Installationseinstellungen auch über die Befehlszeile angeben.

So installieren Sie Light Agent über die Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Ordner **Erweitert → Remote-Installation → Installationspakete** aus.

   Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.
3. Öffnen Sie die Eigenschaften des Installationspakets für Kaspersky Endpoint Security für Windows.

   Erstellen Sie bei Bedarf ein neues Installationspaket.
4. Gehen Sie zum Abschnitt **Einstellungen**.
5. Wählen Sie die Konfiguration **Light Agent für den Schutz virtueller Umgebungen** aus. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.
6. Wählen Sie die Komponenten aus, die Sie installieren möchten.

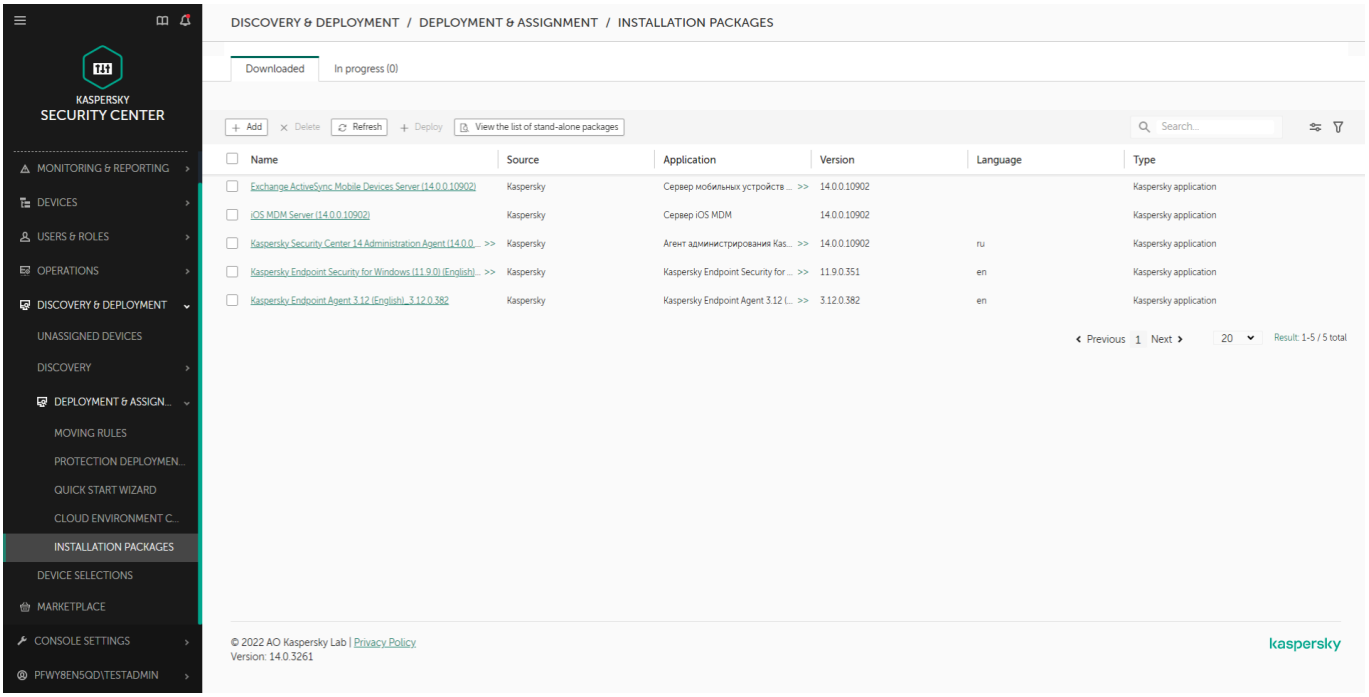
   Nach der Programminstallation können Sie die Auswahl der Komponenten ändern.
7. Vertrauenswürdige Zone konfigurieren Wählen Sie vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme für die virtuelle Umgebung aus, in der Sie das Programm installieren.

   Mithilfe von vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie das Programm schnell einrichten und Kompatibilitätsprobleme mit virtuellen Umgebungen vermeiden.
8. Speichern Sie die vorgenommenen Änderungen.
9. Erstellen Sie eine Remote-Installationsaufgabe. Wählen Sie in den Aufgabeneigenschaften das von Ihnen erstellte Installationspaket aus.

So installieren Sie Light Agent über die Web Console

1. Klicken Sie im Web Console-Hauptfenster auf **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.

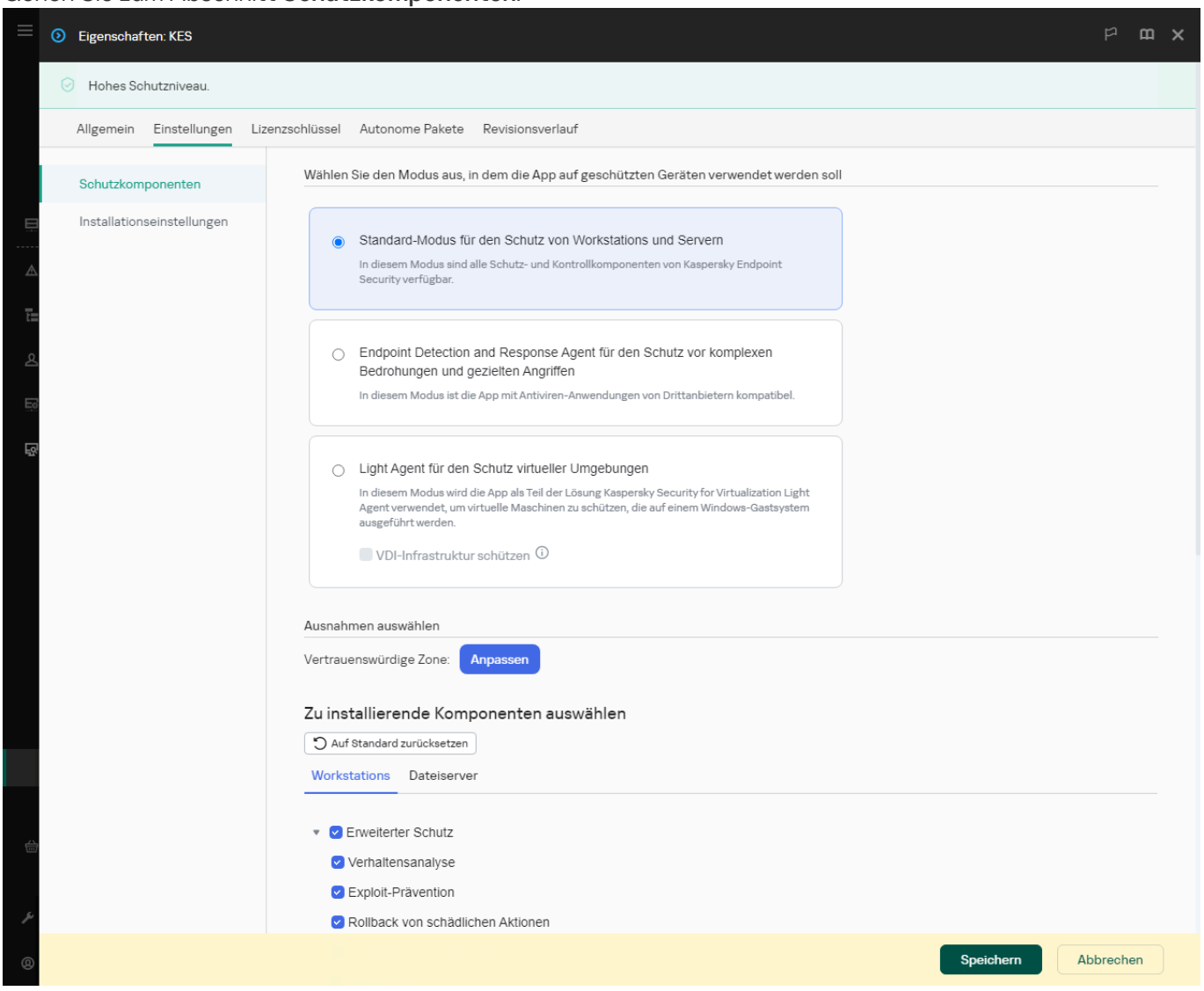
Die Liste der Installationspakete, die in Kaspersky Security Center verfügbar sind, wird geöffnet.



Liste der Installationspakete

2. Öffnen Sie die Eigenschaften des Installationspakets für Kaspersky Endpoint Security für Windows. Erstellen Sie bei Bedarf ein neues Installationspaket.
3. Wählen Sie die Registerkarte **Einstellungen**.

4. Gehen Sie zum Abschnitt **Schutzkomponenten**.



Im Installationspaket enthaltene Komponenten

5. Wählen Sie die Konfiguration **Light Agent für den Schutz virtueller Umgebungen** aus. Diese Konfiguration ist für das Programm vorgesehen, wenn es als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet wird. Light Agent muss auf jeder virtuellen Maschine installiert werden, die mithilfe der Lösung geschützt werden soll. In dieser Konfiguration können Sie die Verschlüsselungskomponenten und die Adaptive Kontrolle von Anomalien nicht verwenden. Wenn Sie Light Agent auf einer Vorlage für virtuelle Maschinen installieren, die zum Erstellen von *nicht-persistenten virtuellen Maschinen* verwendet wird, aktivieren Sie das Kontrollkästchen **VDI-Infrastruktur schützen** (VDI steht für Virtual Desktop Infrastructure). Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. In diesem Modus lehnt Light Agent Programm-Updates ab, die einen Neustart der virtuellen Maschine erfordern. Wenn Programm-Updates empfangen werden, die einen Neustart erfordern, generiert Light Agent ein Ereignis darüber, dass die Vorlage für geschützte virtuelle Maschinen aktualisiert werden muss.

6. Wählen Sie die Komponenten aus, die Sie installieren möchten.

   Nach der Programminstallation können Sie die Auswahl der Komponenten ändern.

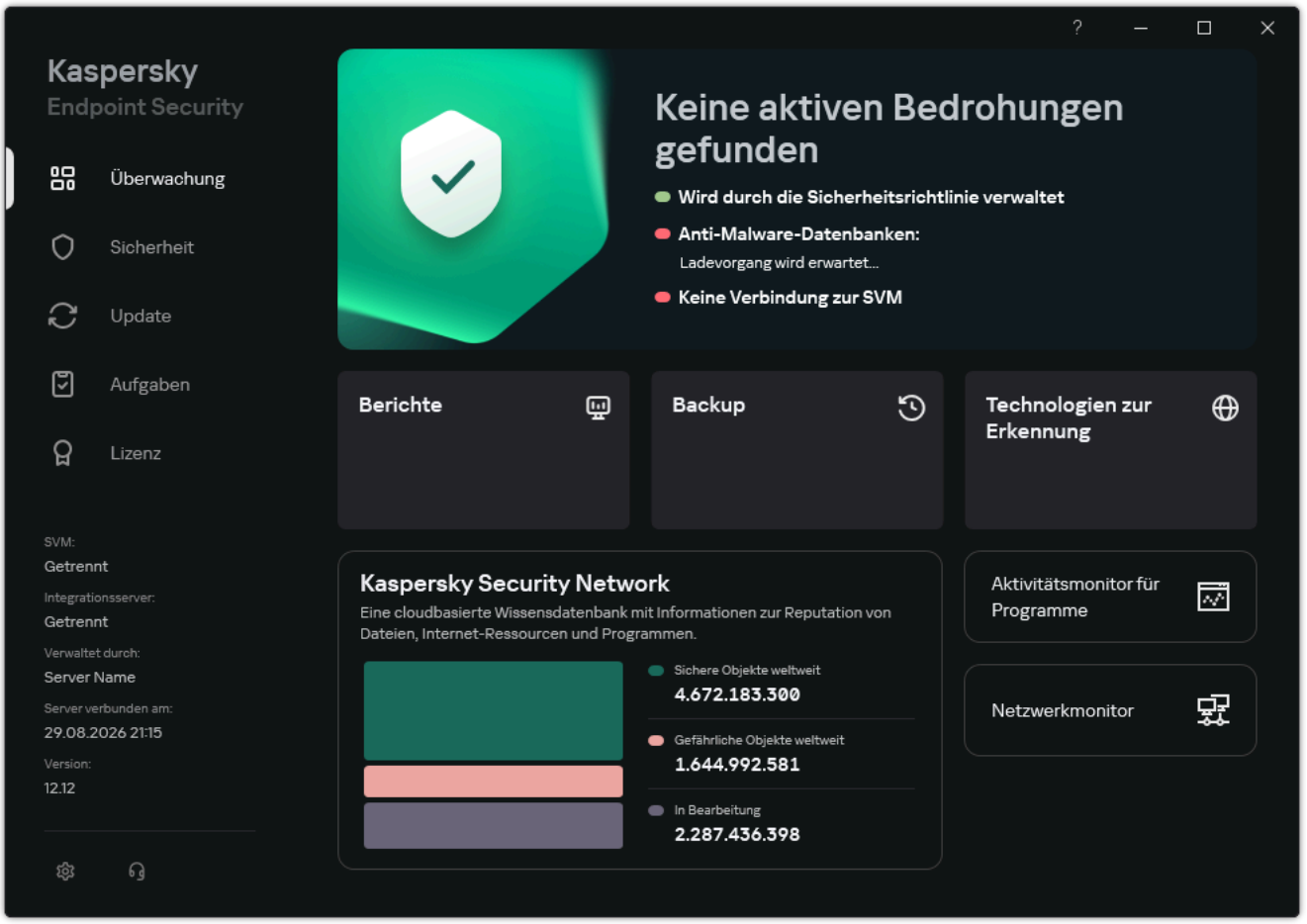
7. Vertrauenswürdige Zone konfigurieren Wählen Sie vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme für die virtuelle Umgebung aus, in der Sie das Programm installieren.

   Mithilfe von vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie das Programm schnell einrichten und Kompatibilitätsprobleme mit virtuellen Umgebungen vermeiden.

8. Speichern Sie die vorgenommenen Änderungen.

9. Erstellen Sie eine Remote-Installationsaufgabe. Wählen Sie in den Aufgabeneigenschaften das von Ihnen erstellte Installationspaket aus.

Dadurch wird Light Agent auf der virtuellen Maschine installiert. Sie können die Benutzeroberfläche des Programms verwenden, und im Infobereich wird ein Symbol für das Programm angezeigt. Jetzt müssen Sie die Verbindung von Light Agent mit einer SVM konfigurieren.



Hauptfenster von Light Agent

Über die Verbindung des Light Agents zur SVM

Die Lösung Kaspersky Security for Virtualization Light Agent erfordert eine kontinuierliche Datenübermittlung zwischen dem Light Agent und der SVM. Dies ist erforderlich, um vom Light Agent gesendete Dateien auf Viren und andere Schadsoftware zu untersuchen. Ohne eine SVM-Verbindung kann der Light Agent keine Dateien zur Untersuchung senden. Wenn länger als fünf Minuten keine Verbindung hergestellt werden kann, wird die Untersuchung mit einem Fehler beendet.

Um einen Light Agent mit einer SVM zu verbinden, sind die folgenden Schritte erforderlich:

1. Light Agent ruft die Liste der verfügbaren SVMs ab.

2. Light Agent verwendet den Algorithmus zur SVM-Auswahl und wählt einen verfügbaren Schutzserver (SVM) aus, der optimal für die Verbindung geeignet ist.

3. Light Agent überprüft zusätzliche Einstellungen der SVM-Verbindung: Tags, Status des Verbindungsschutzes, Programmfunktionalität, die von der Lizenz abgedeckt ist.

4. Light Agent stellt eine Verbindung zur SVM her.

Informationen über den Status der Verbindung von Light Agent mit einer SVM erhalten Sie in Kaspersky Endpoint Security oder über den Programmbefehl. Das Programm generiert jedes Mal ein Ereignis, wenn die Verbindung zwischen Light Agent und SVM unterbrochen oder hergestellt wird, und sendet diese Ereignisse an Kaspersky Security Center. Wenn Sie einen Integrationsserver für die SVM-Ermittlung verwenden, können Sie in der Integrationsserver-Konsole Informationen über den Status der SVM und die Anzahl der verbundenen Light Agents abrufen. Einzelheiten zur Überwachung des SVM-Status finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

SVM-Ermittlung

Sie können eine der Methoden zur SVM-Ermittlung für den Light Agent auswählen.

- Integrationsserver (VIIS) verwenden.

  Der *Integrationsserver* ist die Komponente der Lösung, welche die Interaktion von Kaspersky Security for Virtualization Light Agent mit der virtuellen Infrastruktur ermöglicht und eine Liste der für die Verbindung verfügbaren SVMs erstellt. Light Agent stellt eine Verbindung mit dem Integrationsserver her und ruft die Liste mit SVM-Adressen ab.

  Der Integrationsserver ist in großen virtuellen Infrastrukturen besonders nützlich, da er die Last zwischen den SVMs automatisch ausgleicht, Informationen über verfügbare SVMs abruft, diese Informationen analysiert und den Light Agents eine Liste der Schutzserver (SVMs) bereitstellt, die für die Verbindung optimal sind.

  Damit Light Agent eine Liste mit SVMs abrufen kann, müssen Sie nur die Adresse des Integrationsservers eingeben.

- Verwendung eines Hochverfügbarkeitsclusters aus Integrationsservern.

  Die Bereitstellung eines Hochverfügbarkeitsclusters aus Integrationsservern ist in Kaspersky Security for Virtualization Light Agent ab Version 6.4 verfügbar. Ein Hochverfügbarkeitscluster aus Integrationsservern gewährleistet den unterbrechungsfreien Schutz der virtuellen Umgebung, da SVMs und Light Agents beim Ausfall des primären Integrationsservers auf einen Backup-Integrationsserver umgeschaltet werden. Eine spezielle Cluster-Komponente, der *Load-Balancer*, ist für das Server-Failover verantwortlich. Einzelheiten zu Hochverfügbarkeitsclustern aus Integrationsservern finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

  Damit der Light Agent eine Liste der SVMs abrufen kann, müssen Sie die Adresse des Geräts eingeben, auf dem der Load-Balancer installiert ist.

- Liste mit SVM-Adressen verwenden.

  Wenn Sie einzelne SVMs angeben möchten, mit denen Light Agent eine Verbindung herstellen soll, können Sie manuell eine Liste erstellen.

  Sie müssen die Adressen der verfügbaren SVMs auflisten, mit denen der Light Agent eine Verbindung herstellen kann.

So konfigurieren Sie die SVM-Ermittlung durch Light Agent in der Verwaltungskonsole (MMC)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Richtlinien** aus.

3. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

4. Wählen Sie im Richtlinienfenster **Light Agent-Modus** → **Einstellungen zur SVM-Ermittlung** aus.

5. Wählen Sie eine Methode zur SVM-Ermittlung aus.

   - **Integrationsserver verwenden**. Geben Sie abhängig von Ihrer Infrastruktur die Einstellungen für die Verbindung mit dem Integrationsserver ein:

     - **Einzelner Integrationsserver**. Geben Sie die Einstellungen für die Verbindung mit dem Integrationsserver ein: die IPv4-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Geräts.

     - **Hochverfügbarkeitscluster aus Integrationsservern**. Geben Sie die IP-Adresse und den Port des zum Cluster gehörenden Load-Balancers ein.

   - **Benutzerdefinierte Liste mit SVM-Adressen verwenden**. Erstellen Sie eine Liste der SVMs, mit denen Light Agent eine Verbindung herstellen kann. Geben Sie die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) des Geräts an. Jedes Listenelement muss in einer separaten Zeile eingegeben oder durch ein Semikolon (`;`) vom vorherigen Element getrennt werden.

     In der Liste der SVM-Adressen werden nur vollständige Domänennamen (FQDN) angegeben, denen eine einzige IP-Adresse gegenübergestellt wird. Die Verwendung eines vollqualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann Fehler verursachen.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die SVM-Ermittlung durch Light Agent in der Web Console

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Light Agent-Modus** → **Einstellungen zur SVM-Ermittlung**.

5. Wählen Sie eine Methode zur SVM-Ermittlung aus.

   - **Integrationsserver verwenden**. Geben Sie abhängig von Ihrer Infrastruktur die Einstellungen für die Verbindung mit dem Integrationsserver ein:

     - **Einzelner Integrationsserver**. Geben Sie die Einstellungen für die Verbindung mit dem Integrationsserver ein: die IPv4-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Geräts.

     - **Hochverfügbarkeitscluster aus Integrationsservern**. Geben Sie die IP-Adresse und den Port des zum Cluster gehörenden Load-Balancers ein.

- **Benutzerdefinierte Liste mit SVM-Adressen verwenden**. Erstellen Sie eine Liste der SVMs, mit denen Light Agent eine Verbindung herstellen kann. Geben Sie die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) des Geräts an. Jedes Listenelement muss in einer separaten Zeile eingegeben oder durch ein Semikolon (`;`) vom vorherigen Element getrennt werden.

  In der Liste der SVM-Adressen werden nur vollständige Domänennamen (FQDN) angegeben, denen eine einzige IP-Adresse gegenübergestellt wird. Die Verwendung eines vollqualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann Fehler verursachen.

6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie die SVM-Ermittlung durch Light Agent in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Light Agent-Modus** auf die Kachel **Einstellungen zur SVM-Ermittlung**.
3. Wählen Sie eine Methode zur SVM-Ermittlung aus.
   - **Integrationsserver verwenden**. Geben Sie abhängig von Ihrer Infrastruktur die Einstellungen für die Verbindung mit dem Integrationsserver ein:
     - **Einzelner Integrationsserver**. Geben Sie die Einstellungen für die Verbindung mit dem Integrationsserver ein: die IPv4-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Geräts.
     - **Hochverfügbarkeitscluster aus Integrationsservern**. Geben Sie die IP-Adresse und den Port des zum Cluster gehörenden Load-Balancers ein.
   - **Benutzerdefinierte Liste mit SVM-Adressen verwenden**. Erstellen Sie eine Liste der SVMs, mit denen Light Agent eine Verbindung herstellen kann. Geben Sie die IP-Adresse im IPv4-Format oder den vollqualifizierten Domänennamen (FQDN) des Geräts an. Jedes Listenelement muss in einer separaten Zeile eingegeben oder durch ein Semikolon (`;`) vom vorherigen Element getrennt werden.

     In der Liste der SVM-Adressen werden nur vollständige Domänennamen (FQDN) angegeben, denen eine einzige IP-Adresse gegenübergestellt wird. Die Verwendung eines vollqualifizierten Domänennamens, der mehreren IP-Adressen entspricht, kann Fehler verursachen.
4. Speichern Sie die vorgenommenen Änderungen.

Algorithmus der SVM-Auswahl für Light Agent konfigurieren

Die Infrastruktur des Unternehmens kann über mehrere bereitgestellte SVMs verfügen, mit denen sich Light Agents verbinden können. Um das Netzwerk und die Ressourcen der virtuellen Infrastruktur gleichmäßig auszulasten, müssen Sie die Light Agents auf die SVMs verteilen.

Algorithmen für die SVM-Auswahl

Light Agents können die folgenden Algorithmen für die SVM-Auswahl zum Herstellen der Verbindung verwenden: Standardalgorithmus (standardmäßig) und Erweiterter Algorithmus.

Algorithmen für die SVM-Auswahl

Standardalgorithmus	Erweiterter Algorithmus
Wenn dieser Algorithmus verwendet wird, wählt der Light Agent auf der virtuellen Maschine nach der Installation und dem Start eine Verbindung mit einer SVM aus, die für den Light Agent als *lokal* gilt. Wenn keine lokalen SVMs gefunden werden, die für eine Verbindung geeignet sind, wählt der Light Agent die SVM aus, mit der die wenigsten Light Agents verbunden sind. Dabei bleibt die Platzierung der SVM in der virtuellen Infrastruktur unberücksichtigt. Der Standort der SVM relativ zum Light Agent wird nicht bestimmt, wenn für den Schutzserver auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist. In diesem Fall wird empfohlen, den erweiterten Algorithmus der SVM-Auswahl zu verwenden und als Methode zur SVM-Ermittlung den Integrationsserver auszuwählen. Ob eine SVM in Bezug auf den Light Agent als "lokal" gilt, wird je nach Art der virtuellen Infrastruktur ermittelt.	Wenn dieser Algorithmus angewendet wird, können Sie folgende weitere Parameter zur SVM-Auswahl angeben: • Ob der Standort der SVM innerhalb der Infrastruktur beim Auswählen der Verbindung einer SVM berücksichtigt oder ignoriert werden soll • Falls der SVM-Standort berücksichtigt wird, die Methode zur Bestimmung der SVM-Lokalität relativ zum Light Agent Wenn Light Agents den SVM-Standort innerhalb der Infrastruktur ignorieren, können sich Light Agents mit allen zur Verbindung verfügbaren SVMs verbinden. Wenn Light Agents den SVM-Standort innerhalb der Infrastruktur berücksichtigen, müssen Sie den Typ des SVM-Standorts auswählen, der bei der Ermittlung herangezogen wird, wenn eine SVM in Bezug auf den Light Agent als "lokal" gelten soll. Ob eine SVM in Bezug auf den Light Agent als "lokal" gilt, wird je nach Art der virtuellen Infrastruktur ermittelt. Wenn Light Agents im Rahmen der Verbindungsherstellung bei der SVM-Auswahl den SVM-Standort innerhalb der Infrastruktur berücksichtigen, können Light Agents nur eine Verbindung zu jenen SVMs herstellen, die als "lokal" gelten. Wenn Sie beispielsweise als Typ des SVM-Standorts einen Hypervisoren-Cluster angeben, gelten alle auf diesem Hypervisoren-Cluster bereitgestellten SVMs als lokal für Light Agent, und Light Agent kann sich nur mit einer dieser SVMs verbinden. Wenn in dem Cluster, in dem der Light Agent ausgeführt wird, keine SVM verfügbar ist, stellt der Light Agent keine Verbindung zu einer SVM her. Bei der Auswahl der SVM berücksichtigen die Light Agents außerdem die Anzahl der verbundenen Light Agents, um eine gleichmäßige Zuordnung von Light Agents zu verfügbaren SVMs zu gewährleisten. Wenn für einen Light Agent der erweiterter Algorithmus der SVM-Auswahl verwendet wird, als Methode zur SVM-Ermittlung eine Liste mit SVM-Adressen ausgewählt wurden und auf der SVM der Modus zum Schutz großer Infrastrukturen aktiviert ist, dann ist die Verbindung des Light Agents mit dieser SVM nur möglich, wenn der Light Agent den SVM-Standort ignoriert.
Basis Dynamix Enterprise	
In virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise gilt die SVM als lokal für den Light Agent, wenn sie auf demselben Knoten bereitgestellt wurde wie die virtuelle Maschine mit installiertem Light Agent.	In virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise kann eine SVM in einem der folgenden Fälle als lokal für Light Agent gelten: • Die SVM wurde auf demselben Knoten bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde in derselben Zone bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent.

Standardalgorithmus	Erweiterter Algorithmus
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer und Basis Dynamix Standard	
In virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard gilt eine SVM als lokal für Light Agent, wenn sie auf demselben Hypervisor bereitgestellt wurde wie die virtuelle Maschine mit installiertem Light Agent.	In virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard kann eine SVM in einem der folgenden Fälle als lokal für Light Agent gelten: • Die SVM wurde auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde in demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent.
OpenStack und VK Private Cloud SVM	
In einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird, können Sie mithilfe des Parameters `StandardAlgorithmSvmLocality` im Abschnitt `HypervisorSpecificSettings:Openstack` der Konfigurationsdatei „appsettings.json“ des Integrationsservers festlegen, wie bestimmt wird, ob eine SVM in Bezug auf den Light Agent als lokal gilt. Je nach Version des Integrationsservers befindet sich die Datei in einem der folgenden Pfade: • /var/opt/kaspersky/viis/common/ – Datei des Linux-basierten Integrationsservers. • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ – Datei des Windows-basierten Integrationsservers. Der Parameter `StandardAlgorithmSvmLocality` kann folgende Werte annehmen: • `ServerGroup`: Wenn dieser Wert angegeben ist, gilt eine SVM als lokal für Light Agent, wenn sie sich in derselben Servergruppe befindet wie die virtuelle Maschine mit installiertem Light Agent. Dieser Wert wird standardmäßig verwendet. • `Project`: Wenn dieser Wert angegeben ist, gilt eine SVM als lokal für Light Agent, wenn sie innerhalb desselben OpenStack-Projekts wie die virtuelle Maschine mit installiertem Light Agent bereitgestellt wurde. • `AvailabilityZone`: Wenn dieser Wert angegeben ist, gilt eine SVM als lokal für Light Agent, wenn sie sich in derselben Verfügbarkeitszone befindet wie die virtuelle Maschine mit installiertem Light Agent.	In einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird, kann eine SVM in einem der folgenden Fälle als lokal für Light Agent gelten: • Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM wurde innerhalb desselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent. • Die SVM befindet sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent.

Zusätzlich zu Algorithmen für die SVM-Verbindung können Sie die Verbindung von Light Agents mit SVMs auch mithilfe von Tags regulieren.

Konfiguration des Algorithmus für die SVM-Auswahl

So konfigurieren Sie den Algorithmus zur SVM-Auswahl für Light Agent in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Light Agent-Modus** → **Algorithmus der SVM-Auswahl** aus.

4. Wählen Sie den Algorithmus aus:

   - **Standard-Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die im selben Hypervisor bereitgestellt werden.

   - **Erweiterten Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die an SVM-Standorten des ausgewählten Typs bereitgestellt werden (standardmäßig **Hypervisor**).

5. Wählen Sie bei Bedarf den SVM-Standort für den erweiterten Algorithmus der SVM-Auswahl aus:

   - **Hypervisor**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

     - Die SVMs werden auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

     - Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

     - Die SVM befindet sich auf demselben Knoten wie die virtuelle Maschine mit installiertem Light Agent (in a virtual infrastructure Basis Dynamix Enterprise).

     Wenn auf demselben Hypervisor oder in derselben Servergruppe, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

   - **Cluster**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

     - Die SVMs werden auf demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

     - Die SVMs werden auf demselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

     - Die SVM befindet sich auf demselben Zone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

     Wenn auf demselben Hypervisor-Cluster oder innerhalb eines OpenStack-Projektes, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Datencenter**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs befinden sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich in demselben Rechenzentrum wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

  Wenn in demselben Rechenzentrum oder in derselben Verfügbarkeitszone, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Ignorieren**. Light Agent ignoriert den SVM-Standort für die Verbindung mit dem Schutzserver. Light Agents berücksichtigt weitere Kriterien: Tags, Anzahl der Light Agents, die mit einer SVM verbunden sind, und so weiter.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Algorithmus zur SVM-Auswahl für Light Agent in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.

2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Light Agent-Modus** → **Algorithmus der SVM-Auswahl**.

5. Wählen Sie den Algorithmus aus:

   - **Standard-Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die im selben Hypervisor bereitgestellt werden.

   - **Erweiterten Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die an SVM-Standorten des ausgewählten Typs bereitgestellt werden (standardmäßig **Hypervisor**).

6. Wählen Sie bei Bedarf den SVM-Standort für den erweiterten Algorithmus der SVM-Auswahl aus:

- **Hypervisor**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich auf demselben Knoten wie die virtuelle Maschine mit installiertem Light Agent (in a virtual infrastructure Basis Dynamix Enterprise).

  Wenn auf demselben Hypervisor oder in derselben Servergruppe, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Cluster**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden auf demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs werden auf demselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich auf demselben Zone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

  Wenn auf demselben Hypervisor-Cluster oder innerhalb eines OpenStack-Projektes, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Datencenter**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs befinden sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich in demselben Rechenzentrum wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

Wenn in demselben Rechenzentrum oder in derselben Verfügbarkeitszone, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Ignorieren**. Light Agent ignoriert den SVM-Standort für die Verbindung mit dem Schutzserver. Light Agents berücksichtigt weitere Kriterien: Tags, Anzahl der Light Agents, die mit einer SVM verbunden sind, und so weiter.

7. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Algorithmus zur SVM-Auswahl für Light Agent in der Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Light Agent-Modus** auf die Kachel **Einstellungen zur SVM-Ermittlung**.
3. Wählen Sie den Algorithmus aus:
   - **Standard-Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die im selben Hypervisor bereitgestellt werden.
   - **Erweiterten Algorithmus zur SVM-Auswahl verwenden**. Light Agent wählt SVMs aus, die an SVM-Standorten des ausgewählten Typs bereitgestellt werden (standardmäßig **Hypervisor**).
4. Wählen Sie bei Bedarf den SVM-Standort für den erweiterten Algorithmus der SVM-Auswahl aus:
   - **Hypervisor**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):
     - Die SVMs werden auf demselben Hypervisor bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).
     - Die SVM befindet sich in derselben Servergruppe wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).
     - Die SVM befindet sich auf demselben Knoten wie die virtuelle Maschine mit installiertem Light Agent (in a virtual infrastructure Basis Dynamix Enterprise).

   Wenn auf demselben Hypervisor oder in derselben Servergruppe, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Cluster**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden auf demselben Hypervisor-Cluster bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs werden auf demselben OpenStack-Projekts bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich auf demselben Zone wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

  Wenn auf demselben Hypervisor-Cluster oder innerhalb eines OpenStack-Projektes, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Datencenter**. Der Light Agent wählt für die Verbindung eine SVM aus, welche die Kriterien erfüllt (abhängig von der Art der virtuellen Infrastruktur):

  - Die SVMs werden in demselben Rechenzentrum bereitgestellt wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer oder Basis Dynamix Standard).

  - Die SVMs befinden sich in derselben Verfügbarkeitszone wie die virtuelle Maschine mit installiertem Light Agent (in einer virtuellen Infrastruktur, die auf der OpenStack- oder VK Private Cloud-Plattform ausgeführt wird).

  - Die SVM befindet sich in demselben Rechenzentrum wie die virtuelle Maschine mit installiertem Light Agent (in virtuellen Infrastrukturen auf Basis von Basis Dynamix Enterprise).

  Wenn in demselben Rechenzentrum oder in derselben Verfügbarkeitszone, in der sich die virtuelle Maschine mit installiertem Light Agent befindet, keine SVMs für die Verbindung verfügbar sind, stellt der Light Agent keine Verbindung zur SVM her.

- **Ignorieren**. Light Agent ignoriert den SVM-Standort für die Verbindung mit dem Schutzserver. Light Agents berücksichtigt weitere Kriterien: Tags, Anzahl der Light Agents, die mit einer SVM verbunden sind, und so weiter.

5. Speichern Sie die vorgenommenen Änderungen.

Verbindungen der Light Agents auf SVMs verteilen (Tags)

Mehrere Light Agents können sich mit einer SVM verbinden. Um Auslastung durch Light Agent-Verbindungen auszugleichen, können Sie eine separate Liste mit SVMs angeben. Wenn Sie einen Integrationsserver für die SVM-Ermittlung verwenden, können Sie *Tags* verwenden, um die Light Agent-Verbindungen gleichmäßig auf SVMs zu verteilen. Mithilfe eines Tags können Sie einem Light Agent eine Liste mit SVMs für die Verbindung zuweisen. Dazu müssen Sie dem Light Agent ein Tag zuweisen und dieses Tag in den SVM-Einstellungen angeben. Einzelheiten über die Angabe von Tags in den SVM-Einstellungen finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Beispiel: Die Lösung Kaspersky Endpoint Detection and Response Optimum wird in Ihrer Infrastruktur für bestimmte Hosts der virtuellen Maschinen bereitgestellt. In diesem Fall können Sie dem Light Agent das Tag `[EDROptimum]` zuweisen, damit sich der Light Agent mit den SVMs verbindet, die über einen 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.

So weisen Sie ein Tag für die Verbindung zwischen SVM und Light Agent in der Verwaltungskonsole (MMC) zu

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Light Agent-Modus** → **Tag für die Verbindung zur SVM** aus.
4. Aktivieren Sie das Kontrollkästchen **Tag für die Verbindung verwenden** und geben Sie ein Tag für die Verbindung zur SVM ein.

   Als Tag können Sie eine Zeichenkette von höchstens 255 Zeichen Länge eingeben. Sie können jedes Zeichen mit Ausnahme von `;` verwenden.
5. Speichern Sie die vorgenommenen Änderungen.

So weisen Sie ein Tag für die Verbindung zwischen SVM und Light Agent in der Web Console zu

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Light Agent-Modus** → **Tag für die Verbindung zur SVM**.
5. Aktivieren Sie das Kontrollkästchen **Tag für die Verbindung verwenden** und geben Sie ein Tag für die Verbindung zur SVM ein.

   Als Tag können Sie eine Zeichenkette von höchstens 255 Zeichen Länge eingeben. Sie können jedes Zeichen mit Ausnahme von `;` verwenden.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So weisen Sie ein Tag für die Verbindung zwischen SVM und Light Agent in der Programmoberfläche zu

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Light Agent-Modus** auf die Kachel **Tag für die Verbindung zur SVM**.

3. Aktivieren Sie das Kontrollkästchen **Tag für die Verbindung verwenden** und geben Sie ein Tag für die Verbindung zur SVM ein.

   Als Tag können Sie eine Zeichenkette von höchstens 255 Zeichen Länge eingeben. Sie können jedes Zeichen mit Ausnahme von `;` verwenden.

4. Speichern Sie die vorgenommenen Änderungen.

Schutz der Verbindung zwischen Light Agent und SVM

Sie können die Verschlüsselung der Verbindung zwischen Light Agents und Schutzserver konfigurieren. Dazu müssen Sie in den Einstellungen des Schutzservers auf der SVM und in den Light Agent-Einstellungen die Verschlüsselung des Datenkanals zwischen dem Light Agent und dem Schutzserver aktivieren.

Ein Light Agent, für den der Verbindungsschutz aktiviert ist, kann sich nur mit SVMs verbinden, für die die Verschlüsselung des Datenkanals zwischen dem Light Agent und dem Schutzserver aktiviert ist. Ein Light Agent, für den der Verbindungsschutz deaktiviert ist, kann sich nur mit SVMs verbinden, für die die Kanalverschlüsselung deaktiviert ist oder für die eine unsichere Verbindung zwischen dem Schutzserver und dem Light Agent erlaubt ist.

Einzelheiten zur Konfiguration des Verbindungsschutzes auf dem Schutzserver finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Der Schutz der Verbindung mithilfe der Verschlüsselung kann die Leistung von Kaspersky Security for Virtualization Light Agent verringern.

So konfigurieren Sie den Verbindungsschutz in einem Light Agent in der Verwaltungskonsole (MMC)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Light Agent-Modus** → **Verbindungsschutz** aus.
4. Aktivieren Sie das Kontrollkästchen **Datentransfer zwischen Light Agent und Schutzserver verschlüsseln**.
5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Verbindungsschutz in einem Light Agent in der Web Console

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Light Agent-Modus** → **Verbindungsschutz**.
5. Aktivieren Sie das Kontrollkästchen **Datentransfer zwischen Light Agent und Schutzserver verschlüsseln**.
6. Um die Richtlinie auf Computer anzuwenden, schließen Sie die Vorhängeschloss-Symbole und speichern Sie Ihre Änderungen.

So konfigurieren Sie den Verbindungsschutz in einem Light Agent über die Programmoberfläche

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.
2. Klicken Sie im Fenster mit den Programmeinstellungen unter **Light Agent-Modus** auf die Kachel **Verbindungsschutz**.
3. Aktivieren Sie das Kontrollkästchen **Datentransfer zwischen Light Agent und Schutzserver verschlüsseln**.
4. Speichern Sie die vorgenommenen Änderungen.

Light Agent aktivieren

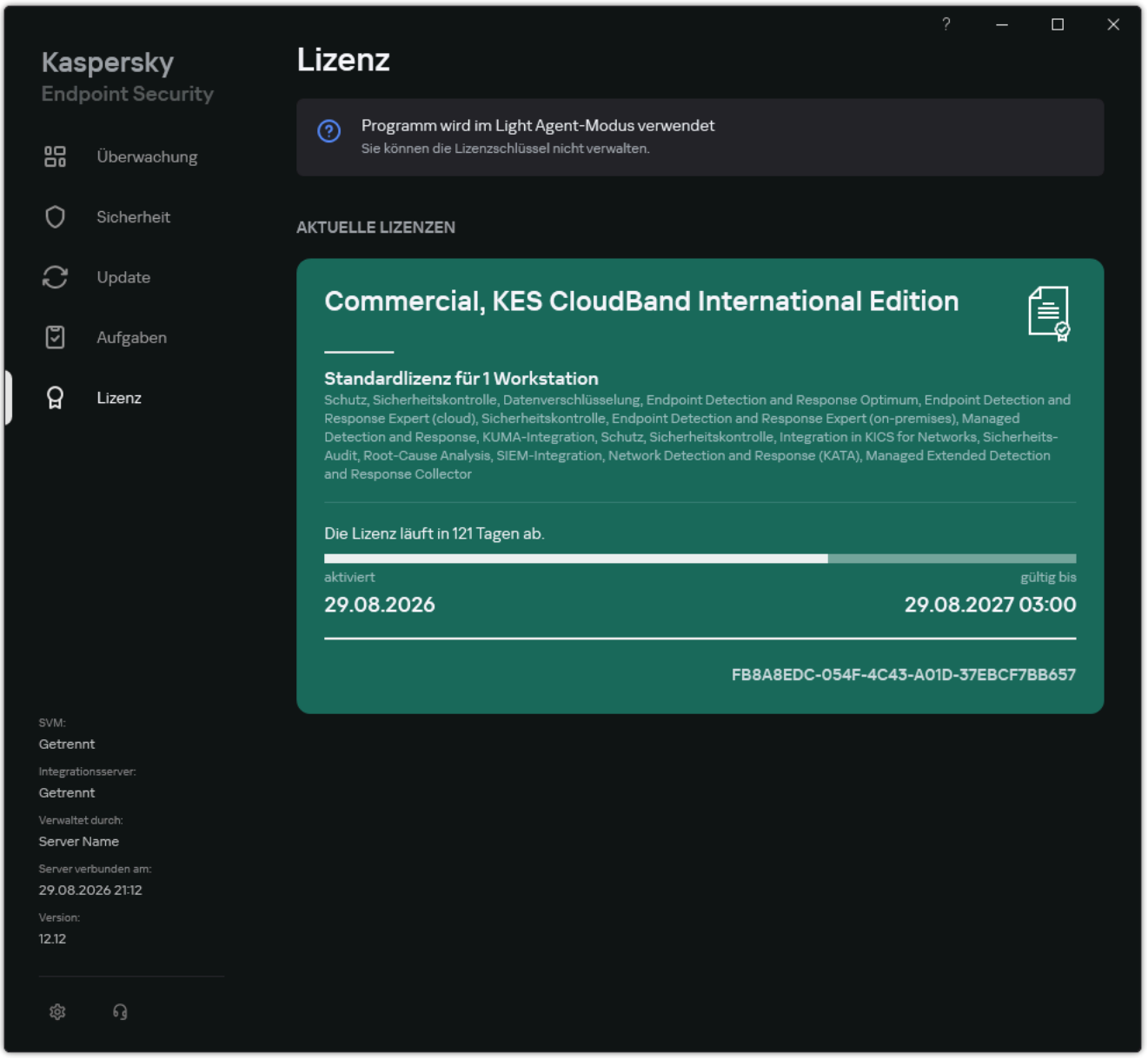
Wenn Kaspersky Endpoint Security im Light Agent-Modus zum Schutz von virtuellen Umgebungen verwendet wird, müssen Sie das Programm nicht separat aktivieren. Um das Programm zu aktivieren, müssen Sie einen Lizenzschlüssel zu der SVM hinzufügen. Einen Lizenzschlüssel können Sie mithilfe einer speziellen Aufgabe in der Konsole von Kaspersky Security Center zu SVM hinzufügen. Sie können Lizenzschlüssel nicht über die Light Agent-Benutzeroberfläche verwalten, Sie können jedoch Lizenzinformationen anzeigen (siehe Abbildung unten). Sie können die Lizenzinformationen für Light Agent auch über die Befehlszeile anzeigen (siehe Anweisungen unten). Light Agent erhält diese Informationen von der SVM. Einzelheiten zur Aktivierung der Lösung und zur Verwaltung von Lizenzschlüsseln finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

So zeigen Sie Lizenzinformationen für Light Agent an:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

```
avp.com LICENSE /CHECK
```

Daraufhin zeigt Kaspersky Endpoint Security Lizenzinformationen an: Adresse der SVM, mit der der Light Agent verbunden ist, Anzahl der Tage bis zum Ablauf der Lizenz sowie weitere Informationen. Sollten bei der Aktivierung von Light Agent Probleme auftreten, finden Sie in der Wissensdatenbank des Technischen Supports weitere Informationen.



Fenster Lizenzverwaltung

Leitfaden zur Migration von KSVLA Light Agent zu KES Light Agent

Kaspersky Security for Virtualization 5.2 Light Agent enthält die Komponente Light Agent für Windows 5.2 (im Folgenden auch „KSVLA Light Agent“ genannt). In Kaspersky Security for Virtualization Light Agent 6.2 wird Kaspersky Endpoint Security im Light Agent-Modus als Light Agent-Komponente verwendet. Um die Lösung auf Version 6.2 zu aktualisieren, müssen Sie von KSVLA Light Agent 5.2 zu Kaspersky Endpoint Security im Light Agent-Modus (im Folgenden auch „KES Light Agent“ genannt) migrieren. Einzelheiten zum Versions-Update der Lösung Kaspersky Security for Virtualization Light Agent finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Softwarevoraussetzungen

Bevor Sie mit der Migration von KSVLA Light Agent zu KES Light Agent beginnen, stellen Sie sicher, dass Ihre virtuelle Maschine die Hard- und Softwareanforderungen von Kaspersky Endpoint Security für Windows erfüllt. Die Listen der unterstützten Betriebssystemversionen sind für KES und KSWS unterschiedlich. Beispielsweise unterstützt KES keine Server, auf denen Windows Server 2003 ausgeführt wird.

Minimale Softwareanforderungen für die Migration von KSVLA Light Agent zu KES Light Agent:

- Kaspersky Endpoint Security für Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (einschließlich der Komponenten Schutzserver und Integrationsserver).
- Kaspersky Security Center 14.2

  Wenn Sie eine ältere Version von Kaspersky Security Center installiert haben, aktualisieren Sie diese auf 14.2 oder höher. In dieser Version von Kaspersky Security Center können Sie mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben Richtlinien in ein Profil migrieren, aber nicht in eine Richtlinie. In dieser Version von Kaspersky Security Center können Sie mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben auch eine breitere Palette von Richtlinieneinstellungen migrieren.

Schritte der Migration

Die Migration von KSVLA Light Agent zu KES Light Agent erfolgt halbautomatisch. Dies ist durch Unterschiede in der Programmarchitektur bedingt.

Die Migration von KSVLA Light Agent zu KES Light Agent umfasst die folgenden Schritte:

1. **Migration der Aufgaben und Richtlinien von KSVLA Light Agent**

   Um die Richtlinieneinstellungen zu migrieren, müssen Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (Migrations-Assistent) ausführen. Nach der Migration der Richtlinieneinstellungen müssen Sie bestimmte Einstellungen manuell konfigurieren. Dies sind Einstellungen, die der Migrations-Assistent nicht automatisch migrieren kann (z. B. Einstellungen für das Datenbanken-Update). Außerdem müssen Sie nach der Migration überprüfen, ob der Migrations-Assistent alle Einstellungen korrekt migriert hat.

   Wenn der Kennwortschutz aktiviert ist, um den Zugriff auf KSVLA Light Agent einzuschränken, müssen Sie vor der Installation von KES Light Agent den Kennwortschutz in der KSVLA Light Agent-Richtlinie deaktivieren. Sie können das Deinstallationskennwort nicht in den Einstellungen des KES Light Agent-Installationspakets eingeben. Nachdem die Installation von KES Light Agent über KSVLA Light Agent abgeschlossen ist, müssen Sie den Kennwortschutz in der KES-Richtlinie aktivieren.

2. **Kaspersky Endpoint Security im Light Agent-Modus installieren**

   Für die Installation von KES Light Agent gibt es folgende Methoden:

   - Installation von KES Light Agent, nachdem KSVLA Light Agent entfernt wurde (empfohlen)
   - Installation von KES Light Agent über KSVLA Light Agent

3. **Überprüfen, ob das Programm nach der Migration funktionsfähig ist**

   Überprüfen Sie nach der Migration von KSVLA Light Agent zu KES Light Agent, ob das Programm ordnungsgemäß funktioniert. Aktivieren Sie die konvertierte Richtlinie. Überprüfen Sie den Status der virtuellen Maschine in der Kaspersky Security Center-Konsole (erforderlicher Status: *OK*). Stellen Sie sicher, dass für das Programm keine Fehler gemeldet wurden, und überprüfen Sie den Zeitpunkt der letzten Verbindung mit einer SVM und den Schutzstatus der virtuellen Maschine. Sie müssen Light Agent nicht aktivieren, da der Lizenzschlüssel zur SVM hinzugefügt wird.

Installation von KES Light Agent anstelle von KSVLA Light Agent

Sie können KES Light Agent wie folgt installieren:

- Installation von KES Light Agent, nachdem KSVLA Light Agent entfernt wurde (empfohlen)
- Installation von KES Light Agent über KSVLA Light Agent

KSVLA Light Agent entfernen

Sie können das Programm per Fernzugriff mithilfe der Aufgabe *Remote-Installation einer Anwendung*, lokal auf der virtuellen Maschine oder in der Vorlage für virtuelle Maschinen entfernen. Nachdem KSVLA Light Agent entfernt wurde, müssen Sie die virtuelle Maschine möglicherweise neu starten.

Nachdem KSVLA Light Agent entfernt wurde, installieren Sie KES Light Agent mithilfe einer passenden Methode.

Kaspersky Endpoint Security installieren

> Wenn der Kennwortschutz aktiviert ist, um den Zugriff auf KSVLA Light Agent einzuschränken, müssen Sie vor der Installation von KES Light Agent den Kennwortschutz in der KSVLA Light Agent-Richtlinie deaktivieren. Sie können das Deinstallationskennwort nicht in den Einstellungen des KES Light Agent-Installationspakets eingeben. Nachdem die Installation von KES Light Agent über KSVLA Light Agent abgeschlossen ist, müssen Sie den Kennwortschutz in der KES-Richtlinie aktivieren.

Wenn Sie Kaspersky Endpoint Security installieren, müssen Sie den Modus **Light Agent für den Schutz virtueller Umgebungen** auswählen. Bevor KES Light Agent auf einer virtuellen Maschine installiert wird, erkennt das Installationsprogramm den KSVLA Light Agent als inkompatible Software und entfernt ihn. Die Migration der KSVLA Light Agent-Konfiguration wird nicht unterstützt. Darum müssen Sie bei der Installation von KES Light Agent die zu installierenden Komponenten angeben. Verwenden Sie dazu die Eigenschaften des Installationspakets oder den Installations-Assistenten. Nachdem KSVLA Light Agent entfernt wurde, müssen Sie die virtuelle Maschine neu starten.

Bei der Installation von KES Light Agent werden die Einstellungen und Aufgaben von KSVLA Light Agent nicht migriert. Um Einstellungen und Aufgaben zu migrieren, führen Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben aus.

Die Liste der installierten Komponenten können Sie wie folgt überprüfen: im Abschnitt **Sicherheit** auf der Benutzeroberfläche des Programms, mithilfe des Befehls `status` oder in der Kaspersky Security Center-Konsole in den Computereigenschaften. Nach der Installation können Sie die Komponentenauswahl ändern, indem Sie die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

Entsprechung der Komponenten von KSVLA Light Agent und KES Light Agent

Die Auswahl der Komponenten von KSVLA Light Agent und KES Light Agent ist praktisch gleich. KES Light Agent bietet mehr Einstellungen als KSVLA Light Agent. Nach der Migration haben die neuen Einstellungen standardmäßige Werte.

Entsprechung der Komponenten von KSVLA Light Agent und KES Light Agent

Light Agent 5.2	KES Light Agent
Untersuchungskernel	Anwendungskernel
Datei-Anti-Virus	Schutz vor bedrohlichen Dateien
Mail-Anti-Virus	Schutz vor E-Mail-Bedrohungen
Web-Anti-Virus	Schutz vor Web-Bedrohungen
Firewall	Firewall
Schutz vor Netzwerkangriffen	Schutz vor Netzwerkbedrohungen
Aktivitätskontrolle für Programme	Programm-Überwachung
Kontrolle des Programmstarts	Programmkontrolle
Web-Kontrolle	Web-Kontrolle
Gerätekontrolle	Gerätekontrolle
Aktivitätsmonitor	In Kaspersky Endpoint Security hat diese Komponente die folgenden Teilkomponenten: • Exploit-Prävention • Verhaltensanalyse • Rollback von schädlichen Aktionen
Überwachung der Systemintegrität	Überwachung der Systemintegrität
Integration mit Kaspersky Endpoint Agent	*(nicht unterstützt)* Ab Kaspersky Endpoint Security für Windows 11.9.0 ist das Verteilungspaket für Kaspersky Endpoint Agent nicht mehr im Lieferumfang enthalten.
AMSI-Schutz	AMSI-Schutz

Migration der Aufgaben und Richtlinien von KSVLA Light Agent

Sie können die Einstellungen der Richtlinien und Aufgaben von KSVLA Light Agent mithilfe des Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (im Folgenden auch als „Migrations-Assistent“ bezeichnet) migrieren.

Der Migrations-Assistent für KSVLA Light Agent ist nur in der Verwaltungskonsole (MMC) verfügbar. Richtlinien- und Aufgabeneinstellungen können nicht über die Web Console oder Cloud Console migriert werden.

Die folgenden Besonderheiten sind bei der Migration von Richtlinien und Aufgaben zu beachten:

- Eine neue Richtlinie hat den Namen *<Richtlinie> (umgewandelt)*.
- Die neue Richtlinie hat den Status *Inaktive Richtlinie*.
- Das Änderungsverbot für Einstellungen („Vorhängeschloss“) wird nicht migriert. Der Migrations-Assistent legt Standardwerte fest.
- Richtlinienprofile werden nicht migriert. Sie müssen die Richtlinienprofile manuell hinzufügen.
- Verbesserte Verwaltung für vertrauenswürdige Zonen. In KSVLA Light Agent konnten Sie vordefinierte Ausnahmen nur beim Erstellen einer Richtlinie hinzufügen. Anschließend konnten Sie in den Richtlinieneigenschaften die zuvor hinzugefügten vordefinierten Ausnahmen konfigurieren oder Ausnahmen manuell hinzufügen. Sie konnten über die Richtlinieneigenschaften keine vordefinierten Ausnahmen hinzufügen. In KES Light Agent sind vordefinierte Ausnahmen sowohl während der Richtlinienerstellung als auch in den Eigenschaften der erstellten Richtlinie verfügbar. Sie können vordefinierte Ausnahmen auch im Installationspaket auswählen.
- Die Konfiguration der Benutzeroberfläche in Kaspersky Endpoint Security wurde aus dem Installationsprogramm in die Richtlinie verschoben. Wenn Sie beispielsweise die Benutzeroberfläche des Programms ausblenden möchten, können Sie die Richtlinieneinstellungen entsprechend anpassen.
- Die Funktionen zur Konfiguration der berechtigungsbasierten Zugriffskontrolle (RBAC) sind in Kaspersky Endpoint Security und KSVLA Light Agent unterschiedlich. Sie müssen die Zugriffsrechte für Benutzer auf Funktionsbereiche komplett neu konfigurieren.

So verwenden Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben, um KSVLA Light Agent-Richtlinieneinstellungen zu migrieren

1. Wählen Sie in der Verwaltungskonsole den Administrationsserver aus und öffnen Sie durch Rechtsklick das Kontextmenü.
2. Wählen Sie die Option **Alle Aufgaben → Assistent für das Massenkonvertieren von Richtlinien und Aufgaben** aus.

   Der „Assistent für das Massenkonvertieren von Richtlinien und Aufgaben“ wird gestartet. Folgen Sie den Anweisungen.

Schritt 1. Auswahl des Programms, für das Sie Richtlinien und Aufgaben konvertieren müssen

Bei diesem Schritt müssen Sie Kaspersky Endpoint Security für Windows auswählen. Weiter zum nächsten Schritt

Schritt 2. Konvertieren von Richtlinien

Wählen Sie die Richtlinie für Kaspersky Security for Virtualization 5.2 Light Agent für Windows aus, die Sie umwandeln möchten. Weiter zum nächsten Schritt

Der Migrations-Assistent beginnt mit der Richtlinienkonvertierung. Während der Konvertierung fordert der Migrations-Assistent Sie auf, die Bedingungen der KSN-Erklärung zu akzeptieren. Eine neue Richtlinie hat den Namen *<Richtlinie> (umgewandelt)*.

Schritt 3. Konvertieren von Aufgaben

Der Migrations-Assistent erstellt neue Aufgaben für Kaspersky Endpoint Security für Windows. Wählen Sie in der Aufgabenliste die KSVLA Light Agent-Aufgaben aus, die Sie für Kaspersky Endpoint Security erstellen möchten. Die neuen Aufgaben erhalten den Namen *<Name der Aufgabe> (konvertiert)*. Weiter zum nächsten Schritt

Schritt 4. Assistent abschließen

Schließen Sie den Assistenten ab.

Nach der Migration einer Richtlinie müssen Sie die Eigenschaften der Richtlinie öffnen, ihre Einstellungen überprüfen und die Richtlinie speichern. Wenn Sie diese Schritte nicht ausführen, ignoriert KES Light Agent die konvertierte Richtlinie möglicherweise.

Achten Sie insbesondere auf die Migration von Verbindungseinstellungen für die SVM von Light Agent, Ausnahmelisten, vertrauenswürdigen Apps, vertrauenswürdigen Webadressen und Regeln der Programmkontrolle.

Migration der Konfiguration [KSVLA Light Agent+KEA] zur Konfiguration [KES Light Agent+built-in agent]

Zur Unterstützung von Kaspersky Endpoint Security für Windows als Teil von EDR (KATA), EDR Optimum und Kaspersky Sandbox wurde der App ein integrierter Agent hinzugefügt. Das separate Programm „Kaspersky Endpoint Agent“ ist nicht mehr erforderlich, um diese Lösungen zu nutzen.

Bei der Migration von KSVLA Light Agent zu KES Light Agent funktionieren die Lösungen EDR (KATA), EDR Optimum und Kaspersky Sandbox weiterhin mit den integrierten Agents von Kaspersky Endpoint Security. Außerdem wird Kaspersky Endpoint Agent vom Computer entfernt.

Bevor Sie von KSVLA Light Agent zu KES Light Agent migrieren, müssen Sie alle Komponenten von Kaspersky Security for Virtualization auf Version 6.2 aktualisieren, auch den Schutzserver und den Integrationsserver. Einzelheiten zum Versions-Update der Lösung Kaspersky Security for Virtualization Light Agent finden Sie in der Hilfe zu Kaspersky Security for Virtualization Light Agent.

Die Migration der Konfiguration [KSVLA Light Agent+KEA] zur Konfiguration [KES Light Agent+built-in agent] umfasst die folgenden Schritte:

1. **Migration der Richtlinie und der Aufgaben**

Die Migration der Richtlinien und Aufgaben von [KSVLA Light Agent+KEA] zu [KES Light Agent+built-in agent] umfasst die folgenden Schritte:

1. Migration der Richtlinien und Aufgaben von KSVLA Light Agent zu KES Light Agent mit dem Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (nur in der Verwaltungskonsole (MMC) verfügbar).

   Dadurch wird eine neue Richtlinie mit dem Namen *<Richtlinie> (umgewandelt)* erstellt. Außerdem werden neue KES-Aufgaben mit den Namen *<Name der Aufgabe> (umgewandelt)* erstellt.

2. Migrieren von Richtlinien und Aufgaben von KEA zu KES mit dem Assistenten für die Migration von Kaspersky Endpoint Agent (nur in Web Console und Cloud Console verfügbar).

   Dadurch wird eine neue Richtlinie mit dem Namen *<Name der Kaspersky Endpoint Security-Richtlinie> & <Name der Kaspersky Endpoint Agent-Richtlinie>* erstellt. Außerdem werden neue Aufgaben und KES-Aufgaben erstellt.

2 Migration von KSVLA Light Agent zu KES Light Agent

Die Migration von KSVLA Light Agent zu KES Light Agent umfasst die Installation von KES Light Agent anstelle von KSVLA Light Agent.

Gewöhnlich aktivieren Administratoren den Kennwortschutz, um den Zugriff auf KSVLA Light Agent und KEA einzuschränken. Das Kennwort für die Deinstallation von KEA können Sie nur in den Eigenschaften der Aufgabe *Remote-Installation einer Anwendung* eingeben. Für die Migration müssen Sie den Kennwortschutz für KSVLA Light Agent deaktivieren.

Um die Migration durchzuführen, müssen Sie die Komponenten auswählen, die zur Unterstützung der Detection and Response-Lösungen als Teil von Kaspersky Endpoint Security erforderlich sind. Nach der Installation des Programms wechselt Kaspersky Endpoint Security zur Verwendung des integrierten Agenten und entfernt Kaspersky Endpoint Agent.

3 Lizenzverwaltung

Wenn das Programm im Light Agent-Modus verwendet wird, müssen Sie das Programm nicht aktivieren. Um das Programm zu aktivieren, müssen Sie einen Lizenzschlüssel zu der SVM hinzufügen. Außerdem müssen Sie der SVM den Lizenzschlüssel zur Aktivierung zusätzlicher Funktionen (z. B. EDR Optimum) hinzufügen. Die Lizenzierung der Funktionalität erfolgt bei der Migration also automatisch.

4 Status von Kaspersky Endpoint Detection and Response Optimum und Kaspersky Sandbox überprüfen

Falls der Computer nach dem Upgrade in der Kaspersky Security Center-Konsole den Status *Kritisch* hat:

- Stellen Sie sicher, dass auf dem Computer der Administrationsagent Version 13.2 oder höher installiert ist.
- Überprüfen Sie den Betriebsstatus des integrierten Agents. Sehen Sie sich dazu den *Bericht über den Status der Programmkomponenten* an. Wenn eine Komponente den Status *Nicht installiert* hat, installieren Sie die Komponente mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*.
- Vergessen Sie nicht, die Erklärung zu Kaspersky Security Network in der neuen Richtlinie für Kaspersky Endpoint Security für Windows zu akzeptieren.

- Stellen Sie mithilfe der Option *Bericht über den Status der Programmkomponenten* sicher, dass die EDR Optimum-Funktionalität aktiviert ist. Wird für eine Komponente der Status *Nicht durch Lizenz abgedeckt* angezeigt wird, stellen Sie sicher, dass die Funktionalität zur automatischen Verteilung von Lizenzschlüsseln in EDR Optimum aktiviert ist.

- Überprüfen Sie den Verbindungsstatus der virtuellen Maschine mit der SVM. Informationen über den Status der Verbindung von Light Agent mit einer SVM erhalten Sie in Kaspersky Endpoint Security oder über den Programmbefehl.

Programm über die Befehlszeile verwalten

Sie können Kaspersky Endpoint Security über die Befehlszeile verwalten. Eine Liste der Befehle für die Programmverwaltung erhalten Sie mithilfe des Befehls `avp.com HELP`. Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, geben Sie den Befehl `avp.com HELP <command>` ein.

Sonderzeichen im Befehl müssen mit Escape-Zeichen versehen werden. Für die Zeichen `&`, `|`, `(`, `)`, `<`, `>`, `^` dient `^` als Escape-Zeichen (Beispiel: Wenn Sie das Zeichen `&` verwenden möchten, geben Sie `^&` ein). Um das `%`-Zeichen als Escape-Zeichen zu versehen, geben Sie `%%` ein.

Anstelle des Werts `1` können die Werte `yes`, `on`, `enable`, `enabled` oder `true` verwendet werden. Anstelle des Werts `0` können die Werte `no`, `off`, `disable`, `disabled` oder `false` verwendet werden.

Setup. Programm installieren

Die Installation des Programms über die Befehlszeile umfasst die folgenden Schritte:

1. **Auswahl eines Programmpakets**

   Kaspersky stellt Programmpakete für verschiedene Lokalisierungen bereit, die mit unterschiedlichen CPU-Architekturen kompatibel sind und verschiedene Verschlüsselungsmodule enthalten.

   Zum Lieferumfang gehören die folgenden Programmpakete:

   - **AES256**

     Dieses Programmpaket ist für die Installation auf Computern mit x86/x64-Architektur vorgesehen. Dieses Programmpaket enthält Verschlüsselungs-Tools, die den AES-Verschlüsselungsalgorithmus (Advanced Encryption Standard) mit einer effektiven Schlüssellänge von 256 Bit realisieren.

   - **AES56**

     Dieses Programmpaket ist für die Installation auf Computern mit x86/x64-Architektur vorgesehen. Das Programmpaket enthält Verschlüsselungs-Tools, die den AES-Verschlüsselungsalgorithmus mit einer effektiven Schlüssellänge von 56 Bit realisieren.

   - **Arm64**

     Dieses Programmpaket ist für die Installation auf ARM-basierten Computern vorgesehen. Dieses Programmpaket ist nicht für die Installation auf Servern vorgesehen.

2. **Übertragen des Programmpakets in den Speicher des Computers**

   Das Programmpaket ist ein selbstentpackendes Archiv im EXE-Format. Wenn Sie den Inhalt des Programmpakets anzeigen möchten, müssen Sie das Archiv in einen separaten Ordner extrahieren. Für die Installation des Programms benötigen Sie alle Dateien aus dem Programmpaket, einschließlich der Datei bases.cab.

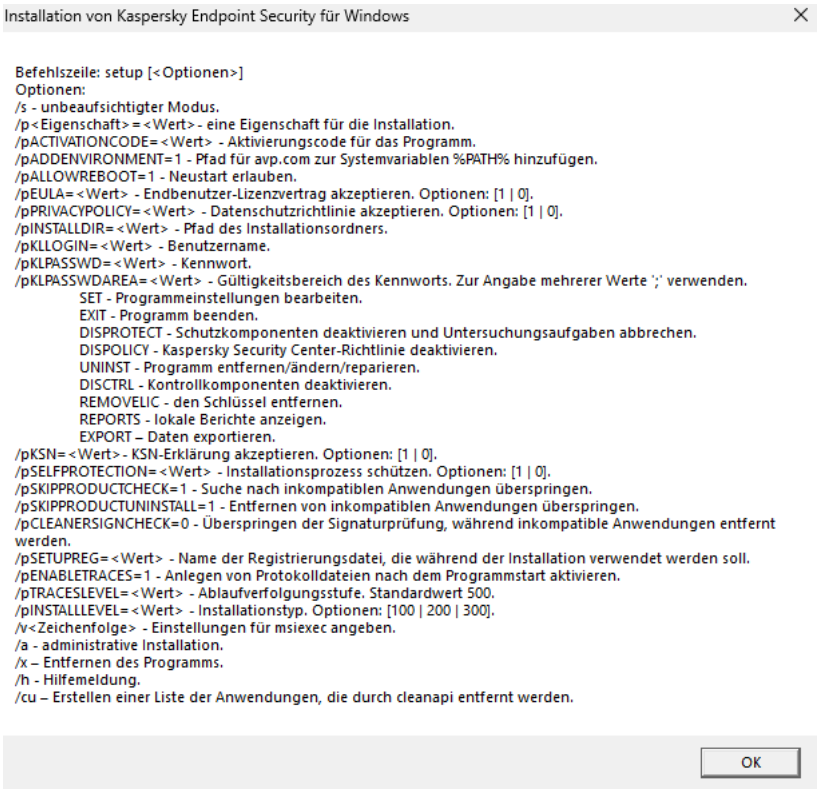
3. **Ausführen des Installationsbefehls**

Die Installation von Kaspersky Endpoint Security aus der Befehlszeile ist in einem der folgenden Modi möglich:

- Im interaktiven Modus mithilfe des Installationsassistenten des Programms
- Im unbeaufsichtigten Modus. Nach dem Start der Installation im unbeaufsichtigten Modus ist Ihre Beteiligung am Installationsvorgang nicht mehr erforderlich (unbeaufsichtigte Installation). Um das Programm im unbeaufsichtigten Modus zu installieren, verwenden Sie die Parameter `/s` und `/qn`.

Bevor Sie das Programm im unbeaufsichtigten Modus installieren, öffnen und lesen Sie bitte den Endbenutzer-Lizenzvertrag und den Text der Datenschutzrichtlinie. Der Endbenutzer-Lizenzvertrag und der Text der Datenschutzrichtlinie gehören zum Lieferumfang von Kaspersky Endpoint Security. Beginnen Sie nur dann mit der Programminstallation, wenn Sie die Bestimmungen und Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen haben, und sie verstehen und akzeptieren, wenn Sie verstehen und damit einverstanden sind, dass Ihre Daten gemäß der Datenschutzrichtlinie verarbeitet und weitergeleitet werden (einschließlich in Drittländer), und wenn Sie die Datenschutzrichtlinie vollständig gelesen haben und sie verstehen. Wenn Sie nicht mit den Bestimmungen und Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, installieren Sie Kaspersky Endpoint Security nicht und verwenden das Programm nicht.

Eine Liste der Befehle für die Programm-Installation erhalten Sie mithilfe des Befehls `/h`. Um Hilfe zur Installationsbefehlssyntax zu erhalten, geben Sie `setup_kes.exe /h` ein. Als Ergebnis zeigt das Installationsprogramm ein Fenster mit einer Beschreibung der Befehlsoptionen an (siehe Abbildung unten).



Beschreibung der Installationsbefehlsoptionen

Um das Programm zu installieren oder eine vorhergehende Programmversion zu aktualisieren, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.

3. Führen Sie den folgenden Befehl aus:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

oder

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

Dadurch wird das Programm auf dem Computer installiert. Mit dem Befehl `status` können Sie überprüfen, ob das Programm installiert ist und welche Programmeinstellungen festgelegt sind.

Installationseinstellungen für das Programm

`EULA=1`	Zustimmung zu den Bedingungen des Endbenutzer-Lizenzvertrags. Der Text des Lizenzvertrags ist im Lieferumfang von Kaspersky Endpoint Security enthalten. Die Bedingungen des Lizenzvertrags müssen akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
`PRIVACYPOLICY=1`	Zustimmung zu der Datenschutzrichtlinie. Der Text der Datenschutzrichtlinie gehört zum Lieferumfang von Kaspersky Endpoint Security. Die Datenschutzrichtlinie muss akzeptiert werden, damit das Programm oder ein Programm-Upgrade installiert werden kann.
`KSN`	Akzeptieren oder Ablehnen der Teilnahme an Kaspersky Security Network (KSN). Ist der Parameter nicht angegeben, so fordert Kaspersky Endpoint Security beim ersten Start des Programms eine Bestätigung der Teilnahme an KSN. Mögliche Werte: • `1` – Zustimmung zur Teilnahme an KSN. • `0` – Ablehnung der Teilnahme an KSN (Standardwert). Das Programmpaket für Kaspersky Endpoint Security ist für die Nutzung von Kaspersky Security Network optimiert. Falls Sie die Teilnahme an Kaspersky Security Network abgelehnt haben, aktualisieren Sie Kaspersky Endpoint Security sofort nach dem Abschluss der Installation.
`CONFIGPATH=<path to the configuration file>`	Installieren des Programms mit vordefinierten Einstellungen. Dazu müssen Sie eine Datei hochladen, welche die Einstellungen für Kaspersky Endpoint Security vorgibt. Sie können eine Konfigurationsdatei auf der lokalen Programmoberfläche erstellen.
`ALLOWREBOOT=1`	Automatischer Neustart des Computers nach der Installation oder Aktualisierung des Programms, falls erforderlich. Wenn dieser Parameter nicht angegeben ist, ist der automatische Neustart des Computers verboten. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Ein Neustart ist nur erforderlich, wenn vor der Installation inkompatible Programme gelöscht werden müssen. Ein Neustart kann auch bei einem Upgrade der Programmversion erforderlich sein.
`SKIPPRODUCTCHECK=1`	Deaktivieren der Überprüfung auf installierte Software. Eine Liste der Software, die Kompatibilitätsprobleme verursachen kann, befindet sich in der Datei „incompatible.txt“, die zum Lieferumfang gehört. Ist dieser Parameter nicht angegeben, so wird beim Fund von Software aus der Liste die Installation von Kaspersky Endpoint Security abgebrochen.

SKIPPRODUCTUNINSTALL=1	Deaktiviert das automatische Entfernen gefundener Anwendungen aus der Liste „incompatible.txt“. Wenn dieser Parameter nicht angegeben ist, versucht Kaspersky Endpoint Security, die Anwendungen zu entfernen, die Kompatibilitätsprobleme verursachen können. Das automatische Entfernen von Software kann nicht aktiviert werden, wenn Kaspersky Endpoint Security über den msiexec-Installer installiert wird. Um Anwendungen, die Kompatibilitätsprobleme verursachen können, automatisch zu entfernen, verwenden Sie die Datei „setup_kes.exe“.
CLEANERSIGNCHECK=0|1	Überprüft die digitalen Signaturen der gefundenen Softwaredateien aus der Liste „incompatible.txt“. Zum Entfernen von Software verwendet Kaspersky Endpoint Security die Installationsdatei der Software. Wenn die Installationsdatei keine digitale Signatur hat, betrachtet Kaspersky Endpoint Security die Datei als nicht vertrauenswürdig und beendet das Entfernen inkompatibler Software. Dadurch wird die Ausführung von potenziell schädlichem Code vermieden. Wenn die digitale Signatur der erkannten Software-Datei nicht überprüft werden kann, beendet Kaspersky Endpoint Security die Installation mit einem Fehler. Der Standardwert variiert je nach Methode der Software-Installation: • 0 bedeutet: Die Überprüfung von digitalen Signaturen ist deaktiviert (Standardwert bei Bereitstellung über Kaspersky Security Center). • 1 bedeutet: Die Überprüfung von digitalen Signaturen ist aktiviert (Standardwert bei der lokalen Installation der App).
STANDALONEMODE=1	Installation des Programms in der Konfiguration Endpoint Detection and Response Agent (EDR Agent) zur Integration in die Lösungen „Kaspersky Endpoint Detection and Response (KATA)“ und „Kaspersky Endpoint Detection and Response Expert (on-premises)“. Diese Konfiguration wird benötigt, wenn in Ihrem Unternehmen die Endpoint Protection Platform (EPP) eines Drittanbieters zusammen mit einer Lösung der Klasse „Kaspersky Endpoint Detection and Response (KATA)“ bereitgestellt wird. Dadurch wird sichergestellt, dass Kaspersky Endpoint Security in der Endpoint Detection and Response Agent-Konfiguration mit Drittanbieter-EPP-Anwendungen kompatibel ist.
KLLOGIN	Festlegen des Benutzernamens für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Komponente Kennwortschutz). Der Benutzername wird zusammen mit den Parametern KLPASSWD und KLPASSWDAREA festgelegt. Als Standard wird der Benutzername KLAdmin verwendet.
KLPASSWD	Festlegen des Kennworts für den Zugriff auf die Verwaltung der Funktionen und Einstellungen von Kaspersky Endpoint Security (Das Kennwort wird zusammen mit den Parametern KLLOGIN und KLPASSWDAREA festgelegt). Falls Sie ein Kennwort angegeben haben, aber mithilfe des Parameters KLLOGIN keinen Benutzernamen festgelegt haben, wird standardmäßig der Benutzername KLAdmin verwendet.
KLPASSWDAREA	Gibt den Gültigkeitsbereich des Kennworts für den Zugriff auf Kaspersky Endpoint Security an. Wenn der Benutzer versucht, eine Aktion aus diesem Bereich auszuführen, fragt Kaspersky Endpoint Security die Anmeldedaten des Benutzers ab (Parameter für KLLOGIN und KLPASSWD). Verwenden Sie das Zeichen „;“, um mehrere Werte anzugeben. Mögliche Werte: • SET – Änderung der Programmeinstellungen. • EXIT – Beenden des Programms. • DISPROTECT – Schutzkomponenten deaktivieren und Untersuchungsaufgaben abbrechen. • DISPOLICY – Richtlinie für Kaspersky Security Center deaktivieren. • UNINST – Programm vom Computer entfernen. • DISCTRL – Kontrollkomponenten deaktivieren. • REMOVELIC – Schlüssel entfernen. • REPORTS – Berichte anzeigen. • EXPORT – Programmeinstellungen exportieren. Beispiel: KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. Das KLAdmin-Benutzerkonto ist berechtigt, jede kennwortgeschützte Aktion auszuführen. Daher kann der Gültigkeitsbereich des Kennworts für das KLAdmin-Benutzerkonto nicht konfiguriert werden. Wenn Sie versuchen, den Gültigkeitsbereich des Kennworts für das KLAdmin-Benutzerkonto zu konfigurieren, verbietet das Programm die angegebenen Aktionen für die Gruppe „Alle“.
PROTECTOSSERVICES	Funktionalität zum Schutz von Betriebssystemdiensten. Der Schutz für Betriebssystemdienste verhindert, dass Drittanbieter-Programme den Betrieb von Betriebssystemdiensten stören. Zu diesen Diensten gehört beispielsweise der Autostart-Dienst für Programme. • 1 bedeutet, dass der Schutz für Betriebssystemdienste aktiviert ist (Standardwert). • 0 bedeutet, dass der Schutz für Betriebssystemdienste deaktiviert ist.

ENABLETRACES	Anwendungsnachverfolgung aktivieren oder deaktivieren. Nach dem Start von Kaspersky Endpoint Security werden Protokolldateien im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` gespeichert. Mögliche Werte: • `1` – Die Nachverfolgung ist aktiviert. • `0` – Die Nachverfolgung ist deaktiviert (Standardwert).
TRACESLEVEL	Genauigkeitsstufe der Ablaufverfolgung. Mögliche Werte: • `100` (kritisch). Nur Meldungen über fatale Fehler. • `200` (hoch). Meldungen über alle Fehler, einschließlich fatale. • `300` (Diagnose). Meldungen über alle Fehler, sowie Warnungen. • `400` (wichtig). Meldungen über alle Fehler, Warnungen, sowie zusätzliche Informationen. • `500` (normal). Meldungen über alle Fehler, Warnungen, sowie ausführliche Informationen über die Nutzung des Programms im normalen Modus (Standardwert). • `600` (niedrig). Alle Meldungen.
ENABLEAZURESUPPORT	Azure WVD-Kompatibilitätsmodus aktivieren oder deaktivieren. Mögliche Werte: • `1` – Azure WVD-Kompatibilitätsmodus ist aktiviert. • `0` – Azure WVD-Kompatibilitätsmodus ist deaktiviert (Standardwert). Diese Funktion sorgt dafür, dass der Status der virtuellen Azure-Maschine in der Kaspersky Anti Targeted Attack Platform-Konsole korrekt angezeigt wird. Zur Überwachung der Computerleistung sendet Kaspersky Endpoint Security Telemetriedaten an die KATA-Server. Die Telemetrie umfasst eine ID des Computers (Sensor ID). Mithilfe des Azure WVD-Kompatibilitätsmodus können Sie diesen virtuellen Computern eine permanente eindeutige Sensor ID zuweisen. Wenn der Kompatibilitätsmodus deaktiviert ist, ändert sich die Sensor ID aufgrund der Funktionsweise von virtuellen Azure-Maschinen möglicherweise nach dem Neustart des Computers. Dies kann dazu führen, dass in der Konsole Duplikate von virtuellen Maschinen angezeigt werden.
AMPPL	Aktivierung oder Deaktivierung des Schutzes für Prozesse von Kaspersky Endpoint Security unter Verwendung der Technologie AM-PPL (Antimalware Protected Process Light). Details über die AM-PPL-Technologie finden Sie auf der Microsoft-Website. Die AM-PPL-Technologie ist verfügbar für die Betriebssysteme Windows 10 Version 1703 (RS2) und höher, sowie für Windows Server 2019. Mögliche Werte: • `1` – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist aktiviert (Standardwert). • `0` – Der Schutz für Prozesse von Kaspersky Endpoint Security unter Verwendung der AM-PPL-Technologie ist deaktiviert.
UPGRADEMODE	Modus für das Programm-Upgrade: • `Seamless` bedeutet, beim Programm-Upgrade wird ein Computerneustart durchgeführt (Standardwert). • `Force` bedeutet, das Programm-Upgrade wird ohne Neustart durchgeführt. 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. Bei der Installation von Kaspersky Endpoint Security ist kein Neustart erforderlich. Der Upgrade-Modus für die App wird in den App-Einstellungen angegeben. Sie können diese Einstellung in den App-Einstellungen oder in der Richtlinie ändern. Wenn die App bereits installiert ist und ein Upgrade durchgeführt wird, hat der Befehlszeilenparameter eine niedrigere Priorität als der Parameter, der in den App-Einstellungen oder in der Datei setup.ini angegeben ist. Wenn beispielsweise der Upgrade-Modus `Force` in der Befehlszeile angegeben ist und der Modus `Seamless` in den App-Einstellungen, wird das Upgrade mit einem Neustart des Computers installiert (`Seamless`).
RESTAPI	Programmverwaltung über eine REST API. Für die Programmverwaltung über eine REST API muss ein Benutzername angegeben werden (Parameter `RESTAPI_User`). Mögliche Werte: • `1` – Die Verwaltung über eine REST API ist erlaubt. • `0` – Die Verwaltung über eine REST API ist verboten (Standardwert). Für die Programmverwaltung über eine REST API muss die Verwaltung mithilfe von Administrationssystemen erlaubt sein. Legen Sie dazu den Parameter `AdminKitConnector=1` fest. Wenn Sie das Programm über eine REST API verwalten, kann das Programm nicht mithilfe der Kaspersky-Administrationssysteme verwaltet werden.
RESTAPI_User	Benutzername des Windows-Domänen-Benutzerkontos für die Programmverwaltung über eine REST API. Die Programmverwaltung über eine REST API ist nur für diesen Benutzer verfügbar. Geben Sie den Benutzernamen im Format `<DOMAIN>\<UserName>` an (z. B. `RESTAPI_User=COMPANY\Administrator`). Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen. Eine Voraussetzung für die Programmverwaltung über eine REST API ist, dass ein Benutzername hinzugefügt wird.
RESTAPI_Port	Port für die Programmverwaltung über eine REST API. Als Standard wird Port 6782 verwendet. Stellen Sie sicher, dass der Port frei ist.
RESTAPI_Certificate	Zertifikat zur Identifizierung von Anfragen (z. B. `RESTAPI_Certificate=C:\cert.pem`). Für die sichere Interaktion von Kaspersky Endpoint Security mit dem REST-Client muss die Anfrage-Identifikation konfiguriert werden. Dazu müssen Sie ein Zertifikat installieren und anschließend die Nutzdaten jeder Anfrage signieren.

`ADMINKITCONNECTOR`	Programmverwaltung mithilfe von Administrationssystemen. Zu den Administrationssystemen zählt beispielsweise Kaspersky Security Center. Sie können Kaspersky-Administrationssysteme oder Lösungen von Drittanbietern verwenden. Kaspersky Endpoint Security bietet eine entsprechende API. Mögliche Werte: • `1` – Die Programmverwaltung mithilfe von Administrationssystemen ist erlaubt (Standardwert). • `0` – Die Programmverwaltung ist nur über die lokale Schnittstelle erlaubt.
`EnableUniqueSensorID`	Eindeutige Computer-ID (Sensor ID) erstellen, während das Programm installiert oder aktualisiert wird. Sensor ID wird in der Lösung Kaspersky Anti Targeted Attack Platform verwendet, um Computer zu identifizieren, die Telemetriedaten an den Server senden. Beim Erstellen einer Sensor ID berücksichtigt ein Algorithmus die Konfiguration des Computers, beispielsweise die Motherboard-Seriennummer. In einigen Fällen, beispielsweise bei der Verwendung des Programms in einer virtuellen Umgebung, kann die Sensor ID doppelt vorhanden sein. Dies hat zur Folge, dass Kaspersky Anti Targeted Attack Platform den Computer, von dem Telemetriedaten gesendet werden, nicht identifizieren kann. Um eine eindeutige Sensor ID zu erstellen, müssen Sie den Parameter `EnableUniqueSensorID=1` angeben. In diesem Fall verwendet das Programm beim Erstellen der Sensor ID einen anderen Algorithmus, der andere Daten über den Computer berücksichtigt. Dadurch wird eine eindeutige Sensor ID erzeugt. Dieser Parameter ist standardmäßig nicht festgelegt. Das Programm erbt die Sensor ID in den folgenden Fällen: • Aktualisierung der Programmversion • Migration der Konfiguration [KES+KEA] zur Konfiguration [KES+built-in agent]. Im Rahmen einer Programmreparatur versucht das Installationsprogramm, die Sensor ID zu vererben. Wenn die Sensor ID nicht wiederhergestellt werden kann, erstellt das Programm eine neue Sensor ID.
`SKIPKB5007186CHECK=1`	Suche nach dem installierten Betriebssystem-Update KB5007186 deaktivieren. Bevor das Programm wird installiert, überprüft das Installationsprogramm die installierten Betriebssystem-Updates. Das Update KB5007186 gehört zu den Betriebssystem-Updates, die Probleme mit dem Programm verursachen können. Ausführliche Informationen finden Sie in der Wissensdatenbank der Technischen Supports. Wenn dieses Update gefunden wird, bricht das Installationsprogramm die Installation ab. Um die Installation fortzusetzen, legen Sie den Wert `SKIPKB5007186CHECK=1` fest.

Beispiel

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Nach der Installation des Programms Kaspersky Endpoint Security erfolgt die Aktivierung im Rahmen einer Testlizenz, es sei denn, Sie haben in der Datei setup.ini einen Aktivierungscode angegeben. Die Testlizenz ist in der Regel nur für eine kurze Zeit gültig. Nach Ablauf der Testlizenz stellt Kaspersky Endpoint Security die Funktion ein. Um die App weiterhin nutzen zu können, müssen Sie die App mit einer kommerziellen Lizenz aktivieren, entweder mithilfe des App-Aktivierungs-Assistenten oder durch einen speziellen Befehl.

Bei der Installation oder beim Upgrade des Programms im unbeaufsichtigten Modus wird die Verwendung folgender Dateien unterstützt:

- setup.ini – allgemeine Installationseinstellungen für die App.

  Um Einstellungen aus der Datei setup.ini zu übernehmen, legen Sie diese Datei im Ordner mit dem Programmpaket für Kaspersky Endpoint Security ab.

- install.cfg – Einstellungen für das Programm Kaspersky Endpoint Security

  Um Einstellungen aus der Konfigurationsdatei install.cfg zu übernehmen, müssen Sie den Dateipfad im folgenden Befehl zur Programminstallation angeben: `CONFIGPATH=<path to the configuration file>`.

- setup.reg – Registrierungsschlüssel.

  Registrierungsschlüssel aus der Datei setup.reg werden nur dann in die Registrierung eingetragen, wenn in der Datei setup.ini der Wert `setup.reg` für den Parameter `SetupReg` angegeben ist. Die Datei setup.reg wird von den Kaspersky-Experten erstellt. Es wird davon abgeraten, den Inhalt dieser Datei zu ändern. Um Einstellungen aus der Datei setup.reg zu übernehmen, legen Sie diese Datei im Ordner mit dem Programmpaket für Kaspersky Endpoint Security ab. Sie können die Datei setup.reg auch in einem anderen Ordner ablegen. Wenn Sie dies tun, müssen Sie den Pfad zu der Datei im folgenden Programmsinstallationsbefehl angeben: `SETUPREG=<path to the setup.reg file>`.

Setup /x. Die App entfernen

Für die Deinstallation von Kaspersky Endpoint Security aus der Befehlszeile gibt es die folgenden Modi:

- Im interaktiven Modus mithilfe des Installationsassistenten des Programms
- Im unbeaufsichtigten Modus. Nach dem Start der Deinstallation im unbeaufsichtigten Modus ist Ihre Beteiligung am Deinstallationsvorgang nicht mehr erforderlich (unbeaufsichtigte Deinstallation). Um das Programm im unbeaufsichtigten Modus zu entfernen, verwenden Sie die Parameter `/s` und `/qn`.

Um das Programm im unbeaufsichtigten Modus zu entfernen, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:

   - Wenn der Deinstallationsvorgang nicht kennwortgeschützt ist:

     ```
     setup_kes.exe /s /x
     ```

     oder

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` ist die einmalige Programm-ID. Die Programm-GUID können Sie in der Wissensdatenbank des Technischen Supports oder mithilfe des folgenden Befehls ermitteln:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - Wenn der Deinstallationsvorgang kennwortgeschützt ist:

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     oder

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

Sie können auch den Parameter `SAVEQB` verwenden, um Dateien zu speichern, die vom Programm untersucht und ins Backup verschoben wurden. Backup-Kopien von Dateien werden im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` gespeichert. Das Speichern von Dateien im Backup ist standardmäßig deaktiviert (`SAVEQB=0`).

Beispiel

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. Programm wiederherstellen

Bei der Wiederherstellung überprüft das Programm die Integrität aller beschädigten Programm-Module und Systemregistrierungsschlüssel, die während der Programm-Installation erstellt wurden, und stellt diese wieder her.

Die Wiederherstellung von Kaspersky Endpoint Security aus der Befehlszeile ist in einem der folgenden Modi möglich:

- Im interaktiven Modus mithilfe des Installationsassistenten des Programms
- Im unbeaufsichtigten Modus. Nachdem die Wiederherstellung im unbeaufsichtigten Modus gestartet wurde, ist Ihre Beteiligung am Wiederherstellungsvorgang nicht mehr erforderlich.

Wenn das Installationsprogramm von Kaspersky Endpoint Security im Wiederherstellungsmodus ausgeführt wird und das Programm keine Wiederherstellung benötigt, nimmt das Installationsprogramm keine Änderungen vor.

Wenn das Installationsprogramm von Kaspersky Endpoint Security im Wiederherstellungsmodus ausgeführt wird und das Programm nicht installiert ist, startet das Installationsprogramm den Installationsprozess.

So stellen Sie das Programm im unbeaufsichtigten Modus wieder her:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security befindet.
3. Führen Sie den folgenden Befehl aus:
   - Wenn der Wiederherstellungsprozess nicht kennwortgeschützt ist:

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     `<GUID>` ist die einmalige Programm-ID. Die Programm-GUID können Sie in der Wissensdatenbank des Technischen Supports oder mithilfe des folgenden Befehls ermitteln:

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

- Wenn der Wiederherstellungsprozess kennwortgeschützt ist:

```
msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
```

Beispiel

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

AVP-Befehle

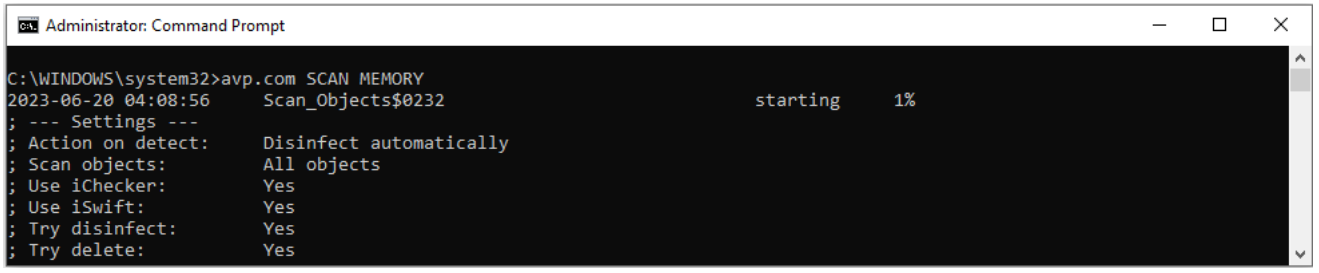
Um Kaspersky Endpoint Security über die Befehlszeile zu verwalten, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

   Den Pfad zur ausführbaren Datei können Sie während der Installation der Anwendung zur Systemvariablen %PATH% hinzufügen.
3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

```
avp.com <command> [options]
```

Dann führt Kaspersky Endpoint Security den Befehl aus (siehe Abbildung unten).



Programm über die Befehlszeile verwalten

SCAN. Schadsoftware-Untersuchung

Aufgabe *Schadsoftware-Untersuchung* starten

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report
file>] [<scan technologies>] [/C:<file with scan settings>]
```

Untersuchungsbereich	
`<files to scan>`	Liste mit Dateien und Ordner, durch Leerzeichen getrennt. Lange Pfade müssen in Anführungszeichen gesetzt werden. Kurze Pfade (Formate MS-DOS) müssen nicht in Anführungszeichen stehen. Beispielsweise: • `"C:\Program Files (x86)\Example Folder"` – langer Pfad. • `C:\PROGRA~2\EXAMPL~1` – kurzer Pfad.
`/ALL`	Aufgabe *Schadsoftware-Untersuchung* starten. Kaspersky Endpoint Security untersucht folgende Objekte: • Kernel-Speicher • Objekte, die beim Hochfahren des Betriebssystems geladen werden • Bootsektoren • Backup des Betriebssystems • alle Festplatten und Wechseldatenträger In Kaspersky Endpoint Security für Windows 12.12 sind E-Mail-Nachrichten aus dem Untersuchungsbereich des Programms ausgeschlossen. Die Untersuchung ein- und ausgehender E-Mail-Nachrichten wird von der Komponente „Schutz vor E-Mail-Bedrohungen“ ausgeführt. Wenn Sie eine ältere Version des Verwaltungs-Plug-ins verwenden, schließt das Programm E-Mail-Nachrichten aus dem Untersuchungsbereich aus, selbst wenn diese durch die Richtlinie eingeschlossen werden.
`/MEMORY`	Untersuchung des Kernel-Speichers
`/STARTUP`	Untersuchung der Objekte, die beim Hochfahren des Betriebssystems geladen werden
`/REMDRIVES`	Wechseldatenträger untersuchen.
`/FIXDRIVES`	Festplatten untersuchen.
`/NETDRIVES`	Netzlaufwerke untersuchen.
`/QUARANTINE`	Dateien im Backup von Kaspersky Endpoint Security untersuchen.
`/@:<file list.lst>`	Untersuchung der Dateien und Ordner, die in der Liste angegeben sind. Jede Datei in der Liste muss in einer separaten Zeile stehen. Lange Pfade müssen in Anführungszeichen gesetzt werden. Kurze Pfade (Formate MS-DOS) müssen nicht in Anführungszeichen stehen. Beispielsweise: • `"C:\Program Files (x86)\Example Folder"` – langer Pfad. • `C:\PROGRA~2\EXAMPL~1` – kurzer Pfad.

Aktion beim Fund einer Bedrohung	
`/i0`	**Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.
`/i1`	**Desinfizieren – Informieren, wenn Desinfektion fehlschlägt**. Bei Auswahl dieser Option versucht Kaspersky Endpoint Security automatisch, alle gefundenen infizierten Dateien zu desinfizieren. Wenn die Desinfektion fehlschlägt, fügt Kaspersky Endpoint Security Informationen über die gefundenen infizierten Dateien zur Liste der aktiven Bedrohungen hinzu.
`/i2`	**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. Diese Aktion ist standardmäßig ausgewählt.
`/i3`	**Löschen, wenn Desinfektion fehlschlägt**. Auch zusammengesetzte Dateien (z. B. Archive) löschen, wenn die infizierte Datei nicht desinfiziert oder gelöscht werden kann.
`/i4`	**Löschen**. Auch zusammengesetzte Dateien (z. B. Archive) löschen, wenn die infizierte Datei nicht gelöscht werden kann.

Dateitypen	
`/fe`	**Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.

`/fi`	**Dateien nach Format untersuchen**. 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.
`/fa`	**Alle Dateien**. Bei Auswahl dieser Option untersucht das Programm ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). Diese Option ist standardmäßig voreingestellt.

Untersuchungsausnahmen	
`-e:a`	Archive der Formate RAR, ARJ, ZIP, CAB, LHA, JAR, ICE von der Untersuchung ausschließen.
`-e:<file mask>`	Dateien nach einer Maske von der Untersuchung ausschließen. Beispielsweise: • Die Maske `*.exe` umfasst alle Pfade von Dateien mit der Erweiterung exe. • Die Maske `example*` umfasst alle Pfade von Dateien mit dem Namen EXAMPLE.
`-e:<seconds>`	Dateien, deren Untersuchung die in Sekunden vorgegebene Dauer überschreitet, von der Untersuchung ausschließen.
`-es:<megabytes>`	Dateien, deren Größe den in Megabyte vorgegebenen Wert überschreitet, von der Untersuchung ausschließen.

Ereignisse im Berichtsdateimodus speichern (nur für die Profile Untersuchung, Updater und Rollback)	
`/R:<report file>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<report file>`	Alle Ereignisse in der Berichtsdatei speichern.

Untersuchungstechnologien	
`/iChecker=on|off`	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).
`/iSwift=on|off`	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.

Erweiterte Einstellungen	
`/C:<file with scan settings>`	Datei mit Einstellungen für die Aufgabe *Schadsoftware-Untersuchung*. Die Datei muss manuell erstellt und im TXT-Format gespeichert werden. Die Datei kann den folgenden Inhalt haben: `[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]`.

Beispiel

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Update der Datenbanken und Programm-Module

Aufgabe *Update der Datenbanken und Programm-Module* starten

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

Befehlssyntax

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

Einstellungen für Update-Aufgaben	
`local`	Starten der Aufgabe *Update der Datenbanken und Programm-Module*, die nach der Programminstallation automatisch erstellt wurde. Sie können die Einstellungen der *Update der Datenbanken und Programm-Module*-Aufgabe auf der lokalen Programmoberfläche oder in Kaspersky Security Center-Konsole ändern. Wenn diese Einstellung nicht konfiguriert ist, startet Kaspersky Endpoint Security die *Update der Datenbanken und Programm-Module*-Aufgabe mit den Standardeinstellungen oder mit den im Befehl angegebenen Einstellungen. Sie können die Einstellungen der *Update der Datenbanken und Programm-Module*-Aufgabe wie folgt konfigurieren: • `UPDATE` startet die *Update der Datenbanken und Programm-Module*-Aufgabe mit den Standardeinstellungen: Als Update-Quelle dienen die Kaspersky-Update-Server, das Benutzerkonto ist System und es gelten weitere Standardeinstellungen. • `UPDATE local` startet die *Update der Datenbanken und Programm-Module*-Aufgabe, die nach der Installation automatisch erstellt wurde (vordefinierte Aufgabe). • `UPDATE <update settings>` startet die *Update der Datenbanken und Programm-Module*-Aufgabe mit manuell festgelegten Einstellungen (siehe unten).

Update-Quelle	
`"<update source>"`	Adresse eines HTTP- oder FTP-Servers oder eines gemeinsamen Ordners mit dem Update-Paket. Sie können nur eine Update-Quelle angeben. Wenn die Update-Quelle nicht angegeben wird, verwendet Kaspersky Endpoint Security die Standardquelle: Kaspersky Update-Server.

Ereignisse im Berichtsdateimodus speichern (nur für die Profile Untersuchung, Updater und Rollback)	
`/R:<report file>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<report file>`	Alle Ereignisse in der Berichtsdatei speichern.

Erweiterte Einstellungen	
`/C:<file with update settings>`	Datei mit Einstellungen für die Aufgabe *Update der Datenbanken und Programm-Module*. Die Datei muss manuell erstellt und im TXT-Format gespeichert werden. Die Datei kann den folgenden Inhalt haben: `["<update source>"] [/R[A]:<report file>]`.

Beispiel

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Rollback des letzten Updates

Letztes Update der Antiviren-Datenbanken rückgängig machen. Dadurch besteht die Möglichkeit, bei Bedarf zur Verwendung der vorherigen Datenbanken und Programm-Module zurückzukehren. Dies ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, welche dazu führt, dass Kaspersky Endpoint Security ein harmloses Programm blockiert.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

Befehlssyntax

```
avp.com ROLLBACK [/R[A]:<report file>]
```

Ereignisse im Berichtsdateimodus speichern (nur für die Profile Untersuchung, Updater und Rollback)	
`/R:<report file>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<report file>`	Alle Ereignisse in der Berichtsdatei speichern.

Beispiel

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Protokollierung

Protokolldateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden endgültig gelöscht, wenn das Programm entfernt wird. Protokolldateien werden im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` gespeichert. Eine Ausnahme bilden die Protokolldateien des Authentifizierungsagenten. Die Protokollierung ist standardmäßig deaktiviert.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

Ablaufverfolgungsstufe	
`<tracing level>`	Genauigkeitsstufe der Ablaufverfolgung. Mögliche Werte: • `100` (kritisch). Nur Meldungen über fatale Fehler. • `200` (hoch). Meldungen über alle Fehler, einschließlich fatale. • `300` (Diagnose). Meldungen über alle Fehler, sowie Warnungen. • `400` (wichtig). Meldungen über alle Fehler, Warnungen, sowie zusätzliche Informationen. • `500` (normal). Meldungen über alle Fehler, Warnungen, sowie ausführliche Informationen über die Nutzung des Programms im normalen Modus (Standardwert). • `600` (niedrig). Alle Meldungen.

Erweiterte Einstellungen	
`all`	Befehl mit den Parametern `file` und `mem` ausführen.
`file`	Eine einzige Protokolldatei speichern (ohne Größenbeschränkung).
`rot`	Ablaufverfolgungsergebnisse in einer beschränkten Anzahl von Dateisätzen mit beschränkter Größe speichern und alte Dateien überschreiben, wenn die maximale Größe erreicht wird.
`mem`	Protokollierungsergebnisse in Dump-Dateien speichern.

Beispiel

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. Ein Profil starten

Starten eines Profils (z. B. Starten eines Datenbanken-Updates oder Aktivieren einer Schutzkomponente).

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com START <profile> [/R[A]:<report file>]
```

Profil	
`<profile>`	Profilname. Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP START`.

Ereignisse im Berichtsdateimodus speichern (nur für die Profile Untersuchung, Updater und Rollback)	
`/R:<report file>`	Nur kritische Ereignisse in der Berichtsdatei speichern.
`/RA:<report file>`	Alle Ereignisse in der Berichtsdatei speichern.

Beispiel

```
avp.com START Scan_Objects
```

STOP. Profil beenden

Beenden der Profilausführung (z. B. Beenden einer Untersuchung von Wechseldatenträgern oder Deaktivieren einer Schutzkomponente).

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigungen **Schutzkomponenten deaktivieren** und **Kontrollkomponenten deaktivieren** haben.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Profilname. Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP STOP`.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

STATUS. Status des Profils

Informationen über den Status von Programmprofilen anzeigen (z. B. `running` oder `completed`). Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP STATUS`.

Außerdem zeigt Kaspersky Endpoint Security Informationen über den Status von Dienstprofilen an. Informationen über den Status von Dienstprofilen können erforderlich sein, wenn Sie sich an den Technischen Support von Kaspersky wenden.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com STATUS [<profile>]
```

Wenn Sie den Befehl ohne ein Profil eingeben, zeigt Kaspersky Endpoint Security den Status für alle Profile des Programms an.

STATISTICS. Ausführungsstatistik für das Profil

Anzeigen von Statistiken für ein Programmprofil (z. B. Untersuchungsdauer oder Anzahl der gefundenen Bedrohungen). Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP STATISTICS`.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com STATISTICS <profile>
```

RESTORE. Dateien aus dem Backup wiederherstellen

Wiederherstellen einer Datei aus dem Backup am ursprünglichen Speicherort. Wenn am angegeben Pfad bereits eine Datei mit diesem Namen vorhanden ist, fragt die App, ob die Datei ersetzt werden soll. Die wiederherzustellende Datei wird mit ihrem ursprünglichen Namen kopiert.

> Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Aus dem Backup wiederherstellen** besitzen.

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 Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` gespeichert.

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.

> In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Erweiterte Einstellungen	
`/REPLACE`	Vorhandene Datei überschreiben.
`<file name>`	Name der wiederherzustellenden Datei.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT. Programmeinstellungen exportieren

Exportieren Sie die Einstellungen für Kaspersky Endpoint Security in eine Datei. Wenn der Befehl nur den Namen der Datei enthält, in die Sie die Einstellungen exportieren möchten, legt das Programm die Datei wie folgt ab:

- Wenn der Pfad zu avp.com zu der Systemvariablen %PATH% hinzugefügt wird, legt das Programm die Datei im Ordner `C:\Windows\SysWOW64` ab.
- Wenn Sie den Befehl im Installationsordner des Programms ausführen, schlägt der Export fehl, da der Selbstschutz des Programms das Erstellen einer neuen Datei im Programmordner blockiert. Um die Programmeinstellungen in eine Datei zu exportieren, geben Sie den Dateipfad ein.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Einstellungen exportieren** besitzen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

Profil	
`<profile>`	Profilname. Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `HELP EXPORT`.

Datei für den Export	
`<file name>`	Name der Datei, in welche die Profileinstellungen exportiert werden sollen. Außerdem können Sie den Dateipfad auch eingeben. Sie können die Profileinstellungen in eine Konfigurationsdatei im DAT- oder CFG-Format, in eine Textdatei im TXT-Format oder in ein Dokument im XML-Format exportieren.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. Programmeinstellungen importieren

Importieren der Einstellungen für Kaspersky Endpoint Security aus einer Datei, die mit dem Befehl `EXPORT` erstellt wurde.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **App-Einstellungen anpassen** besitzen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

Datei für den Import	
`<file name>`	Name der Datei, aus welcher die Programmeinstellungen importiert werden sollen. Sie können die Einstellungen für Kaspersky Endpoint Security aus einer Konfigurationsdatei im DAT- oder CFG-Format, einer Textdatei im TXT-Format oder einem Dokument im XML-Format importieren.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY. Schlüsseldatei übernehmen

Aktivieren von Kaspersky Endpoint Security mit einer Schlüsseldatei. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

Befehlssyntax

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

Schlüsseldatei	
`<file name>`	Name der Schlüsseldatei.

Autorisierung	
`/login=<user name> /password= <password>`	Daten des Benutzerkontos. Die Daten des Benutzerkontos müssen nur eingegeben werden, wenn der Kennwortschutz aktiviert ist.

Beispiel

```
avp.com ADDKEY file.key
```

LICENSE. Lizenzverwaltung

Verwalten der Lizenzschlüssel für Kaspersky Endpoint Security, EDR Optimum oder EDR Expert (Add-on für Kaspersky Endpoint Detection and Response).

Damit der Befehl zum Löschen eines Lizenzschlüssels ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Schlüssel löschen** besitzen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

Befehlssyntax

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

Vorgang	
`/ADD <file name>`	Aktivieren von Kaspersky Endpoint Security mit einer Schlüsseldatei. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.
`/ADD <activation code>`	Kaspersky Endpoint Security mithilfe eines Aktivierungscodes aktivieren. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.
`/REFRESH`	Aktualisierung des Status der Lizenz für Kaspersky Endpoint Security. Dadurch erhält das Programm von den Kaspersky-Aktivierungsservern aktuelle Informationen zum Lizenzstatus.
`/REFRESH <license ID>`	Aktualisierung des Status der Lizenzen, die diese Lizenz-ID verwenden. Mit diesem Befehl können Sie den Status des EDR-Add-ons, des MDR-Add-ons, des KUMA-Add-ons oder anderer Lizenzen aktualisieren. Die Lizenz-ID können Sie im Lizenzzertifikat nachsehen. Dadurch erhält das Programm von den Kaspersky-Aktivierungsservern aktuelle Informationen zum Lizenzstatus.
`/CHECK`	Lizenzinformationen abrufen. Kaspersky Endpoint Security zeigt Informationen über alle hinzugefügten Lizenzschlüssel an, also auch über Reserveschlüssel, Schlüssel für EDR-Add-on, MDR-Add-on, KUMA-Add-on und andere Schlüssel. Für Kaspersky Endpoint Security werden die folgenden Lizenzinformationen angezeigt: • Name der Lizenz • Lizenz-ID • Adresse des Schutzservers (SVM), mit dem die virtuelle Maschine verbunden ist, auf der das Programm im Light Agent-Modus installiert ist • Lizenztyp: Test, kommerziell, Beta oder Abonnement • Datum und Uhrzeit der Programmaktivierung • Datum und Uhrzeit des Ablaufs der Lizenz • Tage bis zum Ablauf der Lizenz.
`/CHECK <license ID>`	Lizenzinformationen nach ID abrufen. Mit diesem Befehl können Sie Lizenzinformationen abrufen. Die Lizenz-ID können Sie im Lizenzzertifikat nachsehen.
`/DEL /login=<user name> /password= <password>`	Entfernen des Lizenzschlüssels für das Programm. Der Reserveschlüssel wird ebenfalls gelöscht.
`/DEL <license ID> /login=<user name> /password=<password>`	Löschen des Schlüssels, der diese Lizenz-ID verwendet. Mit diesem Befehl können Sie einen Schlüssel aus dem EDR-Add-on, MDR-Add-on, KUMA-Add-on oder aus anderen Lizenzen löschen. Die Lizenz-ID können Sie im Lizenzzertifikat nachsehen.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

Beispiel

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. Lizenz kaufen

Öffnen der Kaspersky-Website, um eine Lizenz zu kaufen oder Ihre Lizenz zu verlängern.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

PBATESTRESET. Untersuchungsergebnisse vor der Datenträgerverschlüsselung zurücksetzen

Zurücksetzen der Überprüfungsergebnisse für die Unterstützung der vollständigen Festplattenverschlüsselung (FDE) mithilfe der Kaspersky-Festplattenverschlüsselung und der BitLocker-Laufwerkverschlüsselung.

Vor dem Start der vollständigen Festplattenverschlüsselung führt das Programm eine Reihe von Untersuchungen aus. Dabei wird überprüft, ob der Computer verschlüsselt werden kann. Wenn eine vollständige Festplattenverschlüsselung nicht möglich ist, speichert Kaspersky Endpoint Security Informationen über die Inkompatibilität. Beim nächsten Verschlüsselungsversuch führt das Programm keine Überprüfung aus und warnt davor, dass eine Verschlüsselung nicht möglich ist. Wenn die Hardware-Konfiguration des Computers verändert wurde und anschließend die Systemfestplatte auf Kompatibilität mit der Technologie Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung überprüft werden soll, müssen zuerst die Inkompatibilitätsinformationen zurückgesetzt werden, die das Programm bei der vorherigen Überprüfung ermittelt hat.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

EXIT. Programm beenden

Kaspersky Endpoint Security beenden. Das Programm wird aus dem Arbeitsspeicher des Computers entladen.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **App beenden** besitzen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY. Richtlinie deaktivieren.

Richtlinie für Kaspersky Security Center auf dem Computer deaktivieren. Alle Einstellungen für Kaspersky Endpoint Security können angepasst werden, einschließlich jener Einstellungen, die in der Richtlinie ein geschlossenen Schloss (🔒) haben.

> Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Richtlinie für Kaspersky Security Center deaktivieren** besitzen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY. Richtlinie aktivieren

Aktivieren der Richtlinie für Kaspersky Security Center auf dem Computer. Die Programmeinstellungen werden gemäß der Richtlinie angepasst.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

DISABLE. Schutz deaktivieren

Deaktivierung des „Schutzes vor bedrohlichen Dateien“ auf einem Computer mit einer abgelaufenen Lizenz für Kaspersky Endpoint Security. Dieser Befehl kann nicht ausgeführt werden auf einem Computer, auf dem das Programm nicht aktiviert ist oder auf dem eine aktuelle Lizenz vorliegt.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

SPYWARE. Spyware erkennen

Verwalten der Spyware-Erkennung. Die Spyware-Erkennung ist standardmäßig aktiviert.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com SPYWARE on|off
```

KSN. Zwischen KSN / KPSN umschalten

Auswahl einer Kaspersky-Lösung zur Ermittlung der Reputation von Dateien und Websites. Kaspersky Endpoint Security unterstützt die folgenden Infrastrukturlösungen für die Arbeit mit Kaspersky-Reputationsdatenbanken:

- 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.

  - Die Übertragung von Daten aus dem Land ihres Standorts oder aus dem Unternehmens-LAN ist rechtlich oder durch Unternehmenssicherheitsrichtlinien untersagt.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

Befehlssyntax

```
avp.com KSN /global | /private <file name>
```

Konfigurationsdatei von Kaspersky Security Network	
`<file name>`	Name der Konfigurationsdatei mit den Einstellungen von Kaspersky Private Security Network. Diese Datei hat die Erweiterung PKCS7 oder PEM.

Beispiel

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

Beispiel

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. Den Schutz der Serververbindung deaktivieren

Ausführen der Aufgabe *Schutz der Verbindung zum Administrationsserver*, die das Kennwort für die Verbindung des Computers zum Administrationsserver entfernt. Die Aufgabe deaktiviert also den Schutz der Verbindung zum Administrationsserver.

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

Kennwort	
`/password=<password>`	Das Kennwort des Benutzerkontos KLAdmin oder das Kennwort aus der Aufgabe *Schutz der Verbindung zum Administrationsserver*. Wenn der Parameter nicht angegeben ist, werden Sie von Kaspersky Endpoint Security aufgefordert, in der nächsten Zeile ein Kennwort einzugeben.

KESCLI-Befehle

Mit KESCLI-Befehlen können Sie unter Verwendung der OPSWAT-Komponente Informationen über den Status des Computerschutzes erhalten und Standardaufgaben wie *Schadsoftware-Untersuchung* und *Update der Datenbanken und Programm-Module* ausführen.

Eine Liste der KESCLI-Befehle erhalten Sie mit dem Befehl `kescli --help` oder mit dem Kurzbefehl `kescli -h`.

Um Kaspersky Endpoint Security über die Befehlszeile zu verwalten, gehen Sie wie folgt vor:

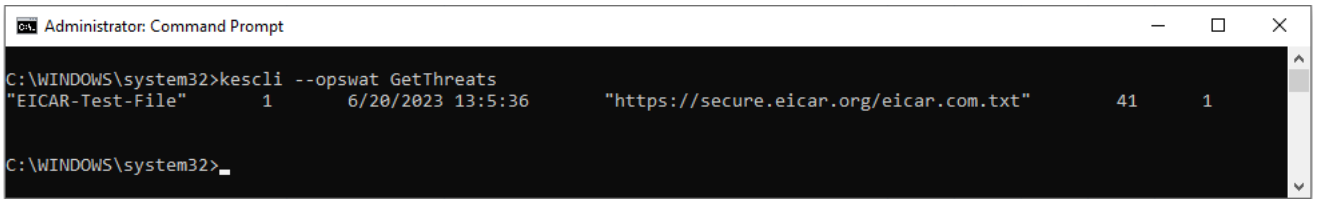
1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

   Den Pfad zur ausführbaren Datei können Sie während der Installation der Anwendung zur Systemvariablen %PATH% hinzufügen.

3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

```
kescli <Befehl> [Parameter]
```

Dann führt Kaspersky Endpoint Security den Befehl aus (siehe Abbildung unten).



Programm über die Befehlszeile verwalten

Scan. Schadsoftware-Untersuchung

Aufgabe *Schadsoftware-Untersuchung* (Vollständige Untersuchung) starten.

Um die Aufgabe auszuführen, muss der Administrator die Verwendung lokaler Aufgaben in der Richtlinie erlauben.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

Sie können den Abschluss-Status der Aufgabe *Schadsoftware-Untersuchung* mithilfe des Befehls `GetScanState` überprüfen. Außerdem können Sie mit dem Befehl `GetLastScanTime` den Zeitpunkt (Datum und Uhrzeit) anzeigen, zu dem die Untersuchung zuletzt abgeschlossen wurde.

Untersuchungsbereich	
`<scan scope>`	`;` Liste mit Dateien und Ordner, durch Leerzeichen getrennt. Beispiel: `"C:\Program Files (x86)\Example Folder"`.

Aktion beim Fund einer Bedrohung	
`0`	**Informieren**. Wenn diese Variante ausgewählt ist, fügt Kaspersky Endpoint Security beim Fund von infizierten Dateien Informationen über diese Dateien zur Liste der aktiven Bedrohungen hinzu.
`1`	**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. Diese Aktion ist standardmäßig ausgewählt.

Beispiel

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. Abschluss-Status der Untersuchung

Abrufen von Informationen über den Abschluss-Status der Aufgabe *Schadsoftware-Untersuchung* (*Vollständige Untersuchung*):

- `1` – die Untersuchung läuft.
- `0` – die Untersuchung läuft nicht.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat GetScanState
```

GetLastScanTime. Abschlusszeit der Untersuchung festlegen

Anzeigen von Informationen über den Zeitpunkt (Datum und Uhrzeit), zu dem die Aufgabe *Schadsoftware-Untersuchung* (*Vollständige Untersuchung*) zuletzt abgeschlossen wurde.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat GetLastScanTime
```

GetThreats. Daten über erkannte Bedrohungen abrufen

Anzeigen einer Liste der erkannten Bedrohungen (*Bericht über Bedrohungen*). Dieser Bericht enthält Informationen über die Bedrohungen und die Virenaktivität während der letzten 30 Tage bevor der Bericht erstellt wurde.

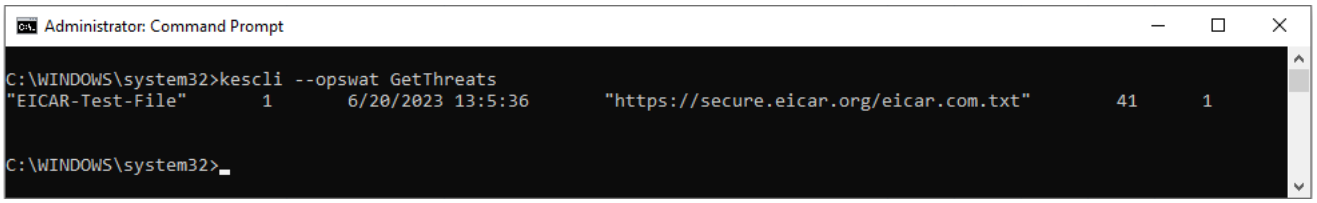
Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat GetThreats
```

Wenn dieser Befehl ausgeführt wird, sendet Kaspersky Endpoint Security eine Antwort mit dem folgenden Format:

<name of detected object> <type of object> <detection date and time> <path to file> <action on threat detection> <threat danger level>



Programm über die Befehlszeile verwalten

Typ des Objekts	
0	Unbekannt (Unknown).
1	Viren (Virware).
2	Trojaner (Trojware).
3	Schadsoftware (Malware).
4	Adware (Adware).
5	Dialer-Programme (Pornware).
6	Anwendungen, mit denen Cyberkriminelle den Computer oder die Benutzerdaten beschädigen können (Riskware).
7	Gepackte Objekte, mit deren Packverfahren bösartiger Code geschützt werden kann (Packed).
20	Unbekannte Objekte (Xfiles).
21	Bekannte Anwendungen (Software).
22	Verdeckte Dateien (Hidden).
23	Anwendungen, die Aufmerksamkeit erfordern (Pupware).
24	Anomales Verhalten (Anomaly).
30	Nicht ermittelt (Undetect).
40	Werbebanner (Banner).
50	Netzwerkangriff (Attack).
51	Registrierungszugriff (Registry).
52	Verdächtige Aktivität (Suspicion).
60	Schwachstellen (Vulnerability).
70	Phishing (Phishing).
80	Unerwünschter E-Mail-Anhang (Attachment).
90	Schadsoftware, die von Kaspersky Security Network erkannt wurde (Urgent).
100	Unbekannter Link (Suspic URL).
110	Andere Schadsoftware (Behavioral).

Aktion beim Fund einer Bedrohung	
0	Unbekannt (unknown).
1	Bedrohung wurde neutralisiert (ok).
2	Objekt war infiziert und wurde nicht desinfiziert (infected).
5	Objekt befindet sich in einem Archiv und wurde nicht desinfiziert (archive).
9	Objekt wurde desinfiziert (disinfected).
10	Objekt wurde nicht desinfiziert (not disinfected).

11	Objekt wurde gelöscht (`deleted`).
13	Eine Backup-Kopie des Objekts wurde erstellt (`backupped`).
15	Objekt wurde ins Backup verschoben (`quarantined`).
23	Objekt wurde beim Neustart des Computers gelöscht (`delete on reboot`).
25	Objekt wurde beim Neustart des Computers desinfiziert (`disinfect on reboot`).
29	Objekt wurde vom Benutzer ins Backup verschoben (`added by user`).
30	Objekt wurde zu den Ausnahmen hinzugefügt (`added to exclude`).
31	Objekt wurde beim Neustart des Computers ins Backup verschoben (`quarantine on reboot`).
36	Fehlalarm (`false alarm`).
38	Prozess wurde beendet (`terminated`).
40	Objekt wurde nicht erkannt (`not found`).
41	Bedrohung kann nicht neutralisiert werden (`untreatable`).
42	Objekt wurde wiederhergestellt (`rolled back`).
43	Objekt wurde aufgrund einer Bedrohungsaktivität erstellt (`produced by threat`).
44	Objekt wurde beim Neustart des Computers wiederhergestellt (`roll back on reboot`).
0xffffffff	Objekt wurde nicht bearbeitet (`discarded`).

Gefahrenstufe der Bedrohung	
`0`	Unbekannt
`1`	Hoch
`2`	Mittlere Untersuchung
`4`	Niedrig
`8`	Info (niedriger als *Niedrig*)

UpdateDefinitions. Update der Datenbanken und Programm-Module

Aufgabe *Update der Datenbanken und Programm-Module* starten Kaspersky Endpoint Security verwendet die Standardquelle: Kaspersky-Update-Server.

Um die Aufgabe auszuführen, muss der Administrator die Verwendung lokaler Aufgaben in der Richtlinie erlauben.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Dieser Befehl kann nicht ausgeführt werden, wenn das Programm im Light Agent-Modus installiert ist.

Befehlssyntax

```
kescli --opswat UpdateDefinitions
```

Den Zeitpunkt (Datum und Uhrzeit), zu dem die aktuellen Antiviren-Datenbanken erschienen sind, können Sie mit dem Befehl `GetDefinitionsetState` anzeigen.

GetDefinitionState. Zeitpunkt (Datum und Uhrzeit) des letzten Datenbanken-Updates ermitteln

Anzeigen von Informationen über den Zeitpunkt (Datum und Uhrzeit), zu dem die verwendeten Antiviren-Datenbanken zuletzt aktualisiert wurden.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat GetDefinitionState
```

EnableRTP. Schutz aktivieren

Aktivieren der Schutzkomponenten von Kaspersky Endpoint Security auf dem Computer: Schutz vor bedrohlichen Dateien, Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Schutz vor Netzwerkbedrohungen, Programm-Überwachung.

Um Schutzkomponenten zu aktivieren, muss der Administrator sicherstellen, dass die entsprechenden Richtlinieneinstellungen geändert werden können (Attribute sind verfügbar).

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat EnableRTP
```

Dadurch werden Schutzkomponenten auch dann aktiviert, wenn Sie die Änderung von Programmeinstellungen über den Kennwortschutz untersagt haben.

Den Betriebsstatus des „Schutzes vor bedrohlichen Dateien“ können Sie mit dem Befehl `GetRealTimeProtectionState` überprüfen.

GetRealTimeProtectionState. Status des „Schutzes vor bedrohlichen Dateien“

Anzeigen von Informationen über den Betriebsstatus der Komponente Schutz vor bedrohlichen Dateien:

- `1` – die Komponente ist aktiviert.
- `0` – die Komponente ist deaktiviert.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. Status der Festplattenverschlüsselung

Anzeigen von Informationen über den Status der Festplattenverschlüsselung:

- `1` bedeutet, dass der Datenträger durch die Kaspersky- oder BitLocker-Festplattenverschlüsselung geschützt ist.
- `0` bedeutet, dass der Datenträger nicht geschützt ist.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --opswat GetEncryptionState
```

Version. Anwendungsversion ermitteln

Version von Kaspersky Endpoint Security für Windows anzeigen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.

Befehlssyntax

```
kescli --Version
```

Sie können auch den Kurzbefehl `-v` verwenden.

Befehle zur Verwaltung von „Detection and Response“

Über die Befehlszeile können Sie die integrierten Funktionen der „Detection and Response“-Lösungen (z. B. „Kaspersky Sandbox“ oder „Kaspersky Endpoint Detection and Response Optimum“) verwalten. Sie können die „Detection and Response“-Lösungen verwalten, wenn die Verwaltung über die Kaspersky Security Center-Konsole nicht möglich ist. Eine Liste der Befehle für die Programmverwaltung erhalten Sie mithilfe des Befehls `HELP`. Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, geben Sie den Befehl `HELP <Befehl>` ein.

Um integrierte Funktionen der „Detection and Response"-Lösungen über die Befehlszeile zu verwalten:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

```
avp.com <command> [options]
```

Dann führt Kaspersky Endpoint Security den Befehl aus.

SANDBOX. Verwaltung von „Sandbox"

Befehle zur Verwaltung der Komponente „Sandbox":

- Aktivieren oder Deaktivieren der Komponente Sandbox.

  Die Sandbox-Komponente ermöglicht die Interaktion mit der Lösung Kaspersky Sandbox und der Komponente KATA Sandbox, die Teil der Kaspersky Anti Targeted Attack Platform ist.

- Konfigurieren der Komponente Kaspersky Sandbox:

  - Verbinden eines Computers mit den Sandbox-Servern.

    Die Server verwenden bereitgestellte virtuelle Abbilder von Microsoft Windows-Betriebssystemen, um die zu untersuchenden Objekte auszuführen. Sie können eine IP-Adresse (IPv4 oder IPv6) oder einen vollständig qualifizierten Domänennamen angeben. Einzelheiten zur Bereitstellung virtueller Images und zur Konfiguration von Kaspersky Sandbox-Servern finden Sie in der Hilfe zu Kaspersky Sandbox und in der Hilfe zu Kaspersky Anti Targeted Attack Platform.

  - Konfigurieren des Timeouts für die Verbindung mit dem Sandbox-Server.

    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.

  - Konfigurieren einer vertrauenswürdigen Verbindung zwischen dem Computer und den Servern.

    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.

  - Konfigurieren des Integrationsmodus.

Sie müssen eine Lösung, zu der Sandbox gehört, auswählen, d. h. Kaspersky Sandbox oder KATA Sandbox. *Kaspersky Sandbox* ist eine eigenständige Detection and Response-Lösung von Kaspersky. *KATA Sandbox* ist eine Komponente der Lösung Kaspersky Anti Targeted Attack Platform. Wenn die Komponente in KATA Sandbox integriert ist, kann sie in den folgenden Modi arbeiten:

- **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**.

- Anzeigen der aktuellen Einstellungen der Komponente.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

Vorgang	
`stop`	Deaktivieren der Komponente „Sandbox“.
`start`	Aktivieren der Komponente „Sandbox“.

`set`	Konfigurieren der Komponente „Sandbox“. Sie können die folgenden Einstellungen konfigurieren:
	• Sandbox-Server hinzufügen (`--servers`)
	• Ein TLS-Zertifikat hinzufügen (`--pinned-certificate`)
	• Einen Krypto-Container hinzufügen (`--client-certificate`)
	• Ein Kennwort für den Krypto-Container eingeben (`--client-certificate-password`)
	• Timeout für die Verbindung zum Server festlegen (`--timeout`)
	• Einen Integrationsmodus auswählen (`--mode`):
	  • `KSB` – Integration in Kaspersky Sandbox
	  • `KATAManual` – manuelle Integration in KATA Sandbox
	  • `KATAAuto` – automatische Integration in KATA Sandbox
	  • `KATAFull` – kombinierte Integration in KATA Sandbox

`show`	Anzeigen der aktuellen Einstellungen der Komponente. Sie erhalten folgende Antwort:
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. Verwaltung der Ausführungsprävention

Deaktivieren der Komponente Ausführungsprävention oder Anzeigen der aktuellen Einstellungen der Komponente, einschließlich der Liste mit Regeln für die Ausführungsprävention.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com prevention disable
```

```
avp.com prevention /show
```

Nach der Ausführung des Befehls `prevention /show` erhalten sie die folgende Antwort:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

Rückgabewerte des Befehls:

- `-1` bedeutet: Die auf dem Computer installierte Version des Programms unterstützt den Befehl nicht.
- `0` bedeutet: Der Befehl wurde erfolgreich ausgeführt.
- `1` bedeutet: Dem Befehl wurde kein obligatorisches Argument übergeben.
- `2` bedeutet: Ein allgemeiner Fehler ist aufgetreten.

- 4 bedeutet: Ein Syntaxfehler ist aufgetreten.
- 9 – falscher Vorgang (z. B. ein Versuch, die Komponente zu deaktivieren, obwohl sie bereits deaktiviert ist).

ISOLATION. Verwalten der Netzwerkisolation

Deaktivieren der Netzwerkisolation des Computers oder Anzeigen der aktuellen Einstellungen der Komponente. Die Einstellungen der Komponente enthalten auch eine Liste der Netzwerkverbindungen, die den Ausnahmen hinzugefügt wurden.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

Nachdem der Befehl `stat` ausgeführt wurde, erhalten Sie folgende Antwort: `Network isolation on|off`.

RESTORE. Wiederherstellen von Dateien aus der Quarantäne

Wiederherstellen einer Datei aus der Quarantäne am ursprünglichen Speicherort. 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. Unter Quarantäne stehende Dateien werden in verschlüsselter Form gespeichert und gefährden die Sicherheit des Gerätes nicht. Kaspersky Endpoint Security verwendet die Quarantäne nur dann, wenn das Programm in Kaspersky Detection and Response-Lösungen integriert ist. In anderen Fällen legt Kaspersky Endpoint Security die entsprechende Datei im Backup ab. Ausführliche Informationen zur Verwaltung der Quarantäne als Teil dieser Lösungen finden Sie in der Hilfe zu Kaspersky Sandbox, Hilfe zu Kaspersky Endpoint Detection and Response Optimum, Hilfe zu Kaspersky Endpoint Detection and Response Expert, Hilfe zu Kaspersky Anti Targeted Attack Platform, und Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises).

Damit der Befehl ausgeführt werden kann, muss der Kennwortschutz aktiviert sein. Der Benutzer muss die Berechtigung **Aus dem Backup wiederherstellen** besitzen.

Das Objekt wird unter dem Systemkonto (SYSTEM) unter Quarantäne gestellt.

Bei der Wiederherstellung von Dateien aus der Quarantäne sind die folgenden Besonderheiten zu beachten:

- Wenn der Zielordner gelöscht wurde oder der Benutzer keine Zugriffsrechte auf diesen Ordner hat, verschiebt die App diese Datei in den Ordner `%DataRoot%\QB\Restored`. Dann müssen Sie die Datei manuell in den Zielordner verschieben.
- Die App berücksichtigt die Groß-/Kleinschreibung im Namen der wiederherzustellenden Datei. Wenn Sie bei der Eingabe des Dateinamens die Groß-/Kleinschreibung nicht beachten, stellt die App die Datei nicht wieder her.

- Wenn der Zielordner bereits eine Datei mit diesem Namen enthält, bricht die App die Dateiwiederherstellung ab.
- Wenn Sie die Lösung KATA (EDR) verwenden, speichert die App eine Kopie der Datei in der Quarantäne, nachdem die Datei wiederhergestellt wurde. Sie können die Quarantäne manuell leeren. Bei den Lösungen EDR Optimum und EDR Expert wird die Datei nach der Wiederherstellung von der App gelöscht.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

Erweiterte Einstellungen	
`/REPLACE`	Vorhandene Datei überschreiben.
`<file name>`	Name der wiederherzustellenden Datei.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

Rückgabewerte des Befehls:

- `-1` bedeutet: Die auf dem Computer installierte Version des Programms unterstützt den Befehl nicht.
- `0` bedeutet: Der Befehl wurde erfolgreich ausgeführt.
- `1` bedeutet: Dem Befehl wurde kein obligatorisches Argument übergeben.
- `2` bedeutet: Ein allgemeiner Fehler ist aufgetreten.
- `4` bedeutet: Ein Syntaxfehler ist aufgetreten.

IOCSCAN. Untersuchung auf Kompromittierungsindikatoren (IOC)

Aufgabe *IOC-Untersuchung* starten Ein *Kompromittierungsindikator (IOC)* ist ein Datensatz, der sich auf ein Objekt oder eine Aktivität bezieht und der auf unbefugten Zugriff auf den Computer (Kompromittierung von Daten) hinweist. Beispielsweise können viele erfolglose Versuche, sich beim System anzumelden, einen Kompromittierungsindikator darstellen. Mithilfe der Aufgabe *IOC-Untersuchung* können Kompromittierungsindikatoren auf dem Computer gefunden und Maßnahmen zur Reaktion auf Bedrohungen ergreifen werden.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Eine IOC-Untersuchung wird nach 128 Übereinstimmungen mit den in IOC-Regeln beschriebenen Kompromittierungsindikatoren abgebrochen. Dies ist erforderlich, um die Anzahl der Einträge im Bericht der IOC-Untersuchungsaufgabe zu begrenzen. Dadurch wird die Analyse vereinfacht und es wird verhindert, dass der Bericht aufgrund ungenau formulierter Kompromittierungsindikatoren zu groß wird. Solche Kompromittierungsindikatoren könnten zu einer sehr hohen Anzahl von Übereinstimmungen führen.

Befehlssyntax

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off] [/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC-Dateien	
`<full path to the IOC file>`	Vollständiger Pfad der IOC-Datei, die Sie zur Untersuchung verwenden möchten. Sie können mehrere durch Leerzeichen getrennte IOC-Dateien angeben. Der vollständige Pfad der IOC-Datei muss ohne das Argument `/path` angegeben werden. Beispiel: `C:\Users\Admin\Desktop\IOC\file1.ioc`
`/path=<path to the folder with IOC files>`	Pfad des Ordners mit den IOC-Dateien, die Sie zur Untersuchung verwenden möchten. *IOC-Dateien* sind Dateien, die Sätze von Indikatoren enthalten, mit denen die Anwendung nach Übereinstimmungen sucht. IOC-Dateien müssen dem OpenIOC-Standard entsprechen. Beispiel: `C:\Users\Admin\Desktop\IOC`

Datentyp für die IOC-Untersuchung	
`/process=on|off`	Analysieren der Prozessdaten, während die IOC-Untersuchung ausgeführt wird (ProcessItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die auf dem Computer ausgeführten Prozesse während der Untersuchung nicht. Falls die IOC-Datei IOC-Bedingungen des ProcessItem-IOC-Dokuments enthält, werden sie ignoriert (als Nicht-Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Prozessdaten nur dann, wenn das ProcessItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/hint=<full path to the executable file of the process|full path to the file>`	Analyse von Dateidaten, während die IOC-Untersuchung ausgeführt wird (Ausdrücke ProcessItem und FileItem). Für die Auswahl einer Datei bestehen folgenden Möglichkeiten: • `<full path to the executable file of the process>` – Ausdruck ProcessItem • `<full path to the file>` – Ausdruck FileItem
`/registry=on|off`	Analysieren von Windows-Registrierungsdaten, während die IOC-Untersuchung ausgeführt wird (RegistryItem-Ausdruck). Wenn der Wert des Arguments `off` ist, durchsucht Kaspersky Endpoint Security die Windows-Registrierung nicht. Wenn die IOC-Datei Ausdrücke des RegistryItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Windows-Registrierung nur dann, wenn das RegistryItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird. Beim Datentyp „RegistryItem“ untersucht Kaspersky Endpoint Security eine Reihe von Registrierungsschlüsseln.

`/dnsentry=on|off`	Analysieren von Daten über Einträge im lokalen DNS-Cache, während die IOC-Untersuchung ausgeführt wird (DnsEntryItem-Ausdruck). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security den lokalen DNS-Cache nicht. Wenn die IOC-Datei Ausdrücke des DnsEntryItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security den lokalen DNS-Cache nur dann, wenn das DnsEntryItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/arpentry=on|off`	Analysieren von Daten über Einträge in der ARP-Tabelle, während die IOC-Untersuchung ausgeführt wird (ArpEntryItem-Begriff). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security die ARP-Tabelle nicht. Wenn die IOC-Datei Ausdrücke des ArpEntryItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die ARP-Tabelle nur dann, wenn das ArpEntryItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/ports=on|off`	Analysieren von Daten über Ports, die während der IOC-Untersuchung zum Abhören geöffnet sind (PortItem-Ausdruck). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security die Tabelle der auf dem Gerät aktiven Verbindungen nicht. Wenn die IOC-Datei Ausdrücke des PortItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Tabelle der aktiven Verbindungen nur dann, wenn das PortItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/services=on|off`	Analysieren von Daten über auf dem Gerät installierte Dienste, während die IOC-Untersuchung ausgeführt wird (ServiceItem-Ausdruck). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security die Daten über auf dem Gerät installierte Dienste nicht. Wenn die IOC-Datei Ausdrücke des ServiceItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Dienstdaten nur dann, wenn das ServiceItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/system=on|off`	Analysieren von Umgebungsdaten, während die IOC-Untersuchung ausgeführt wird (SystemInfoItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die Umgebungsdaten nicht. Wenn die IOC-Datei Ausdrücke des SystemInfoItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Umgebungsdaten nur dann, wenn das SystemInfoItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/users=on|off`	Analysieren von Daten über Benutzer, während die IOC-Untersuchung ausgeführt wird (UserItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die im System über Benutzer erstellten Daten nicht. Wenn die IOC-Datei Ausdrücke des UserItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die im System über Benutzer erstellten Daten nur dann, wenn das UserItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/volumes=on|off`	Analysieren von Daten über Volumes, während die IOC-Untersuchung ausgeführt wird (VolumeItem-Ausdruck). Wenn der Wert des Arguments `off` ist, untersucht Kaspersky Endpoint Security die Daten über Volumes auf dem Gerät nicht. Wenn die IOC-Datei Ausdrücke des VolumeItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Volume-Daten nur dann, wenn das VolumeItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.

`/eventlog=on|off`	Analysieren von Daten über Datensätze im Windows-Ereignisprotokoll, während die IOC-Untersuchung ausgeführt wird (EventLogItem-Ausdruck). Wenn der Wert des Arguments `off` ist, durchsucht Kaspersky Endpoint Security die Einträge im Windows-Ereignisprotokoll nicht. Wenn die IOC-Datei Ausdrücke des EventLogItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security das Windows-Ereignisprotokoll nur dann, wenn das EventLogItem -IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird. Verwenden Sie für den IOC-Ausdruck EventLogItem\source den Wert **Anbietername** aus dem XML-Schema des Ereignisses.
`/datetime=<event publication date>`	Bei der Bestimmung des IOC-Untersuchungsbereichs für das entsprechende IOC-Dokument wird das Datum berücksichtigt, an dem das Ereignis im Windows-Ereignisprotokoll veröffentlicht wurde. Wenn eine IOC-Untersuchung ausgeführt wird, überprüft Kaspersky Endpoint Security die Einträge des Windows-Ereignisprotokolls, die ab dem angegebenen Zeitpunkt (Uhrzeit und Datum) bis zum Zeitpunkt der Aufgabenausführung veröffentlicht wurden. In Kaspersky Endpoint Security kann das Veröffentlichungsdatum des Ereignisses als Wert des Arguments angegeben werden. Die Untersuchung wird nur für Ereignisse durchgeführt, die nach dem angegebenen Datum und vor der Ausführung der Untersuchung im Windows-Ereignisprotokoll veröffentlicht wurden. Ist das Argument nicht angegeben, so untersucht Kaspersky Endpoint Security Ereignisse mit beliebigem Veröffentlichungsdatum. Die Einstellung `TaskSettings::BaseSettings::EventLogItem::datetime` kann nicht bearbeitet werden. Diese Einstellung wird nur verwendet, wenn das EventLogItem-IOC-Dokument in der für die Untersuchung bereitgestellten IOC-Datei beschrieben ist.
`/channel=<list of channels>`	Liste der Kanal-(Protokoll-)Namen, für die Sie eine IOC-Untersuchung durchführen möchten. Wenn das Argument angegeben ist, untersucht Kaspersky Endpoint Security die in den angegebenen Protokollen veröffentlichten Einträge. Der EventLogItem-Ausdruck muss im IOC-Dokument beschrieben sein. Der Name des Protokolls wird als String angegeben, der dem Namen des Protokolls (Kanals) entspricht, das in den Protokolleigenschaften (Parameter „Full Name“) oder in den Ereigniseigenschaften (Parameter „`<Channel></Channel>`“ im XML-Schema des Ereignisses) angegeben ist. Sie können mehrere durch Leerzeichen getrennte Kanäle angeben. Ist das Argument nicht angegeben, so durchsucht Kaspersky Endpoint Security die Einträge nach den Kanälen `Application`, `System` und `Security`.
`/files=on|off`	Analysieren von Dateidaten, während die IOC-Untersuchung ausgeführt wird (FileItem-Ausdruck). Wenn der Wert des Arguments `off` ist, analysiert Kaspersky Endpoint Security die Dateidaten nicht. Wenn die IOC-Datei Ausdrücke des FileItem-IOC-Dokuments enthält, werden diese ignoriert (nicht als Übereinstimmung erkannt). Ist das Argument nicht angegeben, so analysiert Kaspersky Endpoint Security die Dateidaten nur dann, wenn das FileItem-IOC-Dokument in der IOC-Datei beschrieben ist, die für die Untersuchung bereitgestellt wird.
`/drives=<all|system|critical|custom>`	Festlegen des IOC-Untersuchungsbereichs, wenn Daten für das FileItem-IOC-Dokument analysiert werden. Für den Untersuchungsbereich können Sie die folgenden Werte festlegen: • `<all>` für alle verfügbaren Dateibereiche. • `<system>` für Dateien in Ordnern, in denen das Betriebssystem installiert ist. • `<critical>` für temporäre Dateien in Benutzer- und Systemordnern. • `<custom>` für Dateien in benutzerdefinierten Bereichen (`/scope=<list of folders to scan>`). Ist das Argument nicht angegeben, so wird die Untersuchung für kritische Bereiche durchgeführt.
`/excludes=<list of exclusions>`	Festlegen des IOC-Ausnahmebereichs, wenn Daten für das FileItem-IOC-Dokument analysiert werden. Sie können mehrere durch Leerzeichen getrennte Pfade angeben.
`/scope=<list of folders to scan>`	Benutzerdefinierter IOC-Untersuchungsbereich, wenn Daten für das IOC-Dokument FileItem analysiert werden (`/drives=custom`). Sie können mehrere durch Leerzeichen getrennte Pfade angeben.

`/retro /<number of days>`	Die *retrospektive IOC-Untersuchung* ist ein Modus der Aufgabe *IOC-Untersuchung*. Dabei sucht Kaspersky Endpoint Security innerhalb eines bestimmten Zeitraums nach Kompromittierungsindikatoren. Dieser Modus ist für die Suche nach Kompromittierungsindikatoren anhand der Telemetrie des geschützten Computers vorgesehen (z. B. Netzwerkaktivität, Prozesse, Dateien und andere Telemetriedaten). Sie können einen Zeitraum von 1 bis 14 Tagen festlegen. Standardmäßig sucht das Programm einen Tag lang nach Kompromittierungsindikatoren.
`/network=on|off`	Analyse von Netzwerkdaten (Ausdruck NetworkItem).
`/url=on|off`	Analyse der Daten in Browserprotokollen (Ausdruck UrlHistoryItem). Bei der retrospektiven IOC-Untersuchung werden die Protokolle der folgenden Browser analysiert: Google Chrome, Mozilla Firefox, Microsoft Edge (Version 79 oder höher).
`/email`	Analyse von E-Mail-Objekten (Ausdruck EmailItem).
`/route`	Analyse von Routing- und Weiterleitungstabellen (Ausdruck RouteEntryItem).

Rückgabewerte des Befehls:

- `-1` bedeutet: Die auf dem Computer installierte Version des Programms unterstützt den Befehl nicht.
- `0` bedeutet: Der Befehl wurde erfolgreich ausgeführt.
- `1` bedeutet: Dem Befehl wurde kein obligatorisches Argument übergeben.
- `2` bedeutet: Ein allgemeiner Fehler ist aufgetreten.
- `4` bedeutet: Ein Syntaxfehler ist aufgetreten.

Wenn der Befehl erfolgreich ausgeführt wurde (Rückgabewert `0`) und dabei Kompromittierungsindikatoren erkannt wurden, gibt Kaspersky Endpoint Security die folgenden Informationen zu den Aufgabenergebnissen an die Befehlszeile aus:

`Uuid`	ID der IOC-Datei aus der Kopfzeile der IOC-Dateistruktur (Tag `<ioc id="">`)
`Name`	Beschreibung der IOC-Datei aus der Kopfzeile der IOC-Dateistruktur (Tag `<description></description>`)
`Matched Indicator Items`	Liste der IDs aller übereinstimmenden Indikatoren.
`Matched objects`	Daten für jedes IOC-Dokument, für das es eine Übereinstimmung gab.

MDRLICENSE. MDR-Aktivierung

Hinzufügen der BLOB-Konfigurationsdatei, um Managed Detection and Response zu aktivieren. 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“.

Für die Ausführung von Vorgängen mit einer BLOB-Datei sind Administratorrechte erforderlich. Auch die Einstellungen von „Managed Detection and Response“ in der Richtlinie müssen zur Bearbeitung verfügbar sein ().

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

Vorgang	
`/ADD <file name>`	Wenden Sie die BLOB-Konfigurationsdatei an, um die Integration in Kaspersky Managed Detection and Response zu ermöglichen (Dateiformat p7). Sie können nur eine einzige BLOB-Datei anwenden. Wenn dem Computer bereits eine BLOB-Datei hinzugefügt wurde, wird die Datei ersetzt.
`/DEL`	Löschen Sie die BLOB-Konfigurationsdatei.

Autorisierung	
`/login=<user name> /password=<password>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

Beispiel

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. EDR (KATA)-Integration

Befehle zum Verwalten der Komponente Endpoint Detection and Response (KATA):

- Aktivieren oder Deaktivieren der Komponente EDR (KATA).

  Die Komponente EDR (KATA) bietet Interoperabilität mit der Lösung Kaspersky Anti Targeted Attack Platform.

- Konfigurieren der Verbindung zu den Kaspersky Anti Targeted Attack Platform-Servern.

- Anzeigen der aktuellen Einstellungen der Komponente.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<Serveradresse>:<Port> /server-certificate=<Pfad zum TLS-Zertifikat> [/timeout=
<Verbindungs-Timeout für den Central Node-Server (s)>] [/sync-period=<Synchronisierungszeitraum des Central Node-
Servers (min)>]
```

```
avp.com edrkata /show
```

Vorgang	
`stop`	Die Komponente EDR (KATA) deaktivieren.
`start`	Die Komponente EDR (KATA) aktivieren.
`set`	Die Komponente EDR (KATA) konfigurieren. Sie können die folgenden Einstellungen konfigurieren: • Central Node-Server hinzufügen (`servers=<Serveradresse>:<Port>`) • Ein TLS-Zertifikat hinzufügen (`server-certificate=<Pfad des TLS-Zertifikats>`) • Das Timeout für die Verbindung zum Central Node-Server festlegen (`/timeout=<Timeout für die Verbindung zum Central Node-Server (Sekunden)>`) • Den Zeitraum für die Synchronisierung mit dem Central Node-Server festlegen (`/sync-period=<Zeitraum für die Synchronisierung mit dem Central Node-Server (Minuten)>`)
`show`	Anzeigen der aktuellen Einstellungen der Komponente.

EDRExpertOnPrem. Integration von EDR Expert (on-premises)

Befehle zur Verwaltung des integrierten Agenten für die Konfiguration der Integration von Kaspersky Endpoint Detection and Response Expert (on-premises):

- Aktivieren oder Deaktivieren des integrierten Agenten für EDR Expert (on-premises).
- Konfigurieren der Verbindungseinstellungen für die Server von EDR Expert (on-premises).
- Anzeigen der aktuellen Einstellungen des integrierten Agenten.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
[/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
[/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
/telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
[/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
[/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
<0|1>] login=<user name> password=<password>
```

```
avp.com EDRExpertOnPrem /show
```

Vorgang	Beschreibung
`stop`	Den integrierten Agenten für EDR Expert (on-premises) deaktivieren.
`start`	Den integrierten Agenten für EDR Expert (on-premises) aktivieren.

`set`	Den integrierten Agenten für EDR Expert (on-premises) konfigurieren.
	Sie können die folgenden Verbindungseinstellungen für die *Response-Server* konfigurieren:
	• `servers=<server address>:<port>`. Adresse des Response-Servers (FQDN, IPv4, IPv6).
	• `server-certificate=<path to the TLS certificate>`. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. Einen Kryptocontainer für die Zwei-Wege-Authentifizierung verwenden. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel im Format PKCS#12. Um eine solche Authentifizierung zu aktivieren, müssen Sie einen Krypto-Container bei einer externen Zertifizierungsstelle erstellen.
	• `timeout=<server connection timeout (s)>`. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden.
	• `sync-period=<server synchronization period (min)>`. Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung empfängt Kaspersky Endpoint Security Aufgaben zur Reaktion auf Bedrohungen und sendet Aufgabenergebnisse.
	Sie können die folgenden Verbindungseinstellungen für die *Server für die Telemetrieerfassung* konfigurieren:
	• `telemetry-servers=<server address:port>`. Adresse des Servers für die Telemetrieerfassung (FQDN, IPv4, IPv6).
	• `telemetry-server-certificate=<path to the TLS certificat>`. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)).
	• `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. Einen Kryptocontainer für die Zwei-Wege-Authentifizierung verwenden. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel im Format PKCS#12. Um eine solche Authentifizierung zu aktivieren, müssen Sie einen Krypto-Container bei einer externen Zertifizierungsstelle erstellen.
	• `telemetry-timeout=<server connection timeout (s)>`. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden.
	• `events-send-period=<seconds>`. Maximale Verzögerung beim Senden von Ereignissen. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
	• `events-limit=<0|1>`. Begrenzen Sie die Anzahl der Anfragen. Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen.
	• `events-per-hour=<number of events>`. Maximale Anzahl von Ereignissen pro Stunde. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.
	• `max-packet-length=<number of packets>`. Maximale Paketlänge. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.
	• `telemetry-only-tagged-events=<0|1>`. Senden von Telemetriedaten nur mit IOA. Ein *Angriffsindikator (IOA)* ist eine Regel, die ein verdächtiges Verhalten im System beschreibt. Solches Verhaltens kann auf einen gezielten Angriff hinweisen. Das Programm vergleicht das aktuelle Verhalten im System mit diesen Regeln und protokolliert Ereignisse, die auf einen gezielten Angriff hindeuten. Das Programm verwendet die Technologie *Streaming-Scan*, um solche Ereignisse in Echtzeit zu verfolgen.
	Sie können die folgenden allgemeinen Einstellungen konfigurieren:
	• `mode=EDRKATA | EDRExpertOnPrem`. Wechseln zwischen Lösungen:
	  • `EDRKATA`. Endpoint Detection and Response Expert (Version 7.1 oder älter).
	  • `EDRExpertOnPrem`. Endpoint Detection and Response Expert (ab Version 8.0). Standardwert.
	• `login=<user name> password=<password>`. Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

`show`	Anzeigen der aktuellen Einstellungen der Komponente.

KUMA. KUMA-Integration

Befehle zur Verwaltung des integrierten KUMA-Agenten:

- KUMA-Integration aktivieren oder deaktivieren.

  Der integrierte KUMA-Agent gewährleistet die Interoperabilität mit der Lösung Kaspersky Unified Monitoring and Analysis Platform.

- Konfigurieren Sie die Verbindung mit den Servern der Kaspersky Unified Monitoring and Analysis Platform.
- Anzeigen der aktuellen Einstellungen der Komponente.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<Benutzername> /password=<Kennwort>]
```

```
avp.com KUMA /SET /servers=<Serveradresse>:<Port> /server-certificate=<Pfad zum TLS-Zertifikat> [/timeout=<Timeout für die Verbindung zum KUMA-Server (s)>] [/client-certificate=<Pfad zum Krypto-Container>] [ /client-certificate-password=<Kennwort>] [/maximum-data-transfer-time=<maximale Verzögerung bei der Übertragung von Ereignissen (Sek.)>]
```

```
avp.com KUMA /SHOW
```

Vorgang	
`stop`	KUMA-Integration deaktivieren.
`start`	KUMA-Integration aktivieren.
`set`	Den integrierten KUMA-Agenten konfigurieren. Sie können die folgenden Einstellungen konfigurieren: • KUMA-Server hinzufügen (`/servers=<Protokoll>://<Serveradresse>:<Port>`) Das Programm unterstützt die folgenden Serververbindungsprotokolle: `tcp`, `udp`, `http`, `https`. • TLS-Zertifikat hinzufügen (`/server-certificate=<Pfad zum TLS-Zertifikat>`) • Timeout für die Serververbindung festlegen (`/timeout=<Timeout für die Verbindung zum KUMA-Server (s)>`) • Krypto-Container hinzufügen (`/client-certificate=<Pfad zum Krypto-Container> /client-certificate-password=<Kennwort>`) • Verzögerung bei der Übertragung von Ereignissen konfigurieren (`/maximum-data-transfer-time=<maximale Verzögerung bei der Übertragung von Ereignissen (Sek.)`)
`show`	Anzeigen der aktuellen Einstellungen der Komponente.

Autorisierung	
`/login=<Benutzername> /password=<Kennwort>`	Benutzerkonto-Anmeldedaten mit den erforderlichen Kennwortschutz-Berechtigungen.

Beispiel

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15 /login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer /login=login /password=password
```

YARA. YARA-Untersuchung ausführen

Start der Aufgabe *YARA-Untersuchung ausführen*. Das Programm untersucht Dateien und Objekte auf Indikatoren für gezielte Angriffe gegen die IT-Infrastruktur des Unternehmens. Die Untersuchung erfolgt anhand von Datenbanken mit YARA-Regeln. *YARA-Regeln* sind Beschreibungen von Signaturen gezielter Angriffe und Eingriffe in die IT-Infrastruktur des Unternehmens. Diese Signaturen werden von Kaspersky Endpoint Security zur Untersuchung von Objekten verwendet.

Um eine YARA-Untersuchung auszuführen, müssen Sie YARA-Dateien mit Regelbeschreibungen vorbereiten. Beim Erstellen von YARA-Dateien sind die folgenden Anforderungen zu beachten:

- Kaspersky Endpoint Security unterstützt YARA-Dateien mit den Erweiterungen .yara oder .yar, die dem offenen Standard YARA 4.2.3 zur Beschreibung von Kompromittierungsindikatoren entsprechen.
- Für die Aufgabe können nur Dateien mit YARA-Regeln angegeben werden. Die Aufgabe *YARA-Untersuchung ausführen* unterstützt keine anderen Regeltypen.
- Wenn Sie YARA-Dateien hinzugefügt haben, die von Kaspersky Endpoint Security nicht unterstützt werden, oder wenn die Syntax der Regeln fehlerhaft ist, wird die Aufgabe mit einer Fehlermeldung abgebrochen.
- Die Identifikatoren aller YARA-Dateien, die in einer einzelnen Aufgabe verwendet werden, müssen eindeutig sein. Das Vorhandensein von YARA-Dateien mit dem gleichen Identifikator kann sich auf die Ergebnisse der Aufgabenausführung auswirken.
- Eine YARA-Untersuchung wird nach 128 Übereinstimmungen mit den in YARA-Regeln beschriebenen Indikatoren abgebrochen. Dies ist erforderlich, um die Anzahl der Einträge im Bericht der YARA-Untersuchungsaufgabe zu begrenzen. Dadurch wird die Analyse vereinfacht und es wird verhindert, dass der Bericht aufgrund ungenau formulierter YARA-Regeln zu groß wird. Solche Regeln könnten zu einer sehr hohen Anzahl von Übereinstimmungen führen.

Kaspersky empfiehlt, jeweils eine Regel pro YARA-Datei zu erstellen. Dies verbessert die Lesbarkeit der Untersuchungsergebnisse.

Eine YARA-Untersuchung kann relativ zeitaufwendig sein. Je nach Laufwerksgröße, Aufgabeneinstellungen und Anzahl der Objekte auf dem Datenträger kann eine YARA-Untersuchung mehrere Minuten oder sogar Stunden dauern. Das Programm zeigt den Fortschritt der Untersuchung nicht an. Eine YARA-Untersuchung kann nicht beendet oder abgebrochen werden. Es wird empfohlen, abzuwarten, bis die Ergebnisse einer YARA-Untersuchung verfügbar sind.

Befehlssyntax

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA-Dateien	
`<full path to the YARA file>`	Vollständiger Pfad der YARA-Datei, die Sie zur Untersuchung verwenden möchten. Sie können mehrere durch Leerzeichen getrennte Pfade für YARA-Dateien angeben. Erforderliches Argument, wenn der Wert `/path=<path to the folder with YARA files>` nicht angegeben ist. Beispiel: `C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar`

`/path=<path to the folder with YARA files>`	Vollständiger Pfad eines Ordners mit YARA-Dateien, die Sie zur Untersuchung verwenden möchten. Erforderliches Argument, wenn der Wert `<full path to the YARA file>` nicht angegeben ist. Beispiel: `/path=C:\Users\Admin\Desktop\YARA`

Erweiterte Einstellungen	
`/fastScan=<on|off>`	Schnelle YARA-Untersuchung. Das Programm protokolliert das Vorkommen eines gefundenen Indikators für jedes Objekt nur einmal. Außerdem blendet das Programm Duplikate von gefundenen Indikatoren im Protokoll aus. Mit der schnellen YARA-Untersuchung können große Dateien schneller untersucht werden. Wenn diese Einstellung nicht angegeben ist, führt das Programm eine standardmäßige YARA-Untersuchung durch. In diesem Modus protokolliert das Programm Duplikate der gefundenen Indikatoren.
`/maxRules=<maximum number of scan rules>`	Maximale Anzahl von eindeutigen, ausgelösten Erkennungsregeln. Bei Überschreitung dieses Werts wird die YARA-Untersuchung beendet. Wenn der Wert dieser Einstellung nicht angegeben ist oder wenn `0` angegeben ist, führt das Programm die YARA-Untersuchung ohne Einschränkungen durch.
`/timeOut=<stop scan after the specified time in seconds>`	Zulässige Dauer einer YARA-Untersuchung (in Sekunden). Nach Ablauf dieses Zeitraums beendet das Programm die YARA-Untersuchung. Wenn der Wert dieser Einstellung nicht angegeben ist oder wenn `0` angegeben ist, führt das Programm die YARA-Untersuchung ohne Einschränkungen durch.
`/recursive=<on|off>`	Dieses Argument startet eine rekursive Untersuchung von Unterordnern innerhalb von `/scanFolders` (benutzerdefinierte Untersuchung).
`/scanFolders=<list of folders to be scanned>`	Dieses Argument startet eine YARA-Untersuchung der Dateien aus der angegebenen Ordnerliste. Sie können mehrere durch Leerzeichen getrennte Werte angeben. Kaspersky Endpoint Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Ordnerpfad-Maske. Wenn diese Einstellung nicht angegeben ist, führt das Programm eine YARA-Untersuchung aller lokalen Laufwerke durch, unter Ausnahme von Netzwerkfreigaben, Cloud-Laufwerken und Wechseldatenträgern.
`/scanMemory=<on|off>`	Den Speicher aller laufenden Prozesse untersuchen.
`/scanProcess=<process name>`	Arbeitsspeicher nur für die angegebenen Prozessen untersuchen. Geben Sie durch Leerzeichen getrennte vollständige Pfade der ausführbaren Prozessdateien an. Sie können auch die Zeichen `*` und `?` verwenden, um eine Maske einzugeben.
`/maxSize=<file size in bytes>`	Dateigröße für die YARA-Untersuchung begrenzen. Größere Dateien werden vom Programm übersprungen.
`/includes=<list of objects to be scanned>>`	Untersuchungsbereich bearbeiten. Sie können mehrere durch Leerzeichen getrennte Werte angeben. Die folgenden Werte sind verfügbar: • Dateiname • Dateierweiterung Der Untersuchungsbereich muss mit dem Parameter `/scanFolders` angegeben werden. Beispiel: `/scanFolders C:\*.* /includes=*.exe *.dll` – Das Programm untersucht alle Dateien mit den Erweiterungen .EXE und .DLL auf dem Datenträger C.
`/excludes=<list of objects to be scanned>`	Dateien von der YARA-Untersuchung ausschließen. Sie können mehrere durch Leerzeichen getrennte Werte angeben. Die folgenden Werte sind verfügbar: • Dateipfad • Maske des Dateipfads Ausnahmen müssen mit dem Parameter `/scanFolders` angegeben werden. Beispiel: `/scanFolders C:\*.* /excludes readme.txt C:\trusted\*.* *.xml` – Das Programm überspringt die Datei readme.txt file, alle Dateien aus dem Ordner C:\trusted und alle Dateien mit der Erweiterung .xml im Stammordner von Datenträger C.
`/scanAutoruns=<on|off>`	YARA-Untersuchung von Autostart-Punktobjekten.
`/excludeAutoruns=<list of autorun point areas to skip>`	Ausschließen von Autostart-Punkt-Objekten aus dem Untersuchungsbereich. Geben Sie durch Leerzeichen getrennte vollständige Pfade der ausführbaren Prozessdateien an. Sie können auch die Zeichen `*` und `?` verwenden, um eine Maske einzugeben.

`/logFolder=<path to the folder for saving the scan results in a TXT file>`	Wenn Sie einen Pfad zu einem Ordner angeben, speichert das Programm die Untersuchungsergebnisse unter dem angegebenen Pfad in der Datei yara_<Name des Computers>_<Endzeitpunkt der Untersuchung>.txt. Wenn Sie einen Pfad zu einer bestimmten txt-Datei angeben, speichert das Programm die Untersuchungsergebnisse in dieser Datei. Beispielsweise: `/logFolder=C:\test` oder `/logFolder=C:\test\abc.txt`. Die Untersuchungsergebnisse werden in der Befehlszeile ausgegeben, unabhängig davon, ob die Option `/logFolder` angegeben ist.

Rückgabewerte des Befehls:

- `-1` bedeutet: Die auf dem Computer installierte Version des Programms unterstützt den Befehl nicht.
- `0` bedeutet: Der Befehl wurde erfolgreich ausgeführt.
- `1` bedeutet: Dem Befehl wurde kein obligatorisches Argument übergeben.
- `2` bedeutet: Ein allgemeiner Fehler ist aufgetreten.
- `4` bedeutet: Ein Syntaxfehler ist aufgetreten.
- `5` bedeutet: Eine oder mehrere Dateien mit den im Parameter angegebenen YARA-Regeln wurden nicht gefunden.

Wenn der Befehl erfolgreich ausgeführt wurde (Rückgabewert `0`) und dabei Kompromittierungsindikatoren erkannt wurden, gibt Kaspersky Endpoint Security die folgenden Informationen zu den Aufgabenergebnissen an die Befehlszeile aus:

`Started at <time>` `Finished at <time>`	Start- und Endzeitpunkt einer Untersuchung.
`Host name: <computer name>`	Der Name des Computers, auf dem das Objekt gefunden wurde.
`Result: <error>`	Fehlercode für den Fehler, der beim Ausführen der Aufgabe aufgetreten ist. Wenn keine Fehler vorliegen, gibt das Programm `0x00000000` aus.
`Comment: <comment text>`	Fehlerbeschreibung für den Fehler, der beim Ausführen der Aufgabe aufgetreten ist. Beispiel: `Operation timeout`.
`Object Name:` oder `Process:` (bei der Untersuchung eines Prozess-Speichers)	Der Name des Objekts oder Prozesses, für den die YARA-Regel ausgelöst wurde.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	Hashs des Objekts, für das die YARA-Regel ausgelöst wurde.
`Rule Name`	Der Name der ausgelösten YARA-Regel.

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	Metadaten, die in der YARA-Regel angegeben sind.

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	Innerhalb des Objekts wurden Übereinstimmungen gefunden, die die Bedingungen der YARA-Regel erfüllen:
	• Offset im Prozess-Speicher oder in der Datei, in dem bzw. der eine Übereinstimmung gefunden wurde (`Offset`).
	• Der Name der übereinstimmenden Zeichenfolge in der YARA-Regel (`String name`).
	• Die übereinstimmende Zeichenfolge im Prozess-Speicher oder in der Datei (`String data`).

TELEMETRIE-FILTER. Filterung von Ereignissen, die an KUMA gesendet werden sollen

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*. Um die Leistung zu verbessern und die Datenübertragung an den KUMA-Server zu optimieren, können Sie einzelne Ereignisse manuell zur Telemetrie hinzufügen oder davon ausschließen. Sie können beispielsweise Sysmon-Ereignisse ausschließen.

Sie können die Liste der Ausnahmen über die Befehlszeile in eine json-Datei exportieren.

Wenn der Befehl nur den Namen der Datei enthält, in die Sie die Einstellungen exportieren möchten, legt das Programm die Datei wie folgt ab:

- Wenn der Pfad zu avp.com zu der Systemvariablen %PATH% hinzugefügt wird, legt das Programm die Datei im Ordner `C:\Windows\SysWOW64` ab.

- Wenn Sie den Befehl im Installationsordner des Programms ausführen, schlägt der Export fehl, da der Selbstschutz des Programms das Erstellen einer neuen Datei im Programmordner blockiert. Um die Programmeinstellungen in eine Datei zu exportieren, geben Sie den Dateipfad ein.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

Vorgang	
`export`	Export von Ereignisfiltern, die an KUMA gesendet werden sollen.
`import`	Import von Ereignisfiltern, die an KUMA gesendet werden sollen. Falls auf dem Computer bereits Ereignisfilterungsregeln vorhanden sind, ersetzt Kaspersky Endpoint Security während des Importvorgangs.

Datei, die exportiert oder importiert werden soll	
`<file name>`	Name der Datei mit Ereignisfiltern, die an KUMA gesendet werden soll. Außerdem können Sie den Dateipfad auch eingeben. Sie können Filter, die an KUMA gesendet werden sollen, in eine json-Datei exportieren.

Befehle zur Verwaltung von Light Agent

Sie können das Programm in Light Agent-Modus verwalten, um virtuelle Umgebungen über die Befehlszeile zu schützen. Sie können das Programm im Light Agent-Modus verwalten, wenn die Verwaltung über die Kaspersky Security Center-Konsole nicht möglich ist. Eine Liste der Befehle für die Programmverwaltung erhalten Sie mithilfe des Befehls `HELP`. Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, geben Sie den Befehl `HELP <command>` ein.

So verwalten Sie das Programm im Light Agent-Modus über die Befehlszeile:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet.
3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

   ```
   avp.com <command> [options]
   ```

   Dann führt Kaspersky Endpoint Security den Befehl aus.

Das im Light Agent-Modus installierte Programm unterstützt fast alle AVP-Befehle des im Standard-Modus installierten Programms. Im Light Agent-Modus sind die Aufgaben Update der Antiviren-Datenbanken und die Aufgaben zur Verwaltung von Lizenzschlüsseln beschränkt.

KSVLAINFO. Light Agent-Modus bestimmen

Den Light Agent-Modus bestimmen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com KSVLAINFO
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Light Agent-Modus zum Schutz virtueller Umgebungen: aktiviert oder deaktiviert.

  Wenn der Light Agent-Modus aktiviert ist, wird das Programm als Teil der Lösung Kaspersky Security for Virtualization Light Agent verwendet.

- Modus zum Schutz der VDI-Infrastruktur: aktiviert oder deaktiviert.

  Der Modus zum Schutz der VDI-Infrastruktur optimiert die Leistung von Kaspersky Endpoint Security auf nicht-persistenten virtuellen Maschinen. Wenn der Modus zum Schutz der VDI-Infrastruktur aktiviert ist, werden Updates, die einen Neustart der geschützten virtuellen Maschine erfordern, auf nicht-persistenten virtuellen Maschinen nicht installiert. Wenn ein auf einer nicht-persistenten virtuellen Maschine installierter Light Agent Updates erhält, die einen Neustart erfordern, sendet er an Kaspersky Security Center eine Nachricht über die Notwendigkeit, die Vorlage für geschützte virtuelle Maschinen zu aktualisieren.

- Typ der geschützten virtuellen Maschine: persistent oder nicht-persistent.

- Rolle der geschützten virtuellen Maschine in der virtuellen Infrastruktur: Server oder Workstation.

- Bezeichner: UUID.

VIISINFO. Status der Verbindung des Light Agent zum Integrationsserver

Informationen über die Verbindung von Light Agent zum Schutzserver anzeigen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com VIISINFO
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- Adresse und Port des Integrationsservers, mit dem der Light Agent verbunden ist.

- Staus der Verbindung zum Integrationsserver.

- Datum und Uhrzeit der letzten Verbindung zwischen Light Agent und dem Integrationsserver.

SVMINFO. Status der Verbindung von Light Agent zum Schutzserver

Informationen über die Verbindung von Light Agent zum Integrationsserver anzeigen.

Um den Befehl auszuführen, wechseln Sie zu dem Ordner, in dem sich die ausführbare Datei von Kaspersky Endpoint Security befindet. Sie können den Pfad der ausführbaren Datei auch zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne in den Programmordner zu wechseln.

Befehlssyntax

```
avp.com SVMINFO
```

Als Ergebnis der Ausführung des Befehls werden folgende Informationen in die Konsole ausgegeben:

- 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 mit SVM-Adressen, wenn die SVM-Adressliste als Methode der SVM-Ermittlung ausgewählt ist.
- Tag der Verbindung von Light Agent zur SVM.
- Algorithmus zur SVM-Auswahl: standardmäßig oder erweitert. Bei Verwendung des erweiterten Algorithmus zur SVM-Auswahl wird auch der Typ des SVM-Standorts in der virtuellen Infrastruktur angezeigt.
- Schutzstatus für die Verbindung zwischen dem Light Agent und dem Schutzserver.

Fehlercodes

Wenn das Programm über die Befehlszeile verwaltet wird, können Fehler auftreten. Wenn ein Fehler auftritt, zeigt Kaspersky Endpoint Security eine Fehlermeldung an, z. B. `Error: Cannot start task 'EntAppControl'`. Außerdem kann Kaspersky Endpoint Security zusätzliche Angaben in Form eines Codes anzeigen, z. B. `error=8947906D` (s. folgende Tabelle).

Fehlercodes

Fehlercode	Beschreibung
`09479001`	Dieser Schlüssel wird bereits verwendet
`0947901D`	Die Lizenz ist abgelaufen. Datenbank-Updates sind nicht verfügbar
`89479002`	Schlüssel nicht gefunden
`89479003`	Die digitale Signatur ist beschädigt oder wurde nicht gefunden
`89479004`	Die Daten sind beschädigt
`89479005`	Die Schlüsseldatei ist beschädigt
`89479006`	Die Lizenz ist abgelaufen
`89479007`	Es wurde keine Schlüsseldatei angegeben
`89479008`	Ungültige Schlüsseldatei
`89479009`	Die Daten konnten nicht gespeichert werden
`8947900A`	Das Lesen von Daten ist fehlgeschlagen
`8947900B`	Eingabe-/Ausgabefehler
`8947900C`	Die Datenbanken wurden nicht gefunden
`8947900E`	Die Lizenzierungsbibliothek wurde nicht geladen
`8947900F`	Die Datenbanken sind beschädigt oder wurden manuell aktualisiert
`89479010`	Die Datenbanken sind beschädigt
`89479011`	Ein Reserveschlüssel kann nicht mithilfe einer ungültigen Schlüsseldatei hinzugefügt werden
`89479012`	Systemfehler
`89479013`	Die Deny-Liste für Schlüssel ist beschädigt
`89479014`	Die Dateisignatur stimmt nicht mit der digitalen Kaspersky-Signatur überein

Fehlercode	Beschreibung
89479015	Ein Schlüssel für eine Testlizenz kann nicht als Schlüssel für eine kommerzielle Lizenz verwendet werden
89479016	Um die Beta-Version des Programms zu verwenden, ist eine Lizenz für Beta-Tests erforderlich
89479017	Die Schlüsseldatei passt nicht zu diesem Programm. Kaspersky Endpoint Security für Windows kann nicht mit einer Schlüsseldatei für ein anderes Programm aktiviert werden. Bitte überprüfen Sie, ob das richtige Programm installiert ist
89479018	Der Lizenzschlüssel wurde von Kaspersky blockiert
89479019	Das Programm wurde bereits mit einer Testlizenz verwendet. Es ist nicht möglich, erneut einen Schlüssel für eine Testlizenz hinzuzufügen
8947901A	Die Schlüsseldatei ist beschädigt
8947901B	Die digitale Signatur wurde nicht gefunden, ist beschädigt oder weicht von der Kaspersky-Signatur ab
8947901C	Ein Schlüssel kann nicht hinzugefügt werden, wenn die entsprechende nicht-kommerzielle Lizenz abgelaufen ist
8947901E	Das Erstellungs- oder Installationsdatum der Schlüsseldatei ist fehlerhaft. Prüfen Sie das Systemdatum
8947901F	Die Schlüsseldatei für eine Testlizenz kann nicht hinzugefügt werden, wenn bereits eine Testlizenz verwendet wird
89479020	Die Deny-Liste für Schlüssel ist beschädigt oder fehlt
89479021	Die Update-Beschreibung ist beschädigt oder fehlt
89479022	Der Schlüssel passt nicht zu diesem Programm
89479023	Ein Reserveschlüssel kann nicht mithilfe einer ungültigen Schlüsseldatei hinzugefügt werden
89479025	Fehler beim Senden der Anfrage an den Aktivierungsserver. Mögliche Gründe: Fehler bei der Internetverbindung oder vorübergehende Probleme auf dem Aktivierungsserver. Versuchen Sie, das Programm später (in 1-2 Stunden) mithilfe des Aktivierungscodes zu aktivieren. Sollte sich der Fehler wiederholen, kontaktieren Sie Ihren Internetprovider
89479026	Die Anfrage enthält einen ungültigen Aktivierungscode
89479027	Der Status der Antwort kann nicht abgerufen werden
89479028	Fehler beim Speichern einer temporären Datei
89479029	Es wurde ein ungültiger Aktivierungscode angegeben oder das Systemdatum des Computers ist falsch eingestellt. Prüfen Sie das Systemdatum des Computers
8947902A	Der Schlüssel passt nicht zu diesem Programm oder die Lizenz ist abgelaufen
8947902B	Der Download der Schlüsseldatei ist fehlgeschlagen. Es wurde ein ungültiger Aktivierungscode angegeben
8947902C	Der Aktivierungsserver hat den Fehler 400 zurückgegeben
8947902D	Der Aktivierungsserver hat den Fehler 401 zurückgegeben
8947902E	Der Aktivierungsserver hat den Fehler 403 zurückgegeben
8947902F	Eine erforderliche Ressource ist auf dem Aktivierungsserver nicht verfügbar. Der Aktivierungsserver hat den Fehler 404 zurückgegeben. Bitte überprüfen Sie die Einstellungen der Internetverbindung
89479030	Der Aktivierungsserver hat den Fehler 405 zurückgegeben
89479031	Der Aktivierungsserver hat den Fehler 406 zurückgegeben
89479032	Auf dem Proxyserver ist eine Authentifizierung erforderlich. Bitte überprüfen Sie die Netzwerkeinstellungen
89479033	Zeitüberschreitung der Anfrage
89479034	Der Aktivierungsserver hat den Fehler 409 zurückgegeben
89479035	Eine erforderliche Ressource ist auf dem Aktivierungsserver nicht verfügbar. Der Aktivierungsserver hat den Fehler 410 zurückgegeben. Bitte überprüfen Sie die Einstellungen der Internetverbindung
89479036	Der Aktivierungsserver hat den Fehler 411 zurückgegeben
89479037	Der Aktivierungsserver hat den Fehler 412 zurückgegeben
89479038	Der Aktivierungsserver hat den Fehler 413 zurückgegeben
89479039	Der Aktivierungsserver hat den Fehler 414 zurückgegeben
8947903A	Der Aktivierungsserver hat den Fehler 415 zurückgegeben

Fehlercode	Beschreibung
8947903C	Interner Serverfehler
8947903D	Diese Funktion wird nicht unterstützt
8947903E	Ungültige Antwort vom Gateway. Prüfen Sie die Netzwerkeinstellungen
8947903F	Die Ressource ist vorübergehend nicht verfügbar
89479040	Zeitüberschreitung der Antwort vom Gateway. Bitte prüfen Sie die Netzwerkeinstellungen
89479041	Der Server unterstützt dieses Protokoll nicht
89479043	Unbekannter HTTP-Fehler
89479044	Ungültige ID der Ressource
89479046	Ungültige Adresse (URL)
89479047	Ungültiger Zielordner
89479048	Fehler beim Zuteilen von Arbeitsspeicher
89479049	Fehler beim Konvertieren von Einstellungen in ANSI-Zeile (url, folder, agent)
8947904A	Fehler beim Erstellen eines Arbeitsthreads
8947904B	Der Arbeitsthread wurde bereits gestartet
8947904C	Der Arbeitsthread wurde nicht gestartet
8947904D	Die Schlüsseldatei wurde nicht auf dem Aktivierungsserver gefunden
8947904E	Der Schlüssel ist gesperrt
8947904F	Interner Fehler des Aktivierungsservers
89479050	Unzureichende Daten in der Aktivierungsanfrage
89479053	Die Lizenz, die diesem Schlüssel entspricht, ist bereits abgelaufen
89479054	Das Systemdatum des Computers ist falsch eingestellt. Prüfen Sie bitte das Systemdatum des Computers
89479055	Die Testlizenz ist abgelaufen
89479056	Der Aktivierungszeitraum für das Programm ist abgelaufen
89479057	Die mit diesem Code zulässige Anzahl der Programmaktivierungen wurde überschritten
89479058	Beim Aktivierungsvorgang ist ein Systemfehler aufgetreten
89479059	Ein Schlüssel für eine Testlizenz kann nicht als Schlüssel für eine kommerzielle Lizenz verwendet werden
8947905C	Ein Aktivierungscode ist erforderlich
89479062	Die Verbindung mit dem Aktivierungsserver ist fehlgeschlagen
89479064	Der Aktivierungsserver ist nicht verfügbar. Bitte überprüfen Sie die Einstellungen der Internetverbindung und wiederholen Sie den Aktivierungsversuch
89479065	Lizenz abgelaufen
89479066	Ein aktiver Schlüssel kann nicht durch einen abgelaufenen Schlüssel ersetzt werden
89479067	Ein Reserveschlüssel kann nicht hinzugefügt werden, wenn die entsprechende Lizenz vor der aktuellen Lizenz abläuft
89479068	Es ist kein aktueller Abonnementschlüssel vorhanden
8947906A	Ungültiger Aktivierungscode
8947906B	Dieser Schlüssel wird bereits verwendet
8947906C	Der aktive Schlüssel und der Reserveschlüssel haben unterschiedliche Lizenztypen
8947906D	Die Lizenz unterstützt diese Komponente nicht
8947906E	Ein Abonnementschlüssel kann nicht als Reserveschlüssel hinzugefügt werden
89479213	Genereller Fehler auf Transportebene

Fehlercode	Beschreibung
89479214	Es konnte keine Verbindung mit dem Aktivierungsserver hergestellt werden
89479215	Ungültiges Format der Webadresse
89479216	Die Adresse des Proxyservers konnte nicht konvertiert werden
89479217	Die Serveradresse konnte nicht konvertiert werden. Bitte überprüfen Sie die Einstellungen für die Internetverbindung
89479218	Der Verbindungsversuch mit dem Server ist fehlgeschlagen
89479219	Remotezugriff verweigert
8947921A	Time-out des Vorgangs wurde überschritten
8947921B	Fehler beim Senden einer http-Anfrage
8947921C	Fehler bei SSL-Verbindung
8947921D	Der Vorgang wurde wegen eines Rückrufs abgebrochen
8947921E	Zu viele Umleitungen
8947921F	Die Überprüfung des Empfängers ist fehlgeschlagen
89479220	Die Antwort vom Server ist leer
89479221	Fehler beim Senden von Daten
89479222	Fehler beim Datenempfang
89479223	Problem, das mit dem SSL-Zertifikat verbunden ist
89479224	Problem, das mit der SSL-Verschlüsselung verbunden ist
89479225	Problem, das mit der SSL-Zertifizierungsstelle verbunden ist
89479226	Der Inhalt des Netzwerkpakets ist ungültig
89479227	Der Zugriff des Kontos wurde verweigert
89479228	Ungültige Datei des SSL-Zertifikats
89479229	Kann die SSL-Verbindung nicht trennen
8947922A	Erneuter Fehler
8947922B	Die Datei mit den zurückgerufenen Zertifikaten ist ungültig
8947922C	Fehler bei Anfrage des SSL-Zertifikats
89479401	Unbekannter Serverfehler
89479402	Interner Serverfehler
89479403	Für den eingegebenen Aktivierungscode ist kein Schlüssel verfügbar
89479404	Der aktive Schlüssel wurde blockiert
89479405	Es sind keine obligatorischen Einstellungen für die Aktivierungsanfrage vorhanden
89479406	Die Nummer oder das Kennwort des Clients ist ungültig
89479407	Ungültiger Aktivierungscode
89479408	Der Aktivierungscode passt nicht zu diesem Programm. Kaspersky Endpoint Security für Windows kann nicht mit einem Aktivierungscode für ein anderes Programm aktiviert werden. Bitte überprüfen Sie, ob das richtige Programm installiert ist
89479409	Ein Aktivierungscode ist erforderlich
8947940B	Der Aktivierungszeitraum ist abgelaufen
8947940C	Das Programm wurde zu oft mit diesem Code aktiviert
8947940D	Die Anfrage-ID besitzt ein ungültiges Format
8947940E	Der Aktivierungscode wird bereits verwendet
8947940F	Der Aktivierungscode kann nicht aktualisiert werden

Fehlercode	Beschreibung
89479410	Der Aktivierungscode passt nicht zu dieser Region
89479411	Dieser Aktivierungscode ist nicht für die verwendete Sprachversion des Programms vorgesehen
89479412	Der Aktivierungscode ist für eine neue Version dieses Programms vorgesehen. Fordern Sie einen anderen Aktivierungscode an, um die installierte Programmversion zu aktivieren
89479413	Der Aktivierungsserver hat Fehler 643 zurückgegeben
89479414	Der Aktivierungsserver hat Fehler 644 zurückgegeben
89479415	Der Aktivierungsserver hat Fehler 645 zurückgegeben
89479416	Der Aktivierungsserver hat Fehler 646 zurückgegeben
89479417	Ein Aktivierungsserver 1.0 ist erforderlich
89479418	Ungültiges Format des Aktivierungscodes
89479419	Die Computerzeit wurde nicht mit der Uhrzeit des Aktivierungsservers synchronisiert
8947941A	Ungültige Programmversion
8947941B	Das Abonnement ist abgelaufen
8947941C	Die zulässige Anzahl von Aktivierungen wurde überschritten
8947941D	Ungültige Ticket-Signatur
8947941E	Zusätzliche Benutzerdaten sind erforderlich
8947941F	Die Datenüberprüfung ist fehlgeschlagen
89479420	Das Abonnement ist nicht aktiv
89479421	Momentan werden Wartungsarbeiten am Aktivierungsserver durchgeführt
89479501	Unerwarteter Fehler
89479502	Eine ungültige Einstellung wurde übertragen. Beispiel: leere Adressliste für Aktivierungsserver
89479503	Ungültiger Aktivierungscode (falsche Prüfsumme)
89479504	Ungültige Benutzer-ID
89479505	Ungültiges Benutzerkennwort
89479506	Der Aktivierungsserver hat eine falsche Antwort zurückgegeben
89479507	Die Aktivierungsabfrage wurde abgebrochen
89479509	Der Aktivierungsserver hat eine leere Weiterleitungsliste zurückgegeben

Anhang. Programmprofile

Ein *Profil* ist eine Komponente, Aufgabe oder Funktion von Kaspersky Endpoint Security. Profile, die zur Programmverwaltung über die Befehlszeile vorgesehen sind. Sie können Profile für die Ausführung der Befehle `START`, `STOP`, `STATUS`, `STATISTICS` und `EXPORT` verwenden. Mithilfe von Profilen können Sie Programmeinstellungen anpassen (z. B. `STOP DeviceControl`) oder eine Aufgabe starten (z. B. `START Scan_My_Computer`).

Folgende Profile sind verfügbar:

- `AdaptiveAnomaliesControl` – Adaptive Kontrolle von Anomalien
- `AMSI` – AMSI-Schutz.
- `AntiCryptor`

- `BehaviorDetection` – Verhaltensanalyse.
- `DeviceControl` – Gerätekontrolle
- `EntAppControl` – Programmkontrolle
- `File_Monitoring` oder `FM` – Schutz vor bedrohlichen Dateien
- `Firewall` oder `FW` – Firewall
- `HIPS` – Programm-Überwachung.
- `IDS` – Schutz vor Netzwerkbedrohungen
- `IntegrityCheck` – Integritätsprüfung
- `LogInspector` – Protokollanalyse
- `Mail_Monitoring` oder `EM` – Schutz vor E-Mail-Bedrohungen
- `Rollback` – Update-Rollback (das Profil kann nicht angewendet werden, wenn die Anwendung im Light Agent-Modus installiert ist)
- `Scan_ContextScan` – Untersuchung aus dem Kontextmenü
- `Scan_IdleScan` – Untersuchung im Hintergrund
- `Scan_Memory` – Untersuchung des Kernel-Arbeitsspeichers
- `Scan_My_Computer` – Vollständige Untersuchung
- `Scan_Objects` – Benutzerdefinierte Untersuchung
- `Scan_Qscan` – Untersuchung von Objekten, die beim Hochfahren des Betriebssystems geladen werden
- `Scan_Removable_Drive` – Untersuchung von Wechseldatenträgern
- `Scan_Startup` oder `STARTUP` – Untersuchung wichtiger Bereiche
- `Updater` – Update (das Profil kann nicht angewendet werden, wenn die Anwendung im Light Agent-Modus installiert ist)
- `Web_Monitoring` oder `WM` – Schutz vor Web-Bedrohungen
- `WebControl` – Web-Kontrolle

Außerdem unterstützt Kaspersky Endpoint Security auch die Verwendung von Dienstprofilen. Dienstprofile können erforderlich sein, wenn Sie sich an den Technischen Support von Kaspersky wenden.

Programmverwaltung über eine REST API

Kaspersky Endpoint Security bietet die folgenden Möglichkeiten: Programmeinstellungen anpassen, Untersuchung und Update der Antiviren-Datenbanken starten, sowie andere Aufgaben mithilfe von Drittherstеller-Lösungen ausführen. Kaspersky Endpoint Security bietet eine entsprechende API. Die REST API für Kaspersky Endpoint Security verwendet das HTTP-Protokoll und bietet eine Auswahl von „Anfrage/Antwort"-Vorgängen. Das bedeutet, dass Sie Kaspersky Endpoint Security zwar über eine Drittherstеller-Lösung verwalten können, aber nicht über die lokale Programmoberfläche oder über die Verwaltungskonsole von Kaspersky Endpoint Security.

Für die Programmverwaltung über eine REST API muss Kaspersky Endpoint Security mit REST API-Unterstützung installiert werden. Der REST-Client und Kaspersky Endpoint Security müssen auf demselben Computer installiert sein.

So gewährleisten Sie eine sichere Interaktion zwischen Kaspersky Endpoint Security und dem REST-Client:

- Passen Sie den Schutz des REST-Clients vor unbefugtem Zugriff so an, wie es der REST-Client-Entwickler empfiehlt. Passen Sie den Schreibschutz für den REST-Client-Ordner mithilfe von DACL (Discretionary Access Control List) an.
- Um den REST-Client auszuführen, verwenden Sie ein separates Benutzerkonto mit Administratorrechten. Deaktivieren Sie für dieses Benutzerkonto die interaktive Anmeldung im System.

Die Programmverwaltung über eine REST API erfolgt über die Adresse http://127.0.0.1 oder http://localhost. Es ist nicht möglich, Kaspersky Endpoint Security per Fernzugriff über eine REST API zu verwalten.

REST-API-DOKUMENTATION ÖFFNEN

Programminstallation mit einer REST API

Für die Programmverwaltung über eine REST API muss Kaspersky Endpoint Security mit REST API-Unterstützung installiert werden. Wenn Sie Kaspersky Endpoint Security über eine REST API verwalten, kann das Programm nicht mithilfe von Kaspersky Security Center verwaltet werden.

Vorbereitung der Programminstallation mit REST-API-Unterstützung

Für die sichere Interaktion von Kaspersky Endpoint Security mit dem REST-Client muss die Anfrage-Identifikation konfiguriert werden. Dazu müssen Sie ein Zertifikat installieren und anschließend die Nutzdaten jeder Anfrage signieren.

Ein Zertifikat können Sie z. B. mithilfe von OpenSSL erstellen.

Beispiel:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Verwenden Sie den RSA-Verschlüsselungsalgorithmus mit einer Schlüssellänge von 2048 Bit oder mehr.

Dadurch erhalten Sie ein `cert.pem`-Zertifikat und einen privaten `key.pem`-Schlüssel.

Installation des Programms mit REST-API-Unterstützung

Um Kaspersky Endpoint Security mit REST API-Unterstützung zu installieren, gehen Sie wie folgt vor:

1. Starten Sie den Befehlszeileninterpreter cmd als Administrator.
2. Wechseln Sie zu dem Ordner, in dem sich das Programmpaket für Kaspersky Endpoint Security Version 11.2.0 oder höher befindet.
3. Installieren Sie Kaspersky Endpoint Security mit den folgenden Einstellungen:

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     Benutzername für die Programmverwaltung über eine REST API. Geben Sie den Benutzernamen im Format `<DOMAIN>\<UserName>` an (z. B. `RESTAPI_User=COMPANY\Administrator`). Das Programm kann nur unter diesem Benutzerkonto über eine REST API verwaltet werden. Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen.
   - `RESTAPI_Port=<port>`

     Port für die Programmverwaltung über eine REST API. Als Standard wird Port 6782 verwendet. Stellen Sie sicher, dass der Port frei ist. Optionale Einstellung.
   - `RESTAPI_Certificate=<path to certificate>`

     Zertifikat zur Identifizierung von Anfragen (z. B. `RESTAPI_Certificate=C:\cert.pem`).

     Sie können das Zertifikat nach der Programminstallation installieren oder das Zertifikat nach Ablauf des Zertifikats aktualisieren.

     So installieren Sie ein Zertifikat für die Identifizierung von REST-API-Anfragen

     1. Selbstschutz von Kaspersky Endpoint Security deaktivieren

        Der Selbstschutzmechanismus verhindert, dass Programmdateien auf der Festplatte, Prozesse im Arbeitsspeicher und Einträge in der Systemregistrierung verändert oder gelöscht werden.
     2. Wechseln Sie zu dem Registrierungsschlüssel, der die REST-API-Einstellungen enthält: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. Geben Sie den Pfad des Zertifikats ein (z. B. `Certificate = C:\Folder\cert.pem`).
     4. Selbstschutz von Kaspersky Endpoint Security aktivieren
     5. Starten Sie das Programm neu.
   - `AdminKitConnector=1`

     Programmverwaltung mithilfe von Administrationssystemen. Die Verwaltung ist standardmäßig erlaubt.

Sie können die Einstellungen für die Verwendung einer REST API auch mithilfe der Dateien setup.ini angeben.

Beispiel:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
/pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
```

Auf diese Weise können Sie das Programm über eine REST API verwalten. Um die Funktion zu überprüfen, öffnen Sie die Dokumentation für die REST API mithilfe einer GET-Anfrage.

Beispiel:
```
GET http://localhost:6782/kes/v1/api-docs
```

Wenn Sie die Anwendung mit REST-API-Unterstützung installiert haben, erstellt Kaspersky Endpoint Security in den Einstellungen der „Web-Kontrolle“ automatisch eine Erlaubnisregel für den Zugriff auf Webressourcen (*Dienstregel für REST-API*). Diese Regel wird benötigt, damit der REST-Client immer auf Kaspersky Endpoint Security zugreifen kann. Beispiel: Wenn Sie den Benutzerzugriff auf Webressourcen beschränkt haben, hat dies keinen Einfluss auf die Anwendungsverwaltung über die REST-API. Wir raten Ihnen davon ab, die Regel zu löschen oder die Einstellungen der *Dienstregel für REST-API* zu ändern. Falls Sie die Regel gelöscht haben, stellt Kaspersky Endpoint Security sie nach dem Neustart der Anwendung wieder her.

Verwendung einer API

Der Zugriff auf das Programm kann über eine REST API mithilfe des Kennwortschutzes nicht beschränkt werden. Beispielsweise ist es nicht möglich, die Deaktivierung des Schutzes über eine REST API zu verbieten. Sie können den „Kennwortschutz“ über eine REST API anpassen und den Zugriff der Benutzer auf das Programm über die lokale Schnittstelle beschränken.

Um das Programm über eine REST API zu verwalten, muss der REST-Client unter dem Benutzerkonto ausgeführt werden, das Sie bei der Installation des Programms mit REST API-Unterstützung erstellt haben. Für die Arbeit mit einer REST API können Sie nur einen einzigen Benutzer auswählen.



REST-API-DOKUMENTATION ÖFFNEN

Die Programmverwaltung über eine REST API umfasst die folgenden Schritte:

1. Fordern Sie die aktuellen Werte der Programmeinstellungen an. Senden Sie dazu eine GET-Anfrage.

   Beispiel:
   ```
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. Das Programm sendet eine Antwort mit der Struktur und den Werten der Einstellungen. Kaspersky Endpoint Security unterstützt die Formate XML und JSON.

   Beispiel:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. Ändern Sie die Programmeinstellungen. Verwenden Sie die Struktur aus der Antwort auf Ihre GET-Anfrage.

   Beispiel:
   ```
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. Speichern Sie Anwendungseinstellungen (die Nutzdaten) in einem JSON (payload.json).

5. Signieren Sie die JSON im PKCS7-Format.

   Beispiel:
   ```
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out
   signed_payload.pem
   ```

   Dadurch erhalten Sie eine signierte Datei mit den Nutzdaten der Anfrage (`signed_payload.pem`).

6. Ändern Sie die Programmeinstellungen. Senden Sie dazu eine POST-Anfrage und hängen Sie die signierte Datei mit den Anfragenutzdaten an (`signed_payload.pem`).

Die Anwendung wendet die neuen Einstellungen an und sendet eine Antwort mit den Ergebnissen der Anwendungskonfiguration (die Antwort kann leer sein). Sie können mithilfe einer GET-Anfrage überprüfen, ob die Einstellungen aktualisiert wurden.

Informationsquellen zum Programm

Dieser Abschnitt beschreibt die Informationsquellen für die App.

Wählen Sie je nach Wichtigkeit und Dringlichkeit Ihres Problems eine passende Informationsquelle aus.

Seite für Kaspersky Endpoint Security auf der Kaspersky-Website

Auf der Seite für Kaspersky Endpoint Security finden Sie allgemeine Informationen über die App, deren Funktionen und Merkmale.

Die Seite für Kaspersky Endpoint Security enthält einen Link zu unserem Online-Shop. Dort können Sie die App kaufen oder verlängern.

Seite für Kaspersky Endpoint Security in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Bereich der Website des Technischen Supports.

Auf der Seite für Kaspersky Endpoint Security in der Wissensdatenbank finden Sie Artikel mit nützlichen Informationen, Tipps sowie FAQs zum Kauf, zur Installation und zur Nutzung der App.

Die Artikel in der Wissensdatenbank beziehen sich nicht nur auf Kaspersky Endpoint Security, sondern auch auf andere Kaspersky-Apps. 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.

Kontaktaufnahme mit dem Technischen Support

Wenn Sie in der Dokumentation oder in den anderen Informationsquellen zu Kaspersky Endpoint Security keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support. Der Technische Support beantwortet Ihre Fragen zur Installation und Verwendung von Kaspersky Endpoint Security.

Kaspersky unterstützt Kaspersky Endpoint Security während des Lebenszyklus der Programms (siehe Seite zum Produktlebenszyklus). Bitte beachten Sie die Support-Regeln, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Über die Website des Technischen Supports
- mit einer Anfrage an den Technischen Support von Kaspersky aus dem Portal Kaspersky CompanyAccount

Nachdem Sie den Technischen Support von Kaspersky über ein Problem informiert haben, kann es sein, dass die Support-Mitarbeiter Sie auffordern, eine *Protokolldatei* zu erstellen. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Der Technische Support benötigt möglicherweise auch weitere Informationen zum Betriebssystem und den auf dem Computer laufenden Prozessen sowie genaue Verlaufsberichte zur Ausführung von Programmkomponenten.

Es kann sein, dass Sie von den Support-Experten dazu aufgefordert werden, die Programmeinstellungen zu Diagnosezwecken zu ändern.

- Funktionalität zur Ermittlung erweiterter Diagnoseinformationen aktivieren
- Anpassen spezieller Einstellungen für bestimmte Programmkomponenten, die über die standardmäßige Programmoberfläche nicht verfügbar sind.
- Einstellungen für die Speicherung von empfangenen Diagnose-Informationen ändern
- Anpassen von Einstellungen für das Abfangen und für die Speicherung des Netzwerkverkehrs

Alle Informationen, welche für die oben genannten Aktionen erforderlich sind (z. B. Reihenfolge der Schritte, Einstellungsänderungen, Konfigurationsdateien, Skripte, erweiterte Optionen für die Befehlszeile, Debug-Module und spezielle Dienstprogramme) werden Ihnen von den Support-Experten mitgeteilt. Sie erhalten außerdem Informationen über den Umfang der Daten, die im Rahmen der Fehlersuche empfangen werden. Die ermittelten erweiterten Diagnoseinformationen werden auf dem Benutzercomputer gespeichert. Die ermittelten Daten werden nicht automatisch an Kaspersky geschickt.

Die oben genannten Aktionen dürfen nur unter Anleitung der Support-Experten ausgeführt werden. Wenn Sie die Programmeinstellungen auf andere Weise ändern, als in der Online-Hilfe oder in den Anleitungen des Technischen Supports beschrieben ist, kann es sein, dass die Funktion des Betriebssystems verlangsamt oder gestört wird, das Sicherheitsniveau des Computers sinkt, und die Verfügbarkeit und Integrität der verarbeiteten Informationen gestört werden.

Über die Zusammensetzung und Speicherung von Protokolldateien

Bis die erhaltenen Informationen an Kaspersky übertragen werden, sind Sie selbst verantwortlich für die Sicherheit der erhaltenen Informationen und insbesondere für die Kontrolle und Beschränkung des Zugriffs auf die erhaltenen Informationen, die auf dem Computer gespeichert sind.

Protokolldateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden endgültig gelöscht, wenn das Programm entfernt wird.

Protokolldateien werden im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` gespeichert. Eine Ausnahme bilden die Protokolldateien des Authentifizierungsagenten.

Leistungs-Protokolldateien werden nach folgendem Muster benannt:
`KES<14.2_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

Sie können die Daten einsehen, die in Protokolldateien aufgezeichnet wurden.

Alle Protokolldateien enthalten folgende allgemeinen Daten:

- Ereigniszeitpunkt
- Thread-Nummer

  Diese Informationen sind nicht in der Protokolldatei des Authentifizierungsagenten enthalten.

- Programmkomponente, die das Ereignis verursacht hat
- Ereigniskategorie (informativ, Warnung, kritisch, Fehler)
- Ereignisbeschreibung für den Befehl der Programmkomponente und das Ausführungsergebnis für diesen Befehl

Inhalt der Protokolldateien SRV.log, GUI.log und ALL.log

Die Protokolldateien `SRV.log`, `GUI.log` und `ALL.log` können neben allgemeinen Daten auch die folgenden Informationen enthalten:

- Persönliche Daten wie Nachname und Vorname, falls diese Daten Bestandteil eines Dateipfads auf dem lokalen Computer sind.
- Daten über die Hardware, die auf dem Computer installiert ist (z. B. Daten über die BIOS/UEFI-Firmware). Diese Daten werden in einer Ablaufverfolgungsdatei aufgezeichnet, wenn die vollständige Festplattenverschlüsselung mithilfe der Technologie Kaspersky-Festplattenverschlüsselung ausgeführt wird.

- Benutzername und Kennwort, falls diese im Klartext übertragen wurden. Diese Daten können bei der Untersuchung des Internet-Datenverkehrs in den Protokolldateien gespeichert werden.
- Benutzername und Kennwort, falls diese in HTTP-Kopfzeilen enthalten sind.
- Benutzername für die Anmeldung bei Microsoft Windows, falls der Name des Benutzerkontos Bestandteil eines Dateinamens ist.
- Ihre E-Mail-Adresse oder Webadresse mit Benutzername und Kennwort, falls diese im Namen eines gefundenen Objekts enthalten sind.
- Webseiten, die Sie besuchen, sowie Links von diesen Webseiten. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm Webseiten untersucht.
- Adresse des Proxyservers, Computername, Port, IP-Adresse, Benutzername, der bei der Autorisierung auf dem Proxyserver verwendet wird. Diese Daten werden in Protokolldateien aufgezeichnet, wenn das Programm einen Proxyserver verwendet.
- Externe IP-Adressen, mit denen eine Verbindung zu Ihrem Computer aufgebaut wurde
- Nachrichtenbetreff, ID, Name des Absenders und Webadresse des Nachrichtenabsenders in einem sozialen Netzwerk Diese Daten werden in Protokolldateien aufgezeichnet, wenn die Komponente „Web-Kontrolle“ aktiviert ist.
- Daten über den Netzwerkverkehr. Diese Daten werden in einer Ablaufverfolgungsdatei aufgezeichnet, wenn die Komponenten zur Überwachung des Datenverkehrs aktiviert sind (z. B. „Web-Kontrolle“).
- Daten, die von den Kaspersky-Servern stammen (z. B. Version der Antiviren-Datenbanken).
- Status der Komponenten von Kaspersky Endpoint Security und Angaben über die Verwendung dieser Komponenten.
- Daten über die Aktionen, die der Benutzer mit dem Programm ausführt.
- Ereignisse des Betriebssystems.

Inhalt der Ablaufverfolgungsdateien HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Die Protokolldatei `HST.log` enthält neben allgemeinen Daten auch Informationen zur Ausführung der Update-Aufgabe für die Datenbanken und Programm-Module.

Die Protokolldatei `BL.log` enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Programm auftreten, sowie Daten, die im Programm zur Problembehebung benötigt werden. Diese Datei wird erstellt, wenn das Programm mit dem Parameter avp.exe –bl gestartet wird.

Die Protokolldatei `Dumpwriter.log` enthält neben allgemeinen Daten auch Verwaltungsinformationen, die zur Behebung von Problemen benötigt werden, die bei der Protokollierung einer Dump-Datei des Programms auftreten.

Die Protokolldatei `WD.log` enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Dienst avpsus auftreten. Dazu zählen auch Ereignisse über das Update der Programm-Module.

Die Protokolldatei `AVPCon.dll.log` enthält neben allgemeinen Daten auch Informationen über Ereignisse, die im Modul auftreten, das für die Verbindung mit Kaspersky Security Center dient.

Inhalt von Ablaufverfolgungsdateien der Leistung

Ablaufverfolgungsdateien der Leistung werden nach folgendem Muster benannt: `KES<14.2_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`.

Ablaufverfolgungsdateien der Leistung enthalten neben allgemeinen Daten auch Informationen über die Prozessauslastung, über die Bootdauer des Betriebssystems und über aktive Prozesse.

Inhalt der Ablaufverfolgungsdatei der AMSI-Schutzkomponente

Die Ablaufverfolgungsdatei `AMSI.log` enthält neben allgemeinen Daten auch Informationen über die Ergebnisse von Untersuchungen, die von Drittanbieter-Anwendungen angefordert wurden.

Inhalt der Ablaufverfolgungsdatei für die Komponente „Schutz vor E-Mail-Bedrohungen"

Die Ablaufverfolgungsdatei `mcou.OUTLOOK.EXE.log` kann neben allgemeinen Daten auch Bestandteile von E-Mail-Nachrichten enthalten, darunter auch E-Mail-Adressen.

Inhalt der Ablaufverfolgungsdatei für die Komponente „Untersuchung aus dem Kontextmenü"

Die Ablaufverfolgungsdatei `shellex.dll.log` enthält neben allgemeinen Daten auch Informationen über die Ausführung einer Untersuchungsaufgabe und Daten, die zur Behebung von Programmstörungen erforderlich sind.

Inhalt der Ablaufverfolgungsdateien für die Web-Plug-ins des Programms

Ablaufverfolgungsdateien des Programm-Web-Plug-ins werden auf dem Computer gespeichert, auf dem Kaspersky Security Center Web Console bereitgestellt wurde, und zwar im Ordner `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Die Ablaufverfolgungsdateien des Programm-Web-Plug-ins werden nach folgendem Muster benannt: `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`. Web Console startet die Protokollierung nach der Installation und löscht die Ablaufverfolgungsdateien nach der Deinstallation von Web Console.

Die Ablaufverfolgungsdateien für das Web-Plug-in des Programms enthalten neben allgemeinen Daten auch folgende Informationen:

- Kennwort des Benutzers KLAdmin für die Entsperrung der Benutzeroberfläche von Kaspersky Endpoint Security (Kennwortschutz).
- Temporäres Kennwort zur Entsperrung der Benutzeroberfläche von Kaspersky Endpoint Security (Kennwortschutz).

- Benutzername und Kennwort für den SMTP-Mail-Server (E-Mail-Benachrichtigungen).
- Benutzername und Kennwort für den Proxyserver im Internet (Proxyserver).
- Benutzername und Kennwort für die Aufgabe *Auswahl der Programmkomponenten ändern*.
- Anmeldedaten und Pfade, die in den Richtlinieneigenschaften und in den Aufgaben von Kaspersky Endpoint Security angegeben sind.

Inhalt der Protokolldatei des Authentifizierungsagenten

Die Ablaufverfolgungsdatei des Authentifizierungsagenten wird im Ordner System Volume Information gespeichert und nach folgendem Muster benannt: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Die Protokolldatei des Authentifizierungsagenten enthält neben allgemeinen Daten auch Informationen über die Funktion des Authentifizierungsagenten und über Aktionen, die der Benutzer im Authentifizierungsagenten ausführt.

Anwendungsnachverfolgung

Anwendungsnachverfolgung bedeutet die ausführliche Aufzeichnung von Aktionen, die von der App ausgeführt werden, sowie von Mitteilungen über Ereignisse, die bei der Ausführung der App eintreten. Während der Ablaufverfolgung erstellt die App eine Reihe von Dateien mit Daten über den Betrieb verschiedener App-Komponenten (z. B. SRV.log, WD.log und andere).

> Die Anwendungsnachverfolgung sollte nur unter Anleitung des Technischen Supports von Kaspersky ausgeführt werden.

Um eine Ablaufverfolgungsdatei über das Programm zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Klicken Sie im angezeigten Fenster auf **Support-Tools**.
3. Verwenden Sie den Schalter **Programm-Ablaufverfolgung aktivieren**, um die Ablaufverfolgung von Anwendungsvorgängen zu aktivieren oder zu deaktivieren.
4. Wählen Sie in der Dropdown-Liste **Protokollierung** einen Modus für die Anwendungsnachverfolgung aus:
   - **Mit Größenbeschränkung**. Ablaufverfolgungsergebnisse in einer beschränkten Anzahl von Dateisätzen mit beschränkter Größe speichern und alte Dateien überschreiben, wenn die maximale Größe erreicht wird. Wenn dieser Modus ausgewählt ist, können Sie die maximale Anzahl von Dateisätzen für die Rotation und die maximale Größe der einzelnen Dateisätze festlegen.

     Standardmäßig speichert die App fünf Sätze von Ablaufverfolgungsdateien. Die maximale Größe eines einzelnen Dateisatzes beträgt 3.072 MB. Sie benötigen also 15 GB freien Speicherplatz, um die Ablaufverfolgungsdateien zu speichern.
   - **Ohne Beschränkung**. Eine einzige Protokolldatei speichern (ohne Größenbeschränkung).

5. Wählen Sie in der Dropdown-Liste **Stufe** ein Ablaufverfolgungsstufe aus:

   - **Normal**: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie Informationen über den normalen Programmbetrieb gespeichert (Standard).
   - **Detailliert**: In der Ablaufverfolgungsdatei werden alle Informationen über den Programmbetrieb gespeichert.

   Wenn Sie die Einstellungen für die Programm-Ablaufverfolgung über die Befehlszeile verwalten, sind zusätzliche Ablaufverfolgungsstufen verfügbar. Es wird empfohlen, die Support-Experten nach der erforderlichen Protokollierungsstufe zu fragen. Es wird empfohlen, die Stufe **Normal** einzustellen, wenn keine Support-Empfehlungen für die Protokollierungsstufe vorliegen.

   Wenn die Programm-Ablaufverfolgung über die Befehlszeile aktiviert wurde und eine andere Ablaufverfolgungsstufe als **Normal** oder **Detailliert** festgelegt wurde, ist in der Dropdown-Liste **Stufe** der Wert **Normal** ausgewählt.

6. Um die Ablaufverfolgung zu beenden, kehren Sie zum Fenster **Support-Tools** zurück und deaktivieren Sie die Ablaufverfolgung.

Sie können auch Ablaufverfolgungsdateien erstellen, während Sie das Programm aus der Befehlszeile installieren. Dies ist auch mithilfe der Datei setup.ini möglich.

Dadurch werden im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` Ablaufverfolgungsdateien für den App-Betrieb erstellt. Senden Sie die erstellten Ablaufverfolgungsdateien an den Technischen Support von Kaspersky.

Kaspersky Endpoint Security löscht automatisch Protokolldateien, wenn das Programm entfernt wird. Außerdem können Sie eine Dateien auch manuell löschen. Dazu müssen Sie die Protokollierung deaktivieren und die Anwendung stoppen.

Überwachung der Programmleistung

Kaspersky Endpoint Security erlaubt es, Informationen über Probleme zu erhalten, die im Computer bei der Programmverwendung auftreten. Sie können beispielsweise Informationen darüber erhalten, ob sich nach der Programminstallation das Hochfahren des Betriebssystems verzögert. Dazu erstellt Kaspersky Endpoint Security Ablaufverfolgungsdateien der Leistung. Bei der *Leistungsüberwachung* werden vom Programm ausgeführte Aktionen protokolliert, um Leistungsprobleme von Kaspersky Endpoint Security zu erkennen. Um Informationen zu empfangen, verwendet Kaspersky Endpoint Security die Windows-Ereignisverfolgung (ETW – Event Tracing for Windows). Die Funktionsdiagnose für Kaspersky Endpoint Security und die Ermittlung der Problemursachen erfolgt durch den Technischen Support von Kaspersky.

Die Anwendungsnachverfolgung sollte nur unter Anleitung des Technischen Supports von Kaspersky ausgeführt werden.

Um eine Ablaufverfolgungsdatei über die Leistung zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche .
2. Klicken Sie im angezeigten Fenster auf **Support-Tools**.

3. Verwenden Sie den Schalter **Leistungs-Ablaufverfolgung aktivieren**, um die Überwachung der Programmleistung zu aktivieren oder zu deaktivieren.

4. Wählen Sie in der Dropdown-Liste **Protokollierung** einen Modus für die Anwendungsnachverfolgung aus:

   - **Mit Größenbeschränkung**. Protokollierungsergebnisse in einer beschränkten Anzahl von Dateien mit beschränkter Größe speichern und alte Dateien überschreiben, wenn die maximale Größe erreicht wird. Wenn dieser Modus ausgewählt ist, können Sie die maximale Größe für jede Datei festlegen.

   - **Ohne Beschränkung**. Eine einzige Protokolldatei speichern (ohne Größenbeschränkung).

5. Wählen Sie in der Dropdown-Liste **Stufe** ein Ablaufverfolgungsstufe aus:

   - **Oberflächlich**. Kaspersky Endpoint Security analysiert die wichtigsten Betriebssystemprozesse, die mit der Leistung zusammenhängen.

   - **Detailliert**. Kaspersky Endpoint Security analysiert alle Betriebssystemprozesse, die mit der Leistung zusammenhängen.

6. Wählen Sie in der Dropdown-Liste **Protokollierungstyp** einen Ablaufverfolgungstyp aus:

   - **Basisinformationen**. Kaspersky Endpoint Security analysiert Prozesse, während das Betriebssystem ausgeführt wird. Verwenden Sie diesen Ablaufverfolgungstyp, wenn ein Problem nach dem Systemstart reproduziert wird, z. B. ein Problem beim Internetzugriff im Browser.

   - **Beim Neustart**. Kaspersky Endpoint Security analysiert Prozesse nur, während das Betriebssystem geladen wird. Nach dem Systemstart beendet Kaspersky Endpoint Security die Ablaufverfolgung. Verwenden Sie diesen Ablaufverfolgungstyp, wenn das Problem mit einer Verzögerung des Systemstarts zusammenhängt.

7. Starten Sie den Computer neu und reproduzieren Sie das Problem.

8. Um die Ablaufverfolgung zu beenden, kehren Sie ins Fenster „Support-Tools“ zurück und deaktivieren Sie die Ablaufverfolgung.

Dadurch wird im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` eine Leistungs-Protokolldatei erstellt. Senden Sie die erstellte Ablaufverfolgungsdatei an den Technischen Support von Kaspersky.

Aufzeichnung von Dump-Dateien

Eine Dump-Datei enthält alle Informationen über den Arbeitsspeicher der Prozesse von Kaspersky Endpoint Security zum Zeitpunkt, als diese Dump-Datei erstellt wurde.

> Gespeicherte Dump-Dateien können vertrauliche Daten enthalten. Sie müssen selbst für den Schutz der Dump-Dateien sorgen, um die Kontrolle des Zugriffs auf die Daten zu gewährleisten.

Dump-Dateien bleiben während der gesamten Nutzungsdauer des Programms auf Ihrem Computer gespeichert. Sie werden unwiderruflich gelöscht, wenn das Programm entfernt wird. Dump-Dateien werden im Ordner `%ProgramData%\Kaspersky Lab\KES.14.2\Traces` gespeichert.

So aktivieren Sie in der Verwaltungskonsole (MMC) die Aufzeichnung von Dump-Dateien

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
4. Klicken Sie im Block **Debug-Informationen** auf **Einstellungen**.
5. Verwenden Sie im folgenden Fenster das Kontrollkästchen **Dump-Aufzeichnung aktivieren**, um das Schreiben von Programm-Dumps zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie in Web Console und Cloud Console die Aufzeichnung von Dump-Dateien

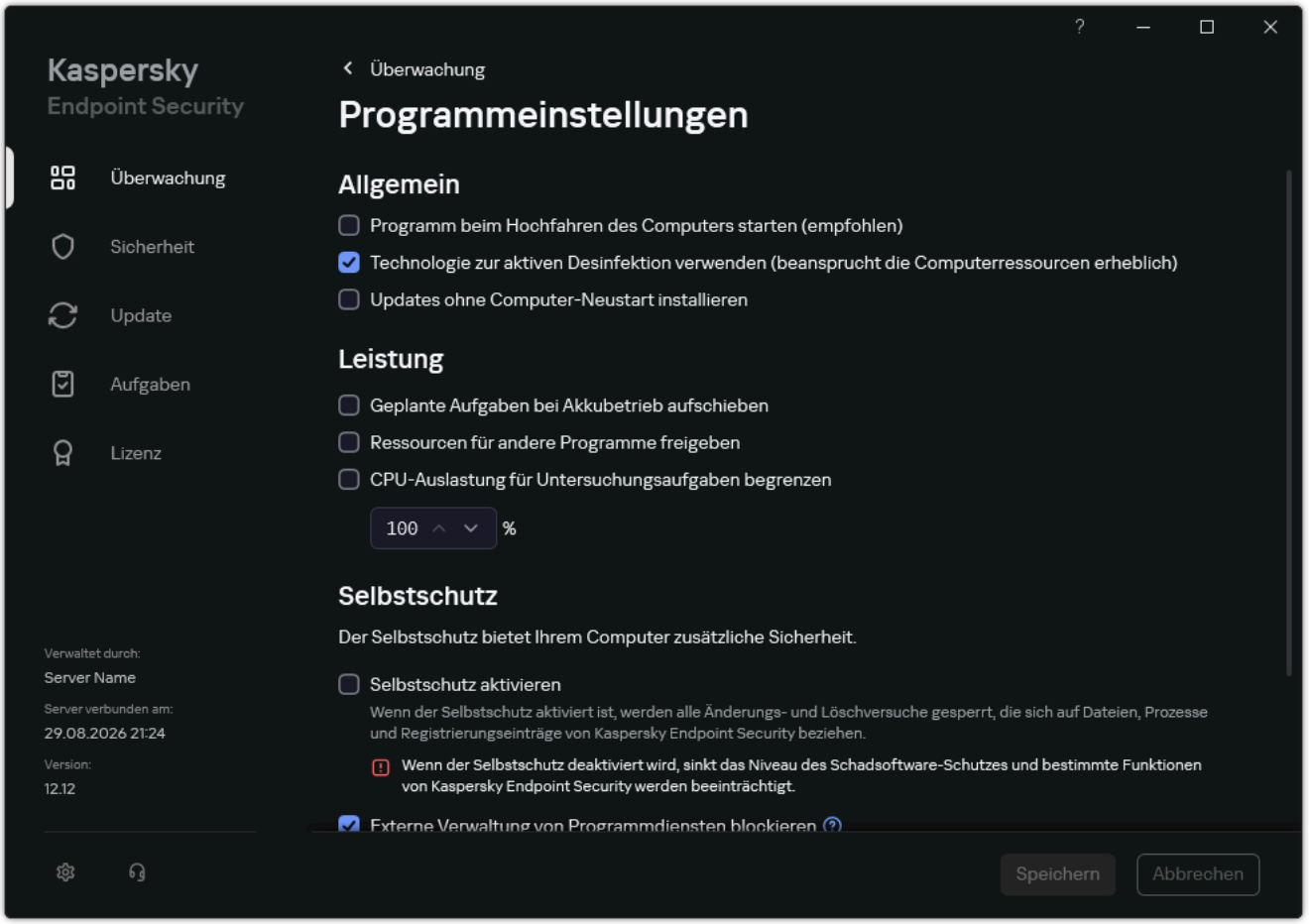
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Technischer Support**.
5. Verwenden Sie im Block **Debug-Informationen** das Kontrollkästchen **Dump-Erstellung AKTIVIERT**, um das Schreiben von Dump-Dateien zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über die App-Benutzeroberfläche die Aufzeichnung von Dump-Dateien

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen** → **Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Verwenden Sie im Block **Debug-Informationen** das Kontrollkästchen **Dump-Aufzeichnung aktivieren**, um das Schreiben von Dump-Dateien zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Schutz von Dump- und Protokolldateien

Dump-Dateien und Protokolldateien enthalten Informationen über das Betriebssystem und können Benutzerdaten enthalten. Um einen unberechtigten Zugriff auf diese Daten zu verhindern, können Sie den Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren.

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.

So aktivieren Sie in der Verwaltungskonsole (MMC) den Schutz für Dump-Dateien und Ablaufverfolgungsdateien

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Wählen Sie im Richtlinienfenster **Allgemeine Einstellungen → Programmeinstellungen** aus.
4. Klicken Sie im Block **Debug-Informationen** auf **Einstellungen**.
5. Verwenden Sie im folgenden Fenster das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Dateischutz zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie in Web Console und Cloud Console den Schutz für Dump-Dateien und Ablaufverfolgungsdateien

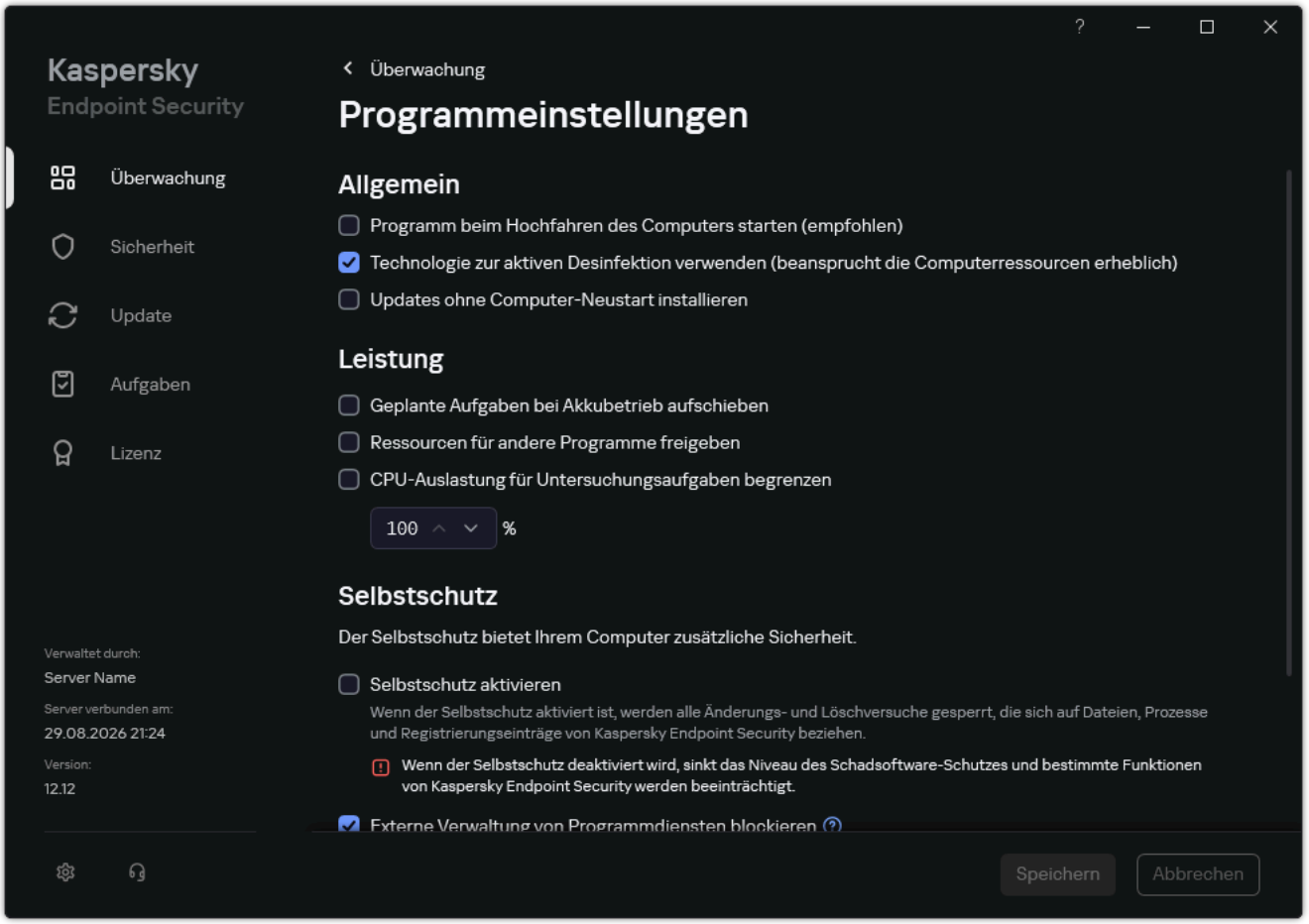
1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Endpoint Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Allgemeine Einstellungen → Technischer Support**.
5. Verwenden Sie im Block **Debug-Informationen** das Kontrollkästchen **Schutz für Dump- und Ablaufverfolgungsdateien AKTIVIERT**, um den Dateischutz zu aktivieren oder zu deaktivieren.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie über die App-Benutzeroberfläche den Schutz für Dump-Dateien und Ablaufverfolgungsdateien

1. Klicken Sie im Programmhauptfenster auf die Schaltfläche ⚙.

2. Wählen Sie im Fenster mit den Programmeinstellungen **Allgemeine Einstellungen → Programmeinstellungen** aus.



Einstellungen für „Kaspersky Endpoint Security für Windows“

3. Verwenden Sie im Block **Debug-Informationen** das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Dateischutz zu aktivieren oder zu deaktivieren.

4. Speichern Sie die vorgenommenen Änderungen.

Dump-Dateien und Protokolldateien, die bei aktiviertem Schutz aufgezeichnet wurden, bleiben nach dem Ausschalten dieser Funktion geschützt.

Betriebssystemdaten abrufen (Kaspersky Get System Info)

Nach der Installation von Kaspersky Endpoint Security kann es vorkommen, dass das Betriebssystem oder ein Programm nicht richtig funktioniert. Möglicherweise liegt ein Konflikt zwischen dem Programm und der Software oder den Treibern der Computerkomponenten vor.

Um die Ursache zu ermitteln, benötigt der Technische Support von Kaspersky einen Bericht des Kaspersky-Dienstprogramms „Get System Info“ (im Folgenden GSI genannt). Ausführliche Informationen über die Verwendung dieses Dienstprogramms finden Sie in der Kaspersky-Wissensdatenbank.

Einschränkungen und Warnungen

Kaspersky Endpoint Security besitzt eine Reihe von nicht kritischen Einschränkungen.

Programm installieren

- Besonderheiten im Hinblick auf die Unterstützung des Betriebssystems Microsoft Windows 10, Microsoft Windows Server 2016 und Microsoft Windows Server 2019 finden Sie in der Wissensdatenbank des Technischen Supports.
- Einzelheiten zur Unterstützung der Betriebssysteme Microsoft Windows 11 und Microsoft Windows Server 2022 finden Sie in der Wissensdatenbank des Technischen Supports.
- Nachdem das Programm auf einem infizierten Computer installiert wurde, informiert es den Benutzer nicht über die Notwendigkeit, eine Computeruntersuchung durchzuführen. Bei der Aktivierung des Programms können Probleme auftreten. Um diese Probleme zu lösen, starten Sie eine Untersuchung wichtiger Bereiche.
- Wenn in den Dateien setup.ini und setup.reg Nicht-ASCII-Zeichen (z. B. russische Buchstaben) verwendet werden, wird empfohlen, die Datei mit notepad.exe zu bearbeiten und die Datei in UTF-16LE-Kodierung zu speichern. Andere Kodierungen werden nicht unterstützt.
- Das Programm unterstützt nicht die Verwendung von Nicht-ASCII-Zeichen bei der Angabe des Programminstallationspfads in den Einstellungen des Installationspakets.
- Wenn Programmeinstellungen aus einer CFG-Datei importiert werden, wird der Wert der Einstellung, die die Teilnahme am Kaspersky Security Network definiert, nicht übernommen. Bitte lesen Sie nach dem Import der Einstellungen den Text der Erklärung zum Kaspersky Security Network und bestätigen Sie Ihr Einverständnis zur Teilnahme am Kaspersky Security Network. Sie können den Text der Erklärung in der Programmoberfläche oder in der Datei ksn_*.txt lesen, die sich in dem Ordner befindet, der das Programmverteilungskit enthält.
- Wenn Sie die Verschlüsselung (FLE oder FDE) oder die Gerätekontrolle-Komponente entfernen und dann neu installieren möchten, müssen Sie das System vor der Neuinstallation neu starten.
- Wenn Sie das Betriebssystem Microsoft Windows 10 verwenden, müssen Sie das System neu starten, nachdem Sie die Komponente File Level Encryption (FLE) entfernt haben.
- Beim Entfernen von individuellen Programmkomponenten (zum Beispiel mithilfe der Aufgabe *Auswahl der Programmkomponenten ändern*) könnte ein Neustart des Computers erforderlich sein.
- In den Eigenschaften der Aufgabe *Auswahl der Programmkomponenten ändern* wird beim Wechsel des Installationsmodus (**Getrennter Modus**/**Kombinierter Modus**) die Synchronisierung des Komponentensatzes zwischen den Modi nicht unterstützt. Das Programm synchronisiert den Komponentensatz zwischen den Modi, nachdem Sie die Aufgabeneigenschaften erneut geöffnet haben.
- Die Installation des Programms kann mit einem Fehler enden, der besagt, dass *ein Programm, dessen Name fehlt oder nicht lesbar ist, auf Ihrem Computer installiert ist*. Das bedeutet, dass inkompatible Programme oder Fragmente davon auf Ihrem Computer verbleiben. Um Artefakte von inkompatiblen Programmen zu entfernen, senden Sie eine Anfrage mit einer detaillierten Beschreibung der Situation über Kaspersky CompanyAccount an den technischen Support von Kaspersky.
- Wenn Sie die Deinstallation von Kaspersky Endpoint Security abgebrochen haben, starten Sie die nach dem Computer-Neustart die Wiederherstellung des Programms.

- Die Anwendung erfordert Microsoft .NET Framework 4.0 oder höher. Microsoft .NET Framework 4.6.1 enthält Schwachstellen. Wenn Sie Microsoft .NET Framework 4.6.1 verwenden, müssen Sie Sicherheits-Updates installieren. Ausführliche Informationen zu Sicherheits-Updates für Microsoft .NET Framework finden Sie auf der Website des technischen Supports von Microsoft.

- Wenn das Programm nicht erfolgreich mit der in einem Serverbetriebssystem ausgewählten Komponente des Kaspersky Endpoint Agent installiert wird und das Fenster *Fehler im Windows Installer Coordinator* erscheint, lesen Sie die Anweisungen auf der Support-Website von Microsoft.

- Wenn das Programm lokal im nicht-interaktiven Modus installiert wurde, verwenden Sie die mitgelieferte setup.ini-Datei, um die installierten Komponenten zu ersetzen.

- Nachdem Kaspersky Endpoint Security für Windows in einigen Konfigurationen von Windows 7 installiert wurde, funktioniert Windows Defender weiterhin. Es wird empfohlen, Windows Defender manuell zu deaktivieren, um eine Beeinträchtigung der Systemleistung zu verhindern.

- Wenn Sie Kaspersky Endpoint Security für Windows auf einem Server installieren, auf dem die Anwendungen Kaspersky Security für Windows Server (KSWS) und Windows Defender installiert sind, müssen Sie das System neu starten. Ein Neustart des Systems ist auch dann erforderlich, wenn Sie die Programm-Installation ohne Systemneustart aktiviert haben. Windows Defender für Windows Server gehört zur Liste der Software, die mit Kaspersky Endpoint Security für Windows inkompatibel ist. Windows Defender für Windows Server wird vom Installationsprogramm vor der Programm-Installation entfernt. Beim Entfernen inkompatibler Software ist ein Systemneustart erforderlich.

- Bevor Sie Kaspersky Endpoint Security für Windows (KES) auf einem Server installieren, auf dem Kaspersky Security für Windows Server (KSWS) installiert ist, müssen Sie den KSWS-Kennwortschutz deaktivieren. Nach der Migration von KSWS zu KES müssen Sie den Kennwortschutz in den Programmeinstellungen aktivieren.

- Um die Anwendung auf Computern unter Windows 7 oder Windows Server 2008 R2 mit installierter Veeam Backup & Replication-Software zu installieren, müssen Sie Ihren Computer möglicherweise neu starten und die Installation erneut durchführen.

- Die Migration von Kaspersky Small Office Security (KSOS) zu Kaspersky Endpoint Security (KES) mit aktiviertem „Kennwortschutz“ ist ab KSOS Version 21.16.*.* verfügbar. Um ältere Versionen von KSOS zu migrieren, müssen Sie den Kennwortschutz deaktivieren oder KSOS manuell entfernen. Die Migration von KSOS zu KES mit deaktiviertem Kennwortschutz wird korrekt ausgeführt.

- Kaspersky Endpoint Security kann nicht auf einem bootfähigen Wechseldatenträger installiert werden. Kaspersky Endpoint Security zeigt während der Installation eine Fehlermeldung an: *Der gewählte Ordner oder das Laufwerk ist ungültig. Das Programm muss auf einer lokalen Festplatte installiert werden.* Falls es Ihnen gelingt, das Programm mithilfe von Drittanbieter-Tools auf einem Wechseldatenträger zu installieren, kann dies zum Absturz des Betriebssystems (BSOD) während des Bootvorgangs führen. Mit anderen Worten: Windows To Go und ähnliche Lösungen werden von Kaspersky Endpoint Security nicht unterstützt. Wenn Sie einen Computer von einem Wechseldatenträger aus untersuchen möchten, verwenden Sie die kostenlose App Kaspersky Notfall-CD.

- Wenn Kaspersky Endpoint Security mit Netzwerkkomponenten auf einem Terminalserver mit Mehrbenutzer-RDP-Sitzungen installiert wird, sind einige Besonderheiten zu beachten. Nach dem Ende der Administratorsitzung erzwingt das Betriebssystem das Beenden aller Benutzersitzungen. Um eine Verbindung mit dem Terminalserver herzustellen, müssen Sie den Server neu starten oder sich lokal am System anmelden. Dieses Verhalten geht auf Besonderheiten des Windows-Betriebssystems zurück.

- Wenn die Web-Plug-ins für Kaspersky Endpoint Security für Windows (Version 12.11.0.2004) und Kaspersky Endpoint Security für Linux (Version 12.4.0.1354) in Kaspersky Security Center 16.0 oder Kaspersky Security Center 16.1 installiert sind, kann ein Update des Web-Plug-ins für Kaspersky Endpoint Security für Windows auf Version 12.11.0.6004 zu Störungen in den Richtlinien von Kaspersky Endpoint Security für Linux führen.

  Mögliche Lösung: Wechseln Sie zum Fenster „**Einstellungen → Web-Plug-ins**“ und entfernen Sie das Web-Plug-in für Kaspersky Endpoint Security für Windows, das Web-Plug-in für Kaspersky Endpoint Security für Linux und das Plug-in für einheitlichen Schutz und Verwaltung aus der Liste. 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.

- In der Web Console wird die Liste der Komponenten in den Eigenschaften des Installationspakets von Kaspersky Endpoint Security 12.11 für Windows fehlerhaft angezeigt. Die separate Komponente „Schutz vor Verschlüsselung“ ist in dieser Programmversion nicht verfügbar. Die Funktionalität zum Schutz vor der externen Verschlüsselung freigegebener Ordner ist in der Komponente „Verhaltensanalyse“ enthalten. In Kaspersky Endpoint Security 12.12 für Windows wird diese Funktionalität von einer separaten Komponente übernommen. Dabei wird in der Verwaltungskonsole (MMC) die Liste der Komponenten korrekt angezeigt.

- Bei Verwendung des Web-Plug-ins ab Version 7.0 wird in den Eigenschaften des Installationspakets für Kaspersky Endpoint Security 14.1 und ältere Versionen die Liste der standardmäßig zur Installation ausgewählten Komponenten falsch angezeigt. Wenn diese Liste beim Erstellen des Installationspakets nicht geändert wird, wird das Programm mit den Standardkomponenten installiert, die für die entsprechende Programmversion festgelegt sind.

Programm-Upgrade

- Ab Anwendungsversion 11.0.0 können Sie das MMC-Plug-in für Kaspersky Endpoint Security für Windows über die vorherige Plug-in-Version installieren. Um zur vorherigen Plug-in-Version zurückzukehren, löschen Sie das aktuelle Plug-in und installieren Sie eine ältere Version des Plug-ins.

- Beim Upgrade von Kaspersky Endpoint Security 11.0.0 oder 11.0.1 für Windows werden die Einstellungen des Zeitplans für lokale Aufgaben für *Update der Datenbanken und Programm-Module*, *Untersuchung wichtiger Bereiche*, *Benutzerdefinierte Untersuchung* und *Prüfung der Anwendungsintegrität* nicht gespeichert.

- Auf Computern mit Windows 10 Version 1903 und 1909 können Upgrades von Kaspersky Endpoint Security 10 für Windows Service Pack 2 Maintenance Release 3 (Build 10.3.3.275), Service Pack 2 Maintenance Release 4 (Build 10.3.3.304), 11.0.0 und 11.0.1 mit installierter File Level Encryption (FLE)-Komponente mit einem Fehler enden. Dies liegt daran, dass die Dateiverschlüsselung für diese Versionen von Kaspersky Endpoint Security für Windows in Windows 10 Version 1903 und 1909 nicht unterstützt wird. Vor der Installation dieses Upgrades wird Ihnen empfohlen, die Dateiverschlüsselungskomponente zu entfernen.

- Die Anwendung erfordert Microsoft .NET Framework 4.0 oder höher. Microsoft .NET Framework 4.6.1 enthält Schwachstellen. Wenn Sie Microsoft .NET Framework 4.6.1 verwenden, müssen Sie Sicherheits-Updates installieren. Ausführliche Informationen zu Sicherheits-Updates für Microsoft .NET Framework finden Sie auf der Website des technischen Supports von Microsoft.

- Beim Upgrade von Kaspersky Endpoint Security deaktiviert die Anwendung die KSN-Verwendung solange, bis die Erklärung zu Kaspersky Security Network akzeptiert wurde. Außerdem kann sich der Computerstatus in Kaspersky Security Center in *Kritisch* ändern; Das Ereignis *KSN-Server sind nicht verfügbar* wird empfangen. Wenn Sie Kaspersky Managed Detection and Response verwenden, erhalten Sie Ereignisse über Verstöße beim Betrieb der Lösung. Die Verwendung von KSN ist für den Betrieb von „Kaspersky Managed Detection and Response“ erforderlich. Kaspersky Endpoint Security aktiviert die KSN-Verwendung, nachdem die Richtlinie übernommen wurde, in welcher der Administrator die KSN-Nutzungsbedingungen akzeptiert. Sobald die Erklärung zu Kaspersky Security Network akzeptiert wurde, wird Kaspersky Endpoint Security fortgesetzt.

- 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.

- Nach dem Upgrade von Kaspersky Endpoint Security auf einem Computer mit Microsoft Windows 11 enthält das Kontextmenü für Dateien möglicherweise Einträge für die vorherige und die neue App-Version. Starten Sie Ihren Computer zweimal neu, um sicherzustellen, dass das Kontextmenü für Dateien korrekt funktioniert.

- Wenn der Selbstschutz der App deaktiviert ist und alle Netzwerkadapter beendet wurden, funktionieren die Netzwerk-Komponenten der App zwischen dem App-Upgrade und dem Neustart des Computers nicht. Zu den Netzwerk-Komponenten der App zählen: Schutz vor Web-Bedrohungen, Schutz vor E-Mail-Bedrohungen, Schutz vor Netzwerkbedrohungen, Firewall, Programm-Überwachung und Web-Kontrolle. Starten Sie den Computer neu, damit die App korrekt funktioniert.

- Die Komponente „Schutz vor modifizierten USB-Geräten" funktioniert zwischen dem App-Upgrade und dem Neustart des Computers nicht. Starten Sie den Computer neu, damit die App korrekt funktioniert.

- Ein Programm-Upgrade ist erst möglich, nachdem der vorherige Upgrade-Vorgang abgeschlossen wurde. Starten Sie den Computer neu, damit die App korrekt funktioniert.

- Nachdem das Programm von Versionen vor Kaspersky Endpoint Security 11 für Windows aktualisiert wurde, muss der Computer neu gestartet werden.

- Wenn Sie Kaspersky Endpoint Security über die Kaspersky Security Center Cloud Console verwalten, ist ein lokales Programm-Update nicht zulässig. Wenn das Programm lokal aktualisiert wird, ist es nicht möglich, die Vereinbarung zur Datenverarbeitung für Kaspersky Security Center Cloud Console zu akzeptieren.

Unterstützung der Arm-Architektur

- Die Installation von Kaspersky Endpoint Security im Light Agent-Modus auf Arm-basierten virtuellen Maschinen wird nicht unterstützt.

- Die Kaspersky-Festplattenverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

- Die Dateiverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

- Die Verschlüsselung von Wechseldatenträgern wird auf Arm-basierten Computern wird nicht unterstützt.

- Auf Computern mit Windows 11 für Arm64 ist EDR Agent nicht mit Bitdefender Endpoint Security Tools kompatibel.

- Die Funktionen zum Schutz von Audiosignalen und zum Schutz des Webcam-Zugriffs werden auf Arm-basierten Computern nicht unterstützt.

- Auf Arm-basierten Computern unterstützt die Erweiterung für den Schutz vor E-Mail-Bedrohungen die 32-Bit- und 64-Bit-Versionen von Outlook 2016, Outlook 2021, Outlook 2024 und Outlook 365 für Arm64.

- Kaspersky Endpoint Security sendet Objekte, die für die Arm-Architektur bestimmt sind, nicht an Kaspersky Sandbox.

- Die Drucksteuerung wird auf Arm-basierten Computern nicht unterstützt.

- Auf Arm-basierten Computern unterstützt die Aufgabe *IOC-Untersuchung* nur E-Mail-Dateien von den folgenden E-Mail-Clients: 32-Bit- und 64-Bit-Versionen von Outlook 2016 und Outlook 2021, 2024 und 365 für Arm64.

- Auf Computern mit Windows 11 für Arm64 ist die tokenbasierte Authentifizierung möglicherweise nicht verfügbar, da das Betriebssystem kein gültiges Zertifikat auf dem Token erkennen kann. Dieses Verhalten wird durch die Art und Weise verursacht, wie das Betriebssystem mit der Token-Software interagiert. Beispielsweise verfügt das Betriebssystem möglicherweise nicht über die Treiber, die für die Funktion des Tokens erforderlich sind. In diesem Fall unterstützt Kaspersky Endpoint Security ebenfalls keine tokenbasierte Authentifizierung (Kennwortschutz). Sie können andere Authentifizierungsmethoden verwenden, beispielsweise Benutzeranmeldedaten.

Unterstützung für virtuelle Plattformen

- Auf Servern, auf denen die *Deduplizierung von Daten* aktiviert ist, müssen Sie die Datei fsdmhost.exe zur Liste der vertrauenswürdigen Programme hinzufügen. Dadurch lässt sich die Leistung optimieren und eine übermäßige Belastung des Prozessors verhindern.

- Das Dateisystem ReFS wird nur eingeschränkt unterstützt:

  - Kaspersky Endpoint Security verarbeitet Ereignisse über die Desinfektion von Bedrohungen möglicherweise falsch. Wenn die Anwendung beispielsweise eine schädliche Datei gelöscht hat, enthält der Bericht möglicherweise den Eintrag „Objekt nicht verarbeitet“. Trotzdem desinfiziert Kaspersky Endpoint Security Bedrohungen gemäß den Programmeinstellungen. Außerdem kann Kaspersky Endpoint Security für dasselbe Objekt ein Duplikat des Ereignisses *Objekt wird beim Neustart desinfiziert* erstellen.

  - Der „Schutz vor bedrohlichen Dateien“ kann manche Bedrohungen überspringen. Die Schadsoftware-Untersuchung funktioniert aber trotzdem korrekt.

  - Nachdem die Aufgabe *Schadsoftware-Untersuchung* gestartet wurde, werden die mit iChecker hinzugefügten Ausnahmen beim Server-Neustart zurückgesetzt.

  - Die iSwift-Technologie wird nicht unterstützt. Kaspersky Endpoint Security ist nicht dafür gedacht, Ausnahmen zu scannen, die unter Verwendung der iSwift-Technologie hinzugefügt wurden.

  - Kaspersky Endpoint Security erkennt die Dateien eicar.com und susp-eicar.com nicht, wenn auf dem Computer die Datei meicar.exe vorhanden war, bevor Kaspersky Endpoint Security installiert wurde.

  - Kaspersky Endpoint Security zeigt möglicherweise inkorrekte Benachrichtigungen über die Bedrohungsdesinfektion an. Beispielsweise kann die Anwendung eine Benachrichtigung über eine Bedrohung anzeigen, die bereits desinfiziert wurde.

- Die Technologien „Verschlüsselung von Dateien“ (FLE) und „Kaspersky-Festplattenverschlüsselung“ (FDE) werden auf Server-Plattformen nicht unterstützt. Gleichzeitig kann Kaspersky Endpoint Security Ereignisse über die Datenverschlüsselung falsch verarbeiten.

- In Serverbetriebssystemen wird keine Warnung bezüglich der Notwendigkeit einer erweiterten Desinfektion angezeigt.

- Microsoft Windows Server 2008 wurde von der Unterstützung ausgeschlossen. Die Programminstallation auf einem Computer mit dem Betriebssystem Microsoft Windows Server 2008 wird nicht unterstützt.

- Wenn Kaspersky Endpoint Security auf einem Server installiert wird, auf dem Microsoft Data Protection Manager (DPM) bereitgestellt wurde, kann es im DPM zu Fehlfunktionen kommen. Dies hängt mit Einschränkungen des DPM zusammen. Um die Fehlfunktionen zu beheben, müssen Sie den Ausnahmen für die Komponenten „Schutz vor bedrohlichen Dateien“ und für die Aufgaben zur *Schadsoftware-Untersuchung* die lokalen Serverlaufwerke hinzufügen.

- Der Server Core-Modus wird mit Einschränkungen unterstützt:
  - Die lokale grafische Benutzeroberfläche ist nicht verfügbar, einschließlich Benachrichtigungen, Pop-up-Benachrichtigungen und sonstiger Elemente der Benutzeroberfläche. Das Programm kann keine Eingabeaufforderungsfenster anzeigen. Dies gilt auch für die folgenden Fenster:
    - Bestätigungsaufforderung für das Upgrade der Programmversion und der Module;
    - Eingabeaufforderung für den Neustart des Computers;
    - Eingabeaufforderung für Anmeldedaten zur Proxyserver-Authentifizierung;
    - Eingabeaufforderung, um Zugriff auf ein Gerät zu erhalten (Gerätekontrolle).
  - Die folgenden Komponente sind nicht verfügbar: „Schutz vor Web-Bedrohungen“, „Schutz vor E-Mail-Bedrohungen“, „Web-Kontrolle“, „Schutz vor modifizierten USB-Geräten“.
  - „Anti-Bridging“ ist nicht verfügbar.
  - Die Erklärung zu Kaspersky Security Network können Sie nur in der Programmrichtlinie in der Kaspersky Security Center-Konsole akzeptieren.
  - Die BitLocker-Laufwerkverschlüsselung ist nur mit einem Trusted Platform Module (TPM) verfügbar. Für die Verschlüsselung kann keine PIN bzw. kein Passwort verwendet werden, da das Programm das Kennwortabfragefenster für die Preboot-Authentifizierung nicht anzeigen kann. Wenn für das Betriebssystem der FIPS-Kompatibilitätsmodus (Federal Information Processing Standard) aktiviert ist, verbinden Sie einen Wechseldatenträger zum Speichern des Chiffrierschlüssels, bevor Sie mit der Verschlüsselung des Laufwerks beginnen.

Unterstützte virtuelle Plattformen:

- Full Disk Encryption (FDE) wird auf virtuellen Hyper-V-Maschinen nicht unterstützt.
- Full Disk Encryption (FDE) wird auf virtuellen Citrix-Plattformen nicht unterstützt.
- Die Betriebssysteme Windows 10 Enterprise Multi-Session und Windows 11 Enterprise Multi-Session werden mit Einschränkungen unterstützt:
  - Kaspersky Endpoint Security desinfiziert aktive Bedrohungen, ohne den Benutzer zu benachrichtigen. Das Vorgehen entspricht der Desinfektion aktiver Bedrohungen auf Servern. Da das Betriebssystem weiterhin im Multisession-Modus ausgeführt wird, verlieren andere aktive Benutzer möglicherweise ihre Daten, wenn die Bedrohung nicht sofort neutralisiert wird.
  - Die vollständige Festplattenverschlüsselung (FDE) wird nicht unterstützt.
  - Die Verwaltung von BitLocker wird nicht unterstützt.
  - Die Verwendung von Kaspersky Endpoint Security mit Wechseldatenträgern wird nicht unterstützt. Die Microsoft Azure-Infrastruktur definiert Wechseldatenträger als Netzlaufwerke.
- Die Installation und Verwendung von Verschlüsselung auf Dateiebene (FLE) wird auf virtuellen Citrix-Plattformen nicht unterstützt.

- Um die Kompatibilität von Kaspersky Endpoint Security für Windows mit Citrix PVS zu gewährleisten, führen Sie die Installation mit aktivierter Option **Kompatibilität mit Citrix PVS gewährleisten** aus. Diese Option kann im Installationsassistenten oder durch Verwendung des Befehlszeilenparameters `/pCITRIXCOMPATIBILITY=1` aktiviert werden. Im Falle einer Ferninstallation muss die KUD-Datei durch Hinzufügen des folgenden Parameters bearbeitet werden: `/pCITRIXCOMPATIBILITY=1`.

- Citrix XenDesktop. Bevor Sie mit dem Klonen beginnen, müssen Sie den Selbstschutz-Mechanismus deaktivieren, um virtuelle Maschinen zu klonen, die vDisk verwenden.

- Wenn Sie einen Referenzcomputer für das Citrix XenDesktop-Master-Image mit vorinstalliertem Kaspersky Endpoint Security für Windows und dem Kaspersky Security Center Administrationsagenten vorbereiten, fügen Sie der Konfigurationsdatei die folgenden Arten von Ausnahmen hinzu:

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  Einzelheiten zu Citrix XenDesktop finden Sie auf der Support-Website von Citrix.

- In einigen Fällen kann der Versuch, einen Wechseldatenträger sicher zu trennen, bei einer virtuellen Maschine fehlschlagen, die auf einem VMware ESXi-Hypervisor bereitgestellt wird. Versuchen Sie noch einmal, das Gerät sicher zu trennen.

- Kaspersky Endpoint Security ist mit dem VMware ESXi-Hypervisor kompatibel, wobei die folgenden Einschränkungen gelten:

  - Kaspersky Endpoint Security ist möglicherweise mit den Guest Introspection-Treibern (vnetWFP.sys, vnetFLT.sys und andere) inkompatibel. Um die Inkompatibilität zu beheben, aktualisieren Sie die Treiber auf die neueste Version oder deinstallieren Sie die Treiber.

  - In einigen Fällen kann der Versuch, einen Wechseldatenträger aus einer virtuellen Maschine sicher zu entfernen, fehlschlagen. Versuchen Sie noch einmal, das Gerät sicher zu trennen.

- Die Installation von Kaspersky Endpoint Security auf virtuellen Maschinen mit dem Citrix VDA-Agenten kann zu einem Kompatibilitätsfehler führen. Der Grund: Citrix Provisioning Services ist nur eingeschränkt mit Antiviren-Lösungen kompatibel. Bewährte Methoden für die Verwendung von Antiviren-Lösungen mit Citrix Provisioning Services finden Sie auf der Support-Website von Citrix.

- Kaspersky Endpoint Security überspringt die Untersuchung eines Wechseldatenträgers, wenn dieser mit einer virtuellen Maschine auf dem Citrix-Hypervisor verbunden ist (Aufgabe *Untersuchung von Wechseldatenträgern*). Auf solchen Geräten erkennt das Betriebssystem den angeschlossenen Wechseldatenträger als Netzlaufwerk. In solchen Fällen können Sie die Aufgabe *Benutzerdefinierte Untersuchung* verwenden. Das Verhalten des Programms im Standardmodus und im Light Agent-Modus ist gleich.

- Ist Kaspersky Endpoint Security auf einer virtuellen Maschine in einer Infrastruktur installiert, die die Citrix App Layering-Technologie verwendet, werden Dateien, die vom Programm als infiziert erkannt wurden und den Status *Objekt wird beim Neustart gelöscht* haben, beim Neustart der virtuellen Maschine nicht automatisch entfernt.

  Um solche Dateien zu löschen, müssen Sie die VHDX-Datei, die den Benutzer-Layer enthält, auf dem Computer des Citrix App Layering-Administrators bereitstellen und auf dem bereitgestellten Datenträger eine Untersuchung auf Schadsoftware ausführen.

- Bevor Sie einen Golden-Image-Snapshot einer virtuellen Maschine mit installiertem Kaspersky Endpoint Security erstellen, wird empfohlen, die virtuelle Maschine herunterzufahren und einen „kalten" Snapshot zu erstellen. Wenn Sie einen Snapshot erstellen, während die virtuelle Maschine ausgeführt wird (einen „heißen" Snapshot), kann der ordnungsgemäße Betrieb des Programms nicht garantiert werden.

Kompatibilität mit Kaspersky Security Center

- In der „Web Console" von Kaspersky Security Center Version 14.1 und früher werden die Namen der Funktionsbereiche für die Komponenten „Protokollanalyse" und „Überwachung der Datei-Integrität" im Abschnitt für die Einstellungen der Benutzerzugriffsberechtigungen in den Administrationsserver-Eigenschaften nicht korrekt angezeigt.

- Nach der Reparatur der Anwendung wird der Schutz für die Verbindung des Computers zum Administrationsserver deaktiviert. Führen Sie nach der Reparatur der Anwendung die Aufgabe *Schutz der Verbindung zum Administrationsserver* erneut aus.

- In der Kaspersky Security Center-Verwaltungskonsole werden im Fenster **Benutzer oder Benutzergruppe auswählen** nur die ersten 50.000 Benutzer aus der Liste der Benutzer von Kaspersky Security Center angezeigt. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Security Center.

- Wenn Sie in der Verwaltungskonsole von Kaspersky Security Center nach verwalteten Geräten suchen, werden auf der Registerkarte **Programmkomponenten** möglicherweise mehrere Varianten des Namens derselben Programmkomponente angezeigt, einschließlich Namen, die älteren Versionen von Kaspersky Endpoint Security entsprechen. Auch die Namen einiger Komponenten können doppelt vorkommen.

  Um nach einer Komponente zu suchen, müssen Sie lediglich eine der angezeigten Varianten auswählen. Weitere Informationen über die Geräte-Ermittlung finden Sie in der Hilfe zu Kaspersky Security Center.

- In Kaspersky Security Center Web Console 15.1 Update 2 funktionieren bei installiertem Kaspersky Endpoint Security für Windows Web-Plug-in der Version 12.11 oder höher und installiertem Unified Protection and Management Plug-in die Profilaktivierungsbedingungen für die Richtlinie nicht. Kaspersky Security Center fügt der Konsole keine neuen Geräte hinzu, welche die Profilaktivierungsbedingungen erfüllen.

Lizenzverwaltung

- Wenn die Systemmeldung *Fehler beim Datenempfang* angezeigt wird, überprüfen Sie, ob der Computer, auf dem Sie die Aktivierung durchführen, über Netzwerkzugriff verfügt, oder konfigurieren Sie die Aktivierungseinstellungen über den Aktivierungs-Proxy von Kaspersky Security Center.

- In der Programmoberfläche wird das Ablaufdatum der Lizenz in der lokalen Zeit des Computers angezeigt.

- Die Installation des Programms mit einer eingebetteten Schlüsseldatei auf einem Computer mit instabilem Internetzugang kann zur temporären Anzeige von Ereignissen führen, die besagen, dass das Programm nicht aktiviert ist oder dass die Lizenz den Betrieb der Komponente nicht zulässt. Der Grund dafür ist, dass die App während des Installationsvorgangs zuerst die eingebettete Testlizenz aktiviert. Ein Internetzugang ist erforderlich.

- Während des Testzeitraums kann die Installation eines Programm-Upgrades oder Patches auf einem Computer mit instabilem Internetzugang dazu führen, dass vorübergehend Ereignisse angezeigt werden, die besagen, dass das Programm nicht aktiviert ist. Der Grund dafür ist, dass die App bei der Update-Installation zuerst die eingebettete Testlizenz aktiviert. Ein Internetzugang ist erforderlich.

- Wenn die Testlizenz bei der Installation des Programms automatisch aktiviert und das Programm dann entfernt wurde, ohne die Lizenzinformationen zu speichern, wird das Programm bei einer Neuinstallation nicht automatisch mit der Testlizenz aktiviert. Aktivieren Sie in diesem Fall das Programm manuell.

- Wenn Sie Kaspersky Security Center Version 11 und Kaspersky Endpoint Security Version 14.2 verwenden, funktionieren die Berichte über die Komponentenleistung möglicherweise fehlerhaft. Wenn Sie Komponenten von Kaspersky Endpoint Security installiert haben, die nicht in Ihrer Lizenz enthalten sind, sendet der Administrationsagent möglicherweise Fehler über den Komponentenstatus an das Windows-Ereignisprotokoll. Um solche Fehler zu vermeiden, entfernen Sie die Komponenten, die nicht in Ihrer Lizenz enthalten sind.

Schutz vor E-Mail-Bedrohungen

- Wenn Sie E-Mails mit der Schutz vor E-Mail-Bedrohungen-Erweiterung für Microsoft Outlook untersuchen, empfehlen wir die Verwendung des Exchange-Server-Cache-Modus (Exchange-Cache-Modus verwenden).

- Kaspersky Endpoint Security unterstützt die 64-Bit-Version des E-Mail-Clients Microsoft Outlook nicht. Das bedeutet: Kaspersky Endpoint Security untersucht Microsoft Outlook-Dateien (PST- und OST-Dateien) nicht, wenn eine 64-Bit-Version von Microsoft Outlook auf dem Computer installiert ist. Dies gilt auch, wenn E-Mails zum Untersuchungsbereich gehören.

- Kaspersky Endpoint Security unterstützt den Mail-Client Microsoft Outlook New nicht.

- Wenn Sie die Desinfektion von Bedrohungen, die vom Schutz vor E-Mail-Bedrohungen erkannt wurden, deaktiviert haben und eine infizierte E-Mail in Ihrem Outlook-Postfach erhalten, kann der Schutz vor Web-Bedrohungen die Kommunikation mit dem Exchange-Server über MAPI blockieren. Der Schutz vor Web-Bedrohungen erstellt daraufhin ein Ereignis über die Erkennung einer Bedrohung und sendet es an Kaspersky Security Center. Um die Verbindung zwischen dem Computer und dem Exchange-Server wiederherzustellen, müssen Sie die infizierte E-Mail manuell aus dem Outlook-Postfach löschen.

  Wenn Sie die Programmversion aktualisieren, ohne den Computer neu zu starten, ist das Schutzniveau des Schutzes vor E-Mail-Bedrohungen vorübergehend reduziert (für bis zu eine Minute). Wenn Sie während der Aktualisierung des Programms eine infizierte E-Mail in Ihrem Outlook-Postfach erhalten, blockiert der Schutz vor Web-Bedrohungen auch die Verbindung zum Exchange-Server über MAPI. Um die Verbindung wiederherzustellen, löschen Sie die infizierte E-Mail aus dem Outlook-Postfach.

Rollback von schädlichen Aktionen

- Das Programm stellt Dateien nur auf Geräten mit dem Dateisystem NTFS und FAT32 wieder her.

- Das Programm stellt Dateien mit einer Größe von bis zu 100 MB wieder her.

- Das Programm stellt Dateien mit folgenden Erweiterungen wieder her: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.

- Dateien, die sich auf Netzlaufwerken und wiederbeschreibbaren CD/DVD-Disks befinden, können nicht wiederhergestellt werden.

- Dateien, die mithilfe von Encryption File System (EFS) verschlüsselt wurden, können nicht wiederhergestellt werden. Details über die Funktion von EFS finden Sie auf der Microsoft-Website.

- Veränderungen von Dateien, die von Prozessen auf der Kernel-Ebene des Betriebssystems ausgeführt wurden, werden vom Programm nicht kontrolliert.

Firewall

- Wenn eine Regel für Netzpakete oder eine Netzwerkregel für Programme DNS-Namen vorgibt, kann Kaspersky Endpoint Security Anfragen an den DNS-Server senden, um die IP-Adressen dieser Ressourcen zu ermitteln. Die Firewall verwendet IP-Adressen, um die Netzwerkaktivität zu überwachen. Aus diesem Grund löst das Programm DNS-Namen in IP-Adressen auf. Es wird empfohlen, DNS-Namen in Regeln nur für LAN-Computer oder interne Dienste zu verwenden.

- Um eine Regel für alle IPv6-Adressen anzugeben, fügen Sie den Adressbereich ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff hinzu. Die Maske ::/0 wird von der Firewall nicht unterstützt.

- Die Filterung von Paketen oder Verbindungen nach lokaler Adresse, physischer Schnittstelle und Paketlaufzeit (TTL) wird in den folgenden Fällen unterstützt:

  - Nach lokaler Adresse für ausgehende Pakete oder Verbindungen in Programmregeln für TCP und UDP und Paketregeln.

  - Nach lokaler Adresse für eingehende Pakete oder Verbindungen (außer UDP) in Blockierungsregeln für Anwendungen und Paketregeln.

  - Nach Paketlaufzeit (TTL) in Blockpaketregeln für eingehende oder ausgehende Pakete.

  - Nach Netzwerkschnittstelle für eingehende und ausgehende Pakete oder Verbindungen in Paketregeln.

- Wenn Sie ein Netzwerkadapter oder eine Paket-Lebensdauer (TTL) für eine Paket-Erlaubnisregel konfiguriert haben, hat diese Regel eine niedrigere Priorität als eine blockierende Programmregel. Mit anderen Worten: Wenn die Netzwerkaktivität für ein Programm blockiert ist (z. B. da das Programm zur Sicherheitsgruppe *Stark beschränkt* gehört), können Sie die Netzwerkaktivität des Programms erlauben, indem Sie eine Paketregel mit diesen Einstellungen verwenden. In allen übrigen Fällen hat eine Paketregel eine höhere Priorität als eine Netzwerkregel für Programme.

- Wenn Firewall-Paketregeln importiert werden, kann Kaspersky Endpoint Security die Regelnamen ändern. Die Anwendung ermittelt Regeln, die identische Sätze von allgemeinen Parametern haben: Protokoll, Richtung, Remote-Ports und lokale Ports, Paket-Lebensdauer (TTL). Haben mehrere Regeln den gleichen Satz mit allgemeinen Parametern, so weist das Programm diesen Regeln denselben Namen zu oder fügt dem Namen einen Parameter-Tag hinzu. Kaspersky Endpoint Security importiert also alle Paketregeln, aber die Namen von Regeln mit identischen allgemeinen Parametern werden eventuell geändert.

- Wenn Sie die Berichterstattung für Anwendungsereignisse in einer Netzwerkregeln aktiviert haben und die Anwendung in eine andere Sicherheitsgruppe verschoben wird, werden die Beschränkungen dieser Gruppe nicht übernommen. Beispiel: Gehört die Anwendung zur Sicherheitsgruppe „Vertrauenswürdig“, so gelten für sie keine Netzwerkbeschränkungen. Dadurch wurde die Berichterstattung für dieses Programm aktiviert und es wurde in die Sicherheitsgruppe *Nicht vertrauenswürdig* verschoben. Dann erzwingt die „Firewall“ keine Netzwerkbeschränkungen für diese Anwendung. Wir empfehlen Ihnen, die Anwendung zuerst in die passende Sicherheitsgruppe zu verschieben und erst danach die Berichterstattung zu aktivieren. Ist diese Methode nicht geeignet, so können Sie die Beschränkungen für diese Anwendung in den Einstellungen der Netzwerkregel manuell anpassen. Die Beschränkung gilt nur für die lokale Schnittstelle der Anwendung. Das Verschieben der Anwendung zwischen unterschiedlichen Sicherheitsgruppe in der Richtlinie funktioniert korrekt.

- Die Komponenten „Firewall“ und „Programm-Überwachung“ haben gemeinsame Einstellungen: Anwendungsrechte und geschützte Ressourcen. Wenn Sie die Einstellungen für die „Firewall“ ändern, übernimmt Kaspersky Endpoint Security die neuen Einstellungen automatisch für die „Programm-Überwachung“. Wenn Sie z. B. Änderungen an den allgemeinen Einstellungen der „Firewall“-Richtlinie erlaubt haben (das Vorhängeschloss ist offen), können auch die Einstellungen der „Programm-Überwachung“ geändert werden.

- Wenn eine Netzwerkregel für Pakete in Kaspersky Endpoint Security 11.6.0 oder älter ausgelöst wird, steht in der Spalte **Programmname** im Firewall-Bericht immer der Wert *Kaspersky Endpoint Security*. Darüber hinaus blockiert die Firewall die Verbindung für alle Programme auf Paketebene. Dieses Verhalten wurde in Kaspersky Endpoint Security 11.7.0 und späteren Versionen verändert. Die Spalte **Regeltyp** wurde dem Firewall-Bericht hinzugefügt. Wird eine Netzwerkregel für Pakete ausgelöst, so bleibt der Wert in der Spalte **Programmname** leer.

- Wenn Sie mithilfe der Firewall alle Netzwerkaktivitäten verboten haben, erkennt die Komponente „Schutz vor Netzwerkbedrohungen“ möglicherweise einen Port-Scanning-Angriff. Dies kann folgenden Grund haben: Das Programm startet den Schutz vor Netzwerkbedrohungen vor der Firewall, um verdächtige Aktivitäten im Netzwerk zu erkennen.

Schutz vor modifizierten USB-Geräten

- Kaspersky Endpoint Security setzt die Zeitüberschreitung der USB-Gerätesperre zurück, wenn der Computer gesperrt ist (z. B. Zeitüberschreitung der Bildschirmsperre). Das heißt, falls Sie einen falschen Autorisierungscode für das USB-Gerät mehrmals eingeben und das Programm das USB-Gerät sperrt, dann ermöglicht Kaspersky Endpoint Security, den Autorisierungsversuch nach dem Entsperren des Computers zu wiederholen. In diesem Fall sperrt Kaspersky Endpoint Security das USB-Gerät nicht für einen Zeitraum, der in den Einstellungen der Komponente Schutz vor modifizierten USB-Geräten festgelegt wurde.

- Kaspersky Endpoint Security setzt das Zeitlimit für die Sperrung des USB-Geräts zurück, wenn der Computerschutz angehalten wird. Das heißt, wenn Sie mehrmals einen falschen Autorisierungscode für das USB-Gerät eingeben und das Programm das USB-Gerät sperrt, dann erlaubt es Kaspersky Endpoint Security, den Autorisierungsversuch nach dem Wiederherstellen des Computerschutzes zu wiederholen. In diesem Fall sperrt Kaspersky Endpoint Security das USB-Gerät nicht für einen Zeitraum, der in den Einstellungen der Komponente Schutz vor modifizierten USB-Geräten festgelegt wurde.

Kaspersky Security Network

- Kaspersky Endpoint Security unterstützt kein HTTPS beim Herstellen einer Verbindung zum KSN-Proxy (das Kontrollkästchen **HTTPS verwenden** ist in den KSN-Proxy-Verbindungseinstellungen aktiviert), wenn die Serveradresse nicht-lateinische Buchstaben (Nicht-ASCII-Symbole) enthält.

- Wird in Kaspersky Security Center von der Verwendung des globalen Kaspersky Security Network zur Verwendung eines privaten Kaspersky Security Network (KPSN) gewechselt oder umgekehrt, so wird in der Richtlinie des entsprechenden Produkts die Option zur Teilnahme an Kaspersky Security Network deaktiviert. Lesen Sie nach dem Wechsel den Text der Erklärung zum Kaspersky Security Network sorgfältig durch und bestätigen Sie Ihr Einverständnis zur Teilnahme am KSN. Sie können den Text der Erklärung in der Programmoberfläche oder beim Bearbeiten der Produktrichtlinie lesen.

- Ab Kaspersky Endpoint Security 12.9 für Windows müssen Sie beim Wechsel von KPSN zu Global KSN erneut der Erklärung zu Kaspersky Security Network zustimmen. Dazu müssen Sie die Verwendung von Kaspersky Security Network in den Richtlinieneigenschaften oder auf der Programmoberfläche aktivieren und die Erklärung zu Kaspersky Security Network akzeptieren. Wenn Sie Global KSN bereits verwendet haben, müssen Sie die KSN-Nutzung zuerst deaktivieren, dann wieder aktivieren und die Erklärung zu Kaspersky Security Network akzeptieren. Wenn Sie nicht mit der Erklärung zu Kaspersky Security Network einverstanden sind, kann das Programm nicht auf die Daten von Kaspersky Security Network zugreifen.

- Kaspersky Endpoint Security sendet Textdateien (z. B. txt-, csv-, log- und docx-Dateien ohne Makros) nicht zur Untersuchung an Kaspersky Security Network. Das Programm sendet Dateien, die eine Gefahr darstellen können, zur Untersuchung an KSN. Zu diesen Dateien gehören ausführbare Dateien oder Dateien, die ausführbaren Code enthalten können (z. B. Makros in docx-Dateien). Für die Untersuchung von Textdateien sind andere Programmkomponenten verantwortlich. Die Reputation einer Textdatei können Sie auch manuell über das Kontextmenü der Datei überprüfen. Wenn eine Textdatei die Reputation *Nicht vertrauenswürdig (Kaspersky Security Network)* hat, ignoriert das Programm die Aktion, die für erkannte Bedrohungen festgelegt wurde.

Programmkontrolle

- Es wird empfohlen, bei der Arbeit mit den Regeln der Programmkontrolle nicht mehr als 100.000 Ein- und Ausschlussbedingungen für Programme aus verschiedenen Kategorien hinzuzufügen. Dabei wird vorausgesetzt, dass Kaspersky Endpoint Security auf einem Computer ausgeführt wird, der die Hardware-Anforderungen erfüllt und unter Microsoft Windows 10 läuft.

- Wenn Regeln der „Programmkontrolle“ über die Kaspersky Security Center Web Console verwendet werden, werden nur Archive im ZIP-Format unterstützt. Andere Archivformate wie RAR oder 7z werden nicht unterstützt. Diese Beschränkung besteht nicht, wenn Regeln der „Programmkontrolle“ über die Verwaltungskonsole (MMC) bearbeitet werden.

- Wenn Sie mit Regeln der Programmkontrolle in der Kaspersky Security Center Web Console arbeiten, ist die Größe einer hochzuladenden Datei auf 104 MB beschränkt. Diese Beschränkung besteht nicht, wenn Regeln der „Programmkontrolle“ über die Verwaltungskonsole (MMC) bearbeitet werden.

- Bei der Arbeit in Microsoft Windows 10 im Denylist-Modus von Programmen können Blockierungsregeln falsch angewendet werden, was zur Blockierung von Programmen führen kann, die nicht in Regeln angegeben sind.

- Wenn Sie neue *vordefinierte Regeln für die Programmkontrolle* hinzugefügt haben und Kaspersky Endpoint Security upgraden, können Sie diese Regeln nicht auf ältere Versionen des Programms anwenden.

- Wenn progressive Webanwendungen (PWA) durch die Komponente Programmkontrolle blockiert werden, wird appManifest.xml im Bericht als das blockierte Programm angezeigt.

- Es wird empfohlen, beim Hinzufügen des Standardprogramms „Editor“ zu einer Regel der Programmkontrolle für Windows 11 nicht den Pfad zum Programm anzugeben. Auf Computern mit Windows 11 verwendet das Betriebssystem das Programm „Metro Notepad“, das sich im Ordner `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` befindet. In früheren Versionen des Betriebssystems befindet sich der Editor in den folgenden Ordnern:

  - `C:\Windows\notepad.exe`
  - `C:\Windows\System32\notepad.exe`
  - `C:\Windows\SysWOW64\notepad.exe`

Beim Hinzufügen des Editors zu einer Regel der Programmkontrolle können Sie z. B. den Programmnamen und den Datei-Hash aus den Eigenschaften des laufenden Programms angeben.

- Wenn die KSWS-Richtlinie in das KES-Richtlinienprofil migriert wird, benennt der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben (Migrations-Assistent) die Programmkategorien um, falls Kategorienamen unzulässige Zeichen enthalten: `'` `*` `<` `>` `?` `\` `:` `|`. Der Migrations-Assistent ersetzt diese Zeichen durch das Zeichen `_`. Beispiel: Die Programmkategorie `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` wird umbenannt in `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

Gerätekontrolle

- Kaspersky Endpoint Security kann Ereignisse beim Verbinden und Trennen externer Geräte protokollieren. Windows-Dienste verwenden das Systembenutzerkonto, um Geräte zu verbinden oder zu trennen. Darum lässt sich nicht feststellen, welcher Benutzer das Gerät verbindet oder trennt. Kaspersky Endpoint Security gibt das Benutzerkonto SYSTEM für das Ereignis an.

- Der Zugriff auf Druckergeräte, die der vertrauenswürdigen Liste hinzugefügt wurden, wird durch Geräte- und Bus-Blockierungsregeln blockiert.

- Bei MTP-Geräten wird die Steuerung von Lese-, Schreib- und Verbindungsvorgängen unterstützt, wenn Sie die integrierten Microsoft-Treiber des Betriebssystems verwenden. Wenn ein Benutzer einen benutzerdefinierten Treiber für die Arbeit mit einem Gerät installiert (z. B. als Teil von iTunes oder Android Debug Bridge), funktioniert die Kontrolle der Lese- und Schreibvorgänge möglicherweise nicht.

- Bei der Arbeit mit MTP-Geräten werden die Zugriffsregeln nach dem erneuten Anschließen des Geräts geändert.

- Die Komponente „Gerätekontrolle“ registriert Ereignisse im Zusammenhang mit überwachten Geräten, wie das Anschließen und Trennen eines Geräts, das Lesen einer Datei von einem Gerät, das Schreiben einer Datei auf ein Gerät und andere Ereignisse. Kaspersky Endpoint Security registriert Trennungsereignisse nur für die folgenden Gerätetypen: Tragbare Geräte (MTP), Wechseldatenträger, Disketten, CD/DVD-Laufwerke. Für andere Gerätetypen registriert die App keine Trennungsereignisse. Ein Vorgang, bei dem ein Gerät mit einem Computer verbunden wird, wird von der App für alle Gerätetypen registriert.

- Wenn Sie der Liste der vertrauenswürdigen Geräte auf der Grundlage einer Modellmaske ein Gerät hinzufügen und Zeichen verwenden, die in der ID, aber nicht im Modellnamen enthalten sind, werden diese Geräte nicht hinzugefügt. Auf einer Workstation werden diese Geräte auf der Grundlage einer ID-Maske zur Liste der vertrauenswürdigen Geräte hinzugefügt.

- Wenn die App ohne Computer-Neustart upgegradet wird, wendet die „Gerätekontrolle“ ihre Regeln nicht auf Geräte an, die neu verbunden werden. Für Geräte, die vor dem Upgrade verbunden wurden, werden die Regeln der „Gerätekontrolle“ allerdings wie vorgesehen angewendet. Starten Sie den Computer neu, damit die App auch mit neu verbundenen Geräten korrekt funktioniert.

- Wenn auf Computer, auf denen Kaspersky Endpoint Security Version 12.0 installiert ist, die Richtlinie von Kaspersky Endpoint Security Version 12.1 angewendet wird, hat der Druckerzugriffsmodus **Erlauben und nicht protokollieren** für den Gerätetyp **Netzwerkdrucker** die Bezeichnung **Von Verbindungsschnittstelle abhängig**. In diesen Modi führt die App die gleichen Aktionen aus. In Kaspersky Endpoint Security Version 12.1 hat der Zugriffsmodus für Netzwerkdrucker die korrekte Bezeichnung **Erlauben und nicht protokollieren**.

- Ab Kaspersky Endpoint Security 12.0 für Windows können im Programm Druckregeln für Drucker konfiguriert werden (Drucksteuerung). Nachdem die Anwendung mit Drucksteuerung installiert oder ein Upgrade auf die Anwendungsversion mit Drucksteuerung durchgeführt wurde, müssen Sie den Computer neu starten. Bis zum Neustart des Computers wendet Kaspersky Endpoint Security keine Druckregeln an und kann den Zugriff auf Drucker nur steuern. Wenn sich ein Neustart des Computers negativ auf die Arbeitsabläufe in Ihrem Unternehmen auswirkt, starten Sie einfach den spoolsv-Dienst (Druckwarteschlange) neu. Die Drucksteuerung wird auf Arm-basierten Computern nicht unterstützt.

- Ab Kaspersky Endpoint Security 12.0 für Windows unterstützt die Anwendung das WPA3-Protokoll für alle **WLAN**-Gerätetypen. Wenn auf einen Computer eine Richtlinie für Kaspersky Endpoint Security Version 12.2 angewendet wird, wird auf Computern mit Kaspersky Endpoint Security Version 11.11.0 und früher das Protokoll WPA2 ausgewählt; für die Versionen 12.0 bis 12.1 wird WPA2/WPA3 ausgewählt; für die Versionen 12.2 und höher wird WPA3 ausgewählt.

- Apple-Geräte werden als portable Geräte (MTP) und iTunes-Geräte klassifiziert. Möglicherweise identifiziert das Betriebssystem die Verbindung des Apple-Gerätes fehlerhaft und erkennt das Apple-Gerät nicht als portables Gerät (MTP). Darum ist das Apple-Gerät im Dateimanager nicht verfügbar, sondern nur in der iTunes-App erreichbar. Folglich kontrolliert Kaspersky Endpoint Security den Zugriff auf das Apple-Gerät nur in der iTunes-App. Um auf Ihr Apple-Gerät als tragbares Gerät (MTP) zugreifen zu können, müssen Sie zum Geräte-Manager gehen und den USB-Treiber für Apple-Mobilgeräte aus der Liste der USB-Controller entfernen. Nach dem Neustart des Computers wird das Apple-Gerät vom Betriebssystem als mobiles Gerät (MTP) und iTunes-Gerät identifiziert. Kaspersky Endpoint Security kontrolliert den Zugriff auf das Gerät sowohl über die iTunes-App als auch über den Dateimanager.

- In Kaspersky Endpoint Security 12.3 für Windows gibt es unterschiedliche Zugriffseinstellungen für den Gerätetyp **Bluetooth**. Wenn Sie in der vorherigen Version des Programms den Wert **Von Verbindungsschnittstelle abhängig** angegeben haben, ändert sich dieser Wert nach dem Programm-Upgrade auf Version 12.3 in **Erlauben und nicht protokollieren**. Das Verhalten des Geräts ändert sich dadurch nicht.

- Die „Gerätekontrolle“ unterstützt Bluetooth-Geräte nur über den Bluetooth-Stack von Microsoft Windows. Bei Bluetooth-Stacks von Drittanbietern funktioniert die „Gerätekontrolle“ möglicherweise fehlerhaft.

- Wenn das Bluetooth-Gerät seine Geräteklasse (COD) verbirgt oder fälscht, funktioniert die „Gerätekontrolle“ möglicherweise fehlerhaft.

- Auf Computern mit Windows 7 oder Windows 8 mit bestimmten Realtek-Bluetooth-Dongle-Treibern ist es eventuell nicht möglich, die Verbindung von Bluetooth-Geräten nur als Eingabegeräte (HID-Klasse) zuzulassen. Das heißt, wenn Sie den Zugriff auf Bluetooth-Geräte in den App-Einstellungen verbieten und Eingabegeräte zu den Ausnahmen hinzufügen, verhindert die Gerätekontrolle stattdessen möglicherweise den Zugriff auf alle Bluetooth-Geräte.

Web-Kontrolle

- Die Formate OGV und WEBM werden nicht unterstützt.

- Das RTMP-Protokoll wird nicht unterstützt.

- Die Web-Kontrolle unterstützt nur WSL1. WSL2-Datenverkehr wird vom Programm nicht kontrolliert.

Adaptive Kontrolle von Anomalien

- Es wird empfohlen, Ausnahmen automatisch auf der Grundlage des Ereignisses zu erstellen. Wenn Sie eine Ausnahme manuell hinzufügen, fügen Sie bei der Angabe des Zielobjekts das Zeichen `*` am Anfang des Pfades ein.

- Der **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“** kann nicht erstellt werden, wenn die Stichprobe auch nur ein Ereignis enthält, dessen Name mehr als 260 Zeichen enthält.

- Aus dem Abschnitt „Auslösen von Regeln“ der Datenverwaltung der Komponente „Adaptive Kontrolle von Anomalien“ können keine Ausnahmen hinzugefügt werden, wenn ein Objekt oder ein Prozess einen Wert hat, der aus über 256 Zeichen besteht (z. B. Pfad des Zielobjekts). Sie können eine Ausnahme manuell in den Richtlinieneinstellungen hinzufügen. Sie können eine Ausnahme auch im Bericht über die ausgelösten Regeln der Komponente „Adaptive Kontrolle von Anomalien“ hinzufügen.

- Kaspersky Security Center 15.1 kann keinen detaillierten **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“** für eine bestimmte Regel generieren.

- Regeln für die adaptive Kontrolle von Anomalien sind nur in der Sprache verfügbar, in der das Web-Plug-in installiert wurde. Wenn Sie die Sprache der Benutzeroberfläche ändern, zeigt Web Console eine leere Liste mit Regeln an. Um auf die Regeln zuzugreifen, ändern Sie die Sprache der Benutzeroberfläche wieder auf die Sprache, in der das Web-Plug-in installiert wurde.

Festplattenverschlüsselung (FDE)

- Die Kaspersky-Festplattenverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

- Die BitLocker-Laufwerkverschlüsselung wird auf Computern, auf denen Windows Home ausgeführt wird, nicht unterstützt.

- Bei der BitLocker-Laufwerkverschlüsselung kann der Benutzer das Authentifizierungskennwort mithilfe der Windows-API manuell ändern. In solchen Fällen ignoriert BitLocker die in der Richtlinie von Kaspersky Endpoint Security festgelegten Kennwortanforderungen. Mit anderen Worten: Der Benutzer kann ein beliebiges Kennwort festlegen.

- Nach der Installation des Programms müssen Sie das Betriebssystem neu starten, damit die Festplattenverschlüsselung ordnungsgemäß funktioniert.

- Der Authentifizierungsagent unterstützt keine Hieroglyphen oder die Sonderzeichen `|` und `\`.

- Damit der Computer nach der Verschlüsselung optimal funktioniert, muss der Prozessor den Befehlssatz AES-NI (Intel Advanced Encryption Standard New Instructions) unterstützen. Wenn der Prozessor den Befehlssatz AES-NI nicht unterstützt, kann die Leistung des Computers sinken.

- Wenn es Prozesse gibt, die versuchen, auf verschlüsselte Geräte zuzugreifen, bevor das Programm den Zugriff auf diese Geräte gewährt hat, zeigt das Programm eine Warnung an, die besagt, dass diese Prozesse beendet werden müssen. Wenn die Prozesse nicht beendet werden können, schließen Sie die verschlüsselten Geräte wieder an.

- Die eindeutigen IDs von Festplattenlaufwerken werden in der Geräteverschlüsselungsstatistik in invertiertem Format angezeigt.

- Es wird nicht empfohlen, Geräte zu formatieren, während sie verschlüsselt werden.

- Wenn mehrere Wechseldatenträger gleichzeitig an einem Computer angeschlossen sind, kann die Verschlüsselungsrichtlinie nur auf einen einzigen Wechseldatenträger angewendet werden. Wenn die Wechseldatenträger wieder angeschlossen werden, wird die Verschlüsselungsrichtlinie korrekt angewendet.

- Auf einer stark fragmentierten Festplatte kann die Verschlüsselung möglicherweise nicht starten. Defragmentieren Sie die Festplatte.

- Wenn Festplatten verschlüsselt werden, wird der Ruhezustand ab dem Zeitpunkt des Beginns der Verschlüsselungsaufgabe bis zum ersten Neustart eines Computers mit Microsoft Windows 7/8/8.1/10 und nach der Installation der Festplattenverschlüsselung bis zum ersten Neustart von Microsoft Windows 8/8.1/10 Betriebssystemen blockiert. Wenn Festplatten entschlüsselt werden, wird der Ruhezustand ab dem Zeitpunkt, an dem das Startlaufwerk vollständig entschlüsselt ist, bis zum ersten Neustart des Betriebssystems blockiert. Wenn die Schnellstart-Option in Microsoft Windows 8/8.1/10 aktiviert ist, können Sie das Betriebssystem nicht herunterfahren, da der Ruhezustand blockiert ist.

- Computer mit Windows 7 können das Kennwort während der Wiederherstellung nicht ändern, wenn das Laufwerk mit der BitLocker-Technologie verschlüsselt ist. Nachdem der Wiederherstellungsschlüssel eingegeben wurde und das Betriebssystem geladen ist, fordert Kaspersky Endpoint Security den Benutzer nicht auf, das Kennwort oder den PIN-Code zu ändern. Daher ist es nicht möglich, ein neues Passwort oder einen neuen PIN-Code festzulegen. Dieses Problem beruht auf Besonderheiten des Betriebssystems. Um fortzufahren, müssen Sie die Festplatte neu verschlüsseln.

- Es wird nicht empfohlen, das Tool xbootmgr.exe mit aktivierten zusätzlichen Providern zu verwenden. Zum Beispiel Dispatcher, Netzwerk oder Treiber.

- Die Formatierung eines verschlüsselten Wechseldatenträgers wird auf einem Computer, auf dem Kaspersky Endpoint Security für Windows installiert ist, nicht unterstützt.

- Die Formatierung eines verschlüsselten Wechseldatenträgers mit dem FAT32-Dateisystem wird nicht unterstützt (das Laufwerk wird als verschlüsselt angezeigt). Um ein Laufwerk zu formatieren, formatieren Sie es in das NTFS-Dateisystem um.

- Mehrere Download-Agenten können nicht nebeneinander auf einem verschlüsselten Computer existieren.

- Der Versuch, das Image eines bootfähigen GPT-Datenträgers im unverschlüsselten Zustand wiederherzustellen, kann zur Funktionsunfähigkeit des Betriebssystems führen. Um dies zu vermeiden, gehen Sie wie folgt vor:

  - Entschlüsseln Sie die Festplatte vollständig, bevor Sie das Image aus dem Backup wiederherstellen.

  - Verwenden Sie das sektorweise Kopieren, wenn Sie das Image erstellen.

  - Löschen Sie die Daten aus den ersten Sektoren des verschlüsselten Datenträgers, bevor Sie das Image wiederherstellen, und initialisieren Sie den Datenträger erneut.

- Es ist unmöglich, auf einen Wechseldatenträger zuzugreifen, der zuvor auf einem anderen Computer verschlüsselt wurde, wenn alle der folgenden Bedingungen gleichzeitig erfüllt sind:

  - Es besteht keine Verbindung zum Server des Kaspersky Security Center.

  - Der Benutzer versucht, sich mit einem neuen Token oder Kennwort zu autorisieren.

  Wenn eine ähnliche Situation eintritt, starten Sie den Computer neu. Nachdem der Computer neu gestartet wurde, wird der Zugriff auf den verschlüsselten Wechseldatenträger gewährt.

- Die Erkennung von USB-Geräten durch den Authentifizierungsagenten wird möglicherweise nicht unterstützt, wenn der xHCI-Modus für USB in den BIOS-Einstellungen aktiviert ist.

- Kaspersky Disk Encryption (FDE) für den SSD-Teil eines Geräts, der für die Zwischenspeicherung der am häufigsten verwendeten Daten verwendet wird, wird für SSHD-Geräte nicht unterstützt.

- Die Verschlüsselung von Festplatten in 32-Bit-Microsoft Windows 8/8.1/10-Betriebssystemen, die im UEFI-Modus laufen, wird nicht unterstützt.

- Starten Sie den Computer neu, bevor Sie eine entschlüsselte Festplatte erneut verschlüsseln.

- Die Festplattenverschlüsselung ist nicht kompatibel mit Kaspersky Anti-Virus für UEFI. Es wird nicht empfohlen, Festplattenverschlüsselung auf Computern zu verwenden, auf denen Kaspersky Anti-Virus für UEFI installiert ist.

- Das Erstellen von Authentifizierungsagent-Konten auf der Grundlage von Microsoft-Konten wird mit den folgenden Einschränkungen unterstützt:

  - Die Single-Sign-On-Technologie wird nicht unterstützt.

  - Die automatische Erstellung von Authentifizierungsagent-Konten wird nicht unterstützt, wenn die Option zur Erstellung von Konten für Benutzer, die sich in den letzten n Tagen am System angemeldet haben, ausgewählt wurde.

- Wenn der Name eines Authentifizierungsagent-Kontos im Format `<Domäne>/<Windows-Kontoname>` vorliegt, müssen Sie nach der Änderung des Computernamens auch die Namen von Konten ändern, die für lokale Benutzer dieses Computers erstellt wurden. Stellen Sie sich zum Beispiel vor, es gibt einen lokalen Benutzer `Ivanov` auf dem `Ivanov-Computer`, und für diesen Benutzer wurde ein Authentifizierungsagent-Konto mit dem Namen `Ivanov/Ivanov` erstellt. Wenn der Computername `Ivanov` in `Ivanov-PC` geändert wurde, müssen Sie den Namen des Authentifizierungsagent-Kontos für den Benutzer `Ivanov` von `Ivanov/Ivanov` in `Ivanov-PC/Ivanov` ändern. Sie können den Kontonamen ändern, indem Sie die Verwaltungsaufgabe für lokale Konten des Authentifizierungsagenten verwenden. Bevor der Name des Kontos geändert wurde, ist die Authentifizierung in der Pre-Boot-Umgebung mit dem alten Namen möglich (z. B. `Ivanov/Ivanov`).

- Wenn ein Benutzer nur mit einem Token auf einen Computer zugreifen darf, der mit der Kaspersky Disk Encryption-Technologie verschlüsselt wurde, und dieser Benutzer das Verfahren zur Wiederherstellung des Zugriffs abschließen muss, stellen Sie sicher, dass diesem Benutzer nach der Wiederherstellung des Zugriffs auf den verschlüsselten Computer kennwortbasierter Zugriff auf diesen Computer gewährt wird. Das Kennwort, das der Benutzer bei der Wiederherstellung des Zugriffs festgelegt hat, wird möglicherweise nicht gespeichert. In diesem Fall muss der Benutzer das Verfahren zur Wiederherstellung des Zugriffs auf den verschlüsselten Computer beim nächsten Neustart des Computers erneut durchführen.

- Beim Entschlüsseln einer Festplatte mit dem FDE Recovery Tool kann der Entschlüsselungsprozess mit einem Fehler enden, wenn Daten auf dem Quellgerät mit den entschlüsselten Daten überschrieben werden. Ein Teil der Daten auf der Festplatte bleibt verschlüsselt. Es wird empfohlen, die Option zum Speichern entschlüsselter Daten in eine Datei in den Geräteentschlüsselungseinstellungen zu wählen, wenn das FDE-Wiederherstellungs-Tool verwendet wird.

- Wenn das Kennwort des Authentifizierungsagenten geändert wurde, erscheint eine Nachricht mit dem Text *Ihr Kennwort wurde erfolgreich geändert. Klicken Sie auf OK* erscheint und der Benutzer startet den Computer neu. Das neue Kennwort wird nicht gespeichert. Das alte Kennwort muss für die nachfolgende Authentifizierung in der Pre-Boot-Umgebung verwendet werden.

- Die Festplattenverschlüsselung ist mit der Intel Rapid Start-Technologie inkompatibel.

- Die Festplattenverschlüsselung ist mit der ExpressCache-Technologie nicht kompatibel.

- In einigen Fällen erkennt das Tool beim Versuch, ein verschlüsseltes Laufwerk mit dem FDE Recovery Tool zu entschlüsseln, fälschlicherweise den Gerätestatus als „unverschlüsselt“, nachdem das „Anfrage-Antwort“-Verfahren abgeschlossen ist. Das Protokoll des Tools zeigt ein Ereignis, das besagt, dass das Gerät erfolgreich entschlüsselt wurde. In diesem Fall müssen Sie das Datenwiederherstellungsverfahren neu starten, um das Gerät zu entschlüsseln.

- Nachdem das Plug-In von Kaspersky Endpoint Security für Windows in der Web Console aktualisiert wurde, zeigen die Eigenschaften des Client-Computers den BitLocker-Wiederherstellungsschlüssel erst nach dem Neustart des Web Console-Dienstes an.

- Weitere Informationen zu den anderen Einschränkungen der Unterstützung der vollen Festplattenverschlüsselung und eine Liste der Geräte, für die die Festplattenverschlüsselung mit Einschränkungen unterstützt wird, finden Sie in der Wissensdatenbank des Technischen Supports.

Verschlüsselung von Dateien (File Level Encryption, FLE).

- Die Dateiverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.
- Die Datei- und Ordnerverschlüsselung wird auf Microsoft Windows Embedded-Betriebssystemen nicht unterstützt.
- Nachdem Sie die Anwendung installiert haben, müssen Sie das Betriebssystem neu starten, damit die Datei- und Ordnerverschlüsselung ordnungsgemäß funktioniert.
- Die Anwendung unterstützt die Dateiverschlüsselung nur auf Geräten mit NTFS- und FAT32-Dateisystem. Wenn eine verschlüsselte Datei auf ein Gerät mit einem nicht unterstützten Dateisystem übertragen wird (z. B. exFAT), wird die Datei auf diesem Gerät nicht verschlüsselt und kann verändert werden.
- Wenn eine verschlüsselte Datei auf einem Computer gespeichert ist, der über eine verfügbare Verschlüsselungsfunktion verfügt, und Sie auf die Datei von einem Computer zugreifen, auf dem keine Verschlüsselung verfügbar ist, wird ein direkter Zugriff auf diese Datei ermöglicht. Eine verschlüsselte Datei, die in einem Netzwerkordner auf einem Computer gespeichert ist, der über eine verfügbare Verschlüsselungsfunktion verfügt, wird in entschlüsselter Form auf einen Computer kopiert, der nicht über eine verfügbare Verschlüsselungsfunktion verfügt.
- Es wird empfohlen, Dateien zu entschlüsseln, die mit Encrypting File System verschlüsselt wurden, bevor Sie Dateien mit Kaspersky Endpoint Security für Windows verschlüsseln.
- Nachdem eine Datei verschlüsselt wurde, erhöht sich ihre Größe um 4 KB.
- Nachdem eine Datei verschlüsselt wurde, wird das Attribut *Archiv* in den Dateieigenschaften gesetzt.
- Wird die entschlüsselte Datei beispielsweise auf einen Wechseldatenträger kopiert, bleibt die Datei möglicherweise verschlüsselt. Dies kann folgenden Grund haben: Der Dateimanager (z. B. explorer.exe) versucht, auf die verschlüsselte Datei zuzugreifen, und speichert den Datei-Hash in einer speziellen Liste des Prozesses. Wenn der Dateimanager nach der Entschlüsselung der Datei versucht, auf die Datei zuzugreifen, sucht der Prozess in der Liste nach dem Datei-Hash. Wird der Hash gefunden, belässt Kaspersky Endpoint Security die Datei in verschlüsseltem Zustand. Um dies zu vermeiden, müssen Sie die Liste der Prozesse löschen. Das Betriebssystem löscht die Liste der Prozesse automatisch, wenn sie voll ist. Sie können die Liste auch manuell löschen. Dazu können Sie den Computer neu starten, den Prozess, mit dem Sie auf die Datei zugreifen (z. B. explorer.exe) neu starten oder einen anderen Dateimanager verwenden, den Sie noch nicht für den Zugriff auf die verschlüsselte Datei verwendet haben.
- Wenn eine aus einem verschlüsselten Archiv entpackte Datei den gleichen Namen hat wie eine bereits auf Ihrem Computer vorhandene Datei, so wird letztere durch die neue, aus dem verschlüsselten Archiv entpackte Datei überschrieben. Der Benutzer wird nicht über den Überschreibvorgang benachrichtigt.
- Bevor Sie ein verschlüsseltes Archiv entpacken, stellen Sie sicher, dass genügend freier Speicherplatz zum Entpacken der Dateien vorhanden ist. Sollte der Speicherplatz nicht ausreichen, wird das Entpacken des Archivs möglicherweise abgeschlossen, die Dateien können jedoch beschädigt sein. In diesem Fall zeigt Kaspersky Endpoint Security möglicherweise keine Fehlermeldungen an.
- Die Schnittstelle des portablen Dateimanagers zeigt keine Meldungen über Fehler an, die während seines Betriebs auftreten.
- Kaspersky Endpoint Security für Windows startet den portablen Dateimanager nicht auf einem Computer, auf dem die Komponente „Dateien verschlüsseln“ installiert ist.

- Sie können mit dem portablen Dateimanager nicht auf einen Wechseldatenträger zugreifen, wenn die folgenden Bedingungen gleichzeitig zutreffen:
  - Es besteht keine Verbindung zu Kaspersky Security Center.
  - Kaspersky Endpoint Security für Windows ist auf dem Computer installiert.
  - Auf dem Computer ist keine Datenverschlüsselung (FDE oder FLE) erfolgt.

  Der Zugriff ist auch dann nicht möglich, wenn Sie das Kennwort für den portablen Dateimanager kennen.
- Wenn die Dateiverschlüsselung verwendet wird, ist das Programm nicht mit dem Mail-Client Sylpheed kompatibel.
- Kaspersky Endpoint Security für Windows unterstützt die Regeln zur Zugriffsbeschränkung auf verschlüsselte Dateien für einige Apps nicht. Das liegt daran, dass einige Dateivorgänge durch Drittanbieter-Programme ausgeführt werden. Beispielsweise wird das Kopieren von Dateien durch den Dateimanager ausgeführt, nicht durch die App. Falls dem E-Mail-Client Outlook der Zugriff auf verschlüsselte Dateien verweigert wird, ermöglicht Kaspersky Endpoint Security dem E-Mail-Client auf diese Weise den Zugriff auf die verschlüsselte Datei, wenn der Benutzer Dateien über die Zwischenablage oder mit Drag-and-Drag-Funktion in die E-Mail-Nachricht kopiert hat. Der Kopiervorgang wurde von einem Dateimanager durchgeführt, für den keine Regeln zur Einschränkung des Zugriffs auf verschlüsselte Dateien festgelegt sind, d. h. der Zugriff ist erlaubt.
- Wenn Wechseldatenträger mit Unterstützung des portablen Modus verschlüsselt sind, kann die Kontrolle des Alters des Kennworts nicht deaktiviert werden.
- Das Ändern der Seitendatei-Einstellungen wird nicht unterstützt. Das Betriebssystem verwendet die Standardwerte anstelle der angegebenen Parameterwerte.
- Verwenden Sie das sichere Entfernen, wenn Sie mit verschlüsselten Wechseldatenträgern arbeiten. Wir können die Datenintegrität nicht garantieren, wenn der Wechseldatenträger nicht sicher entfernt wird.
- Nachdem die Dateien verschlüsselt wurden, werden ihre unverschlüsselten Originale sicher gelöscht.
- Die Synchronisierung von Offline-Dateien mithilfe von Client-Side Caching (CSC) wird nicht unterstützt. Die Verschlüsselung von Offline-Dateien und die Branch Caching-Technologie über SMB für Server werden ebenfalls nicht unterstützt. Es wird empfohlen, die Offline-Verwaltung von gemeinsam genutzten Ressourcen auf der Ebene der Gruppenrichtlinien zu verbieten. Dateien, die sich im Offline-Modus befinden, können bearbeitet werden. Nach der Synchronisierung können an einer Offline-Datei vorgenommene Änderungen verloren gehen.
- Die Erstellung eines verschlüsselten Archivs im Stammverzeichnis der Systemfestplatte wird nicht unterstützt.
- Beim Zugriff auf verschlüsselte Dateien über das Netzwerk können Probleme auftreten. Es wird empfohlen, die Dateien in eine andere Quelle zu verschieben oder sicherzustellen, dass der Computer, der als Dateiserver verwendet wird, vom gleichen Kaspersky Security Center-Administrationsserver verwaltet wird.
- Eine Änderung des Tastaturlayouts kann dazu führen, dass das Kennworteingabefenster für ein verschlüsseltes selbstextrahierendes Archiv hängen bleibt. Um dieses Problem zu beheben, schließen Sie das Kennworteingabefenster, ändern Sie das Tastaturlayout in Ihrem Betriebssystem und geben Sie das Kennwort für das verschlüsselte Archiv erneut ein.
- Wenn die Dateiverschlüsselung auf Systemen mit mehreren Partitionen auf einer Festplatte verwendet wird, empfiehlt es sich, die Option zu verwenden, die automatisch die Größe der pagefile.sys-Datei bestimmt. Nach dem Neustart des Computers kann sich die pagefile.sys-Datei zwischen den Festplattenpartitionen bewegen.

- Stellen Sie nach dem Anwenden der Dateiverschlüsselungsregeln, einschließlich der Dateien im Ordner *Eigene Dateien*, sicher, dass Benutzer, für die die Verschlüsselung angewendet wurde, auf verschlüsselte Dateien zugreifen können. Dazu muss sich jeder Benutzer beim System anmelden, wenn eine Verbindung zum Kaspersky Security Center verfügbar ist. Wenn ein Benutzer versucht, auf verschlüsselte Dateien zuzugreifen, ohne eine Verbindung zum Kaspersky Security Center zu haben, kann das System hängen.

- Wenn Systemdateien irgendwie in den Geltungsbereich der Verschlüsselung auf Dateiebene einbezogen sind, können Ereignisse bezüglich Fehlern beim Verschlüsseln dieser Dateien in Berichten erscheinen. Die in diesen Ereignissen angegebenen Dateien sind nicht wirklich verschlüsselt.

- Pico-Prozesse werden nicht unterstützt.

- Groß-/Kleinschreibung von Pfaden wird nicht unterstützt. Wenn Verschlüsselungsregeln oder Entschlüsselungsregeln angewendet werden, werden die Pfade in Produktereignissen in Kleinbuchstaben angezeigt.

- Es wird nicht empfohlen, Dateien zu verschlüsseln, die vom System beim Systemstart verwendet werden. Wenn diese Dateien verschlüsselt sind, kann der Versuch, auf verschlüsselte Dateien ohne Verbindung zum Kaspersky Security Center zuzugreifen, zum Hängen des Systems oder zu Aufforderungen zum Zugriff auf unverschlüsselte Dateien führen.

- Wenn Benutzer gemeinsam mit einer Datei über das Netzwerk unter FLE-Regeln über Programme, die die Datei-zu-Speicher-Zuordnungsmethode verwenden (wie WordPad oder FAR), und Programme, die für die Arbeit mit großen Dateien ausgelegt sind (wie Notepad ++), arbeiten, kann die Datei in unverschlüsselter Form auf unbestimmte Zeit blockiert werden, ohne die Möglichkeit, von dem Computer, auf dem sie sich befindet, darauf zuzugreifen.

- Dateien, die sich im OneDrive-Cloud-Speicher oder in anderen Ordnern mit dem Namen OneDrive befinden, werden von Kaspersky Endpoint Security nicht verschlüsselt. Außerdem blockiert Kaspersky Endpoint Security das Kopieren verschlüsselter Dateien in OneDrive-Ordner, wenn diese Dateien nicht zu einer Entschlüsselungsregel hinzugefügt wurden.

- Wenn die Verschlüsselungskomponente auf Dateiebene installiert ist, funktioniert die Verwaltung von Benutzern und Gruppen nicht im WSL-Modus (Windows-Subsystem für Linux).

- Wenn die Verschlüsselungskomponente auf Dateiebene installiert ist, wird POSIX (Portable Operating System Interface) zum Umbenennen und Löschen von Dateien nicht unterstützt.

- Es wird nicht empfohlen, temporäre Dateien zu verschlüsseln, da dies zu Datenverlust führen kann. Beispielsweise erstellt Microsoft Word beim Verarbeiten eines Dokuments temporäre Dateien. Wenn temporäre Dateien verschlüsselt sind, die Originaldatei jedoch nicht, erhält der Benutzer möglicherweise den Fehler *Zugriff abgelehnt* beim Versuch, das Dokument zu speichern. Außerdem kann es vorkommen, dass Microsoft Word die Datei speichert, aber das Dokument beim nächsten Mal nicht mehr geöffnet werden kann, d.h. die Daten gehen verloren. Um Datenverlust zu vermeiden, müssen Sie den Ordner mit den temporären Datei von den Verschlüsselungsregeln ausschließen.

Detection and Response (EDR, NDR, MDR, XDR, Sandbox)

- Sie können ein Objekt nicht untersuchen, das aufgrund der Aufgabe *Datei in Quarantäne verschieben* in die Quarantäne verschoben wurde.

- Es ist nicht möglich, einen alternativen Datenstrom (ADS) mit einer Größe von mehr als 4 MB in die Quarantäne zu verschieben. Kaspersky Endpoint Security überspringt alle alternativen Datenströme mit dieser Größe, ohne den Benutzer zu benachrichtigen.

- Kaspersky Endpoint Security führt auf Netzlaufwerken keine *IOC-Untersuchung*-Aufgaben aus, wenn der Ordnerpfad in den Aufgabeneigenschaften mit einem Laufwerksbuchstaben beginnt. Für *IOC-Untersuchung*-Aufgaben auf Netzlaufwerken unterstützt Kaspersky Endpoint Security nur das UNC-Pfadformat. Beispiel: `\\server\shared_folder`.

- Um sicherzustellen, dass die Aufgabe *IOC-Untersuchung*, die EmailItem-Ausdrücke verwendet, ordnungsgemäß funktioniert, muss das Web-Plug-in von Kaspersky Endpoint Security auf die neueste Version aktualisiert werden.

- Auf Arm-basierten Computern unterstützt die Aufgabe *IOC-Untersuchung* nur E-Mail-Dateien von den folgenden E-Mail-Clients: 32-Bit- und 64-Bit-Versionen von Outlook 2016 und Outlook 2021, 2024 und 365 für Arm64.

- Der Import der Konfigurationsdatei eines Programms endet mit einem Fehler, wenn die Einstellung Integration mit Kaspersky Sandbox in der Konfigurationsdatei aktiviert ist. Deaktivieren Sie Kaspersky Sandbox vor dem Export der Programmeinstellungen. Führen Sie anschließend den Export-/Import-Vorgang aus. Aktivieren Sie Kaspersky Sandbox nach dem Import der Konfigurationsdatei.

- Beim Importieren einer Richtlinie aus einer KLP-Datei wird der Parameterwert, der die Annahme der Bedingungen der Vereinbarung zu Kaspersky Detection and Response Expert bestimmt, nicht übernommen. Infolgedessen führt Kaspersky Endpoint Security nach dem Import der Richtlinie die Funktionen des EDR-Agenten nicht aus. Damit der EDR-Agent funktioniert, öffnen Sie die Richtlinie, ändern Sie einen beliebigen Parameter und speichern Sie die Richtlinieneinstellungen.

- Wird während der Ausführung der Aufgabe *IOC-Untersuchung* ein Kompromittierungsindikator gefunden, so verschiebt die App die Datei nur anhand des Ausdrucks „FileItem“ in die Quarantäne. Das Verschieben einer Datei in die Quarantäne anhand anderer Ausdrücke wird nicht unterstützt.

- Das Web-Plug-in von Kaspersky Endpoint Security für Windows 11.7.0 oder höher ist erforderlich, um Alarm-Details zu verwalten. Alarm-Details sind für die Verwendung der Lösungen von Endpoint Detection and Response (EDR Optimum und EDR Expert) erforderlich. Alarm-Details sind nur in „Kaspersky Security Center Web Console“ und „Kaspersky Security Center Cloud Console“ verfügbar.

- Die Migration der Konfiguration [KES+KEA] zur Konfiguration [KES+built-in agent] wird möglicherweise mit einem Fehler bei der Deinstallation des Programms Kaspersky Endpoint Agent abgeschlossen. Der Fehler bei der Programm-Deinstallation wurde in der neuesten Version von Kaspersky Endpoint Agent behoben. Um Kaspersky Endpoint Agent zu entfernen, starten Sie den Computer neu und erstellen Sie eine Aufgabe zur Programm-Deinstallation.

- Die Konfiguration [KES+KEA+built-in agent] wird nicht unterstützt. Diese Konfiguration beeinträchtigt die Interaktion zwischen Anwendungen und der in Ihrem Unternehmen bereitgestellten Detection and Response-Lösung. Wenn Kaspersky Endpoint Agent und der integrierte Agent auf demselben Computer verwendet werden, werden zudem die Telemetriedaten möglicherweise dupliziert und die Belastung des Computers und des Netzwerks kann steigen. Stellen Sie nach der Migration zur Konfiguration [KES + built-in agent] sicher, dass Kaspersky Endpoint Agent von Ihrem Computer entfernt wurde. Wenn Kaspersky Endpoint Agent nach der Migration weiterhin ausgeführt wird, müssen Sie die App manuell deinstallieren (beispielsweise mit der Aufgabe *Remote-Deinstallation einer Anwendung*).

  Mithilfe des Installationsprogramms können Sie Kaspersky Endpoint Agent auf einem Computer bereitstellen, auf dem Kaspersky Endpoint Security und der integrierte Agent installiert sind. Kaspersky Endpoint Agent und der integrierte Agent können auch durch die Aufgabe *Auswahl der Programmkomponenten ändern* auf einem Computer installiert werden. Das Verhalten ist von den Versionen von Kaspersky Endpoint Security und Kaspersky Endpoint Agent abhängig.

- Wenn das Programm Warnungsdetails generiert, stellt es Informationen über die erkannte Bedrohung bereit, einschließlich der Hash-Werte geänderter Dateien. Kaspersky Endpoint Security berechnet den Hash der Datei, wenn es Warnungsdetails generiert. Beachten Sie: Der ursprüngliche Hash der Datei, der beim Generieren des Dateiänderungsereignisses berechnet wurde, möglicherweise nicht mit dem Hash übereinstimmt, der beim Generieren der Warnungsdetails berechnet wurde.

- Der integrierte Agent EDR (KATA) setzt die Netzwerkisolation eines Computers nach einem Computerneustart fort, selbst wenn die Isolationsdauer abgelaufen ist. Um die wiederholte Isolierung des Computers zu verhindern, müssen Sie die Netzwerkisolierung in der Konsole von Kaspersky Anti Targeted Attack Platform deaktivieren.

- Wir empfehlen, nach Abschluss der Netzwerkisolation ein App-Upgrade auszuführen. Nach dem Upgrade von Kaspersky Endpoint Security kann die Netzwerkisolation beendet werden.

- Integrierte Agenten für EDR (KATA), EDR Optimum und EDR Expert sind nicht miteinander kompatibel. Daher kann die Aktivierung des integrierten EDR Agent mit einer eigenständigen Lizenz für das Add-on von Kaspersky Endpoint Detection and Response übersprungen werden, wenn Sie Kaspersky Endpoint Security mit einer anderen EDR-Funktionalität aktiviert haben. Beispielsweise wird die Aktivierung des integrierten EDR (KATA)-Agenten mit einer eigenständigen Lizenz übersprungen, wenn Sie Kaspersky Endpoint Security mit der [KES+EDR Optimum]-Lizenz aktiviert haben.

- In Kaspersky Endpoint Security Version 12.1 unterstützt der integrierte EDR (KATA)-Agent die folgenden Metadateien für die Aufgabe *NTFS-Metadateien abrufen* nicht: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA. Die Unterstützung für diese Metadateien wurde zu Kaspersky Endpoint Security Version 12.2 hinzugefügt.

- Wenn Sie die Migration von Kaspersky Endpoint Agent zu Kaspersky Endpoint Security für die Lösung Kaspersky Anti Targeted Attack Platform (EDR) ausführen, können beim Verbinden des Computers mit Central Node-Servern Fehler auftreten. Der Grund ist, dass der Migrations-Assistent in Web Console die folgenden Richtlinieneinstellungen überspringt und diese nicht migriert:

  - Verbot von Einstellungsänderungen **Verbindungseinstellungen** („Schloss“).

    Die Einstellungen können standardmäßig geändert werden (das „Schloss“ ist geöffnet). Die Einstellungen werden daher nicht auf dem Computer übernommen. Sie müssen Einstellungsänderungen verbieten und das „Schloss“ verriegeln.

  - Krypto-Container.

    Wenn Sie die Zwei-Wege-Authentifizierung zur Verbindung mit Central Node-Servern verwenden, müssen Sie den Krypto-Container erneut hinzufügen. Der Migrations-Assistent migriert das TLS-Zertifikat des Servers korrekt.

  Der Migrations-Assistent für Richtlinien und Aufgaben in der Verwaltungskonsole (MMC) migriert alle Einstellungen für die Lösung Kaspersky Anti Targeted Attack Platform (EDR).

- Der Aktivierungsstatus der App wird fehlerhaft angezeigt, wenn die App im Modus „Endpoint Detection and Response Agent“ installiert wurde, um die Lösung Kaspersky Managed Detection and Response ohne Verbindung zu Kaspersky Security Center zu unterstützen. Nach dem Download der BLOB-Datei wird im Infobereich der Windows-Taskleiste ein falscher Status angezeigt: *Das Programm ist nicht aktiviert*. Auf der Benutzeroberfläche der App wird der Aktivierungsstatus jedoch korrekt angezeigt. Starten Sie den Computer neu, damit die App korrekt funktioniert.

- Kaspersky Endpoint Security ermöglicht die Integration mit Kaspersky Anti Targeted Attack Platform mittels der Komponente „EDR (KATA)“ oder mittels Endpoint Sensor (nicht unterstützt). Beachten Sie, dass Sie für die Interaktion mit Kaspersky Anti Targeted Attack Platform nur eine der Komponenten verwenden können. Um den Status der Komponente anzuzeigen, öffnen Sie die Computereigenschaften in der Verwaltungskonsole (MMC) und öffnen Sie im Menü **Anwendungen** die Eigenschaften von Kaspersky Endpoint Security für Windows. Wechseln Sie anschließend zum Abschnitt **Komponenten**. Für das Anzeigen des Komponentenstatus im Rahmen der Interaktion mit der Kaspersky Anti Targeted Attack Platform gelten folgende Besonderheiten:

  - Für das Verwaltungs-Plug-in bis einschließlich Version 12.0 zeigt die Anwendung den aktuellen Status von **Endpoint Sensor** an. In Kaspersky Endpoint Security bis einschließlich Version 12.0 ist die Komponente „EDR (KATA)“ nicht verfügbar. EDR (KATA) ist ab Version 12.1 verfügbar.

  - Beginnend ab Version 12.1 des Verwaltungs-Plug-ins zeigt die Anwendung den Gesamtstatus von **Endpoint Detection and Response (KATA)** an, was entweder der Status von Endpoint Sensor oder von EDR (KATA) sein kann. Das ist Abhängig von der Version der Anwendung, die auf dem Computer des Benutzers installiert ist, und von den verfügbaren Komponenten, die für die Interaktion mit Kaspersky Anti Targeted Attack Platform verwendet werden können.

- Beginnend mit Version 12.6 von Kaspersky Endpoint Security zeigt die Kaspersky Security Center Web Console Version bis einschließlich Version 14.2 den Namen der Komponente **Endpoint Detection and Response (KATA)** in den Computereigenschaften falsch an. Anstelle des Namens der Komponente **Endpoint Detection and Response (KATA)** zeigt die Anwendung den Namen der Komponente **Endpoint Detection and Response Expert (KATA EDR)** an. Um die Liste der Komponente anzuzeigen, öffnen Sie die Computereigenschaften in der Web Console und öffnen Sie im Menü **Anwendungen** die Eigenschaften von Kaspersky Endpoint Security für Windows. Wechseln Sie anschließend zum Abschnitt **Komponenten**. Beginnend mit Version 15.1 der Kaspersky Security Center Web Console zeigt die Anwendung den Namen der Komponente korrekt an.

- Beim Update des Verwaltungs-Plug-ins von Kaspersky Endpoint Detection and Response auf Version 15.3, das in den Web Console-Versionen 14.0 bis 14.2 installiert ist, werden die Warnungsdetails fehlerhaft angezeigt. Damit die Warnungsdetails korrekt funktionieren, starten Sie den Administrationsserver von Kaspersky Security Center neu.

- Das Verwaltungs-Plug-in von Kaspersky Endpoint Detection and Response Version 15.4 und höher unterstützt Kaspersky Security Center Version 14.0 nicht. Nach der Aktualisierung des Verwaltungs-Plug-ins werden die Warnungsdetails fehlerhaft angezeigt.

- Die Lösungen der Klasse Kaspersky Extended Detection and Response (XDR) Version 1.4 unterstützen das Web-Plug-in von Kaspersky Endpoint Security für Windows Version 12.12 oder höher nicht. Sie können entweder die aktuelle Version des Web-Plug-ins beibehalten oder die XDR-Lösung auf Version 2.0 oder höher aktualisieren.

- Kaspersky Endpoint Security sendet Objekte, die für die Arm-Architektur bestimmt sind, nicht an Kaspersky Sandbox.

- Kaspersky Endpoint Security unterstützt für EDR Expert (on-premises) bis zu 10.000 Filterregeln, mit denen Ereignisse ein- oder ausgeschlossen werden.

- Die Ereignisfilterregeln für EDR Expert (on-premises) werden aus der Richtlinie nicht an verwaltete Geräte übertragen, auf denen Kaspersky Endpoint Security Version 14.0 oder älter ausgeführt wird, falls die maximale Anzahl für gespeicherte Filterregeln überschritten wird. Die Anwendung zeigt eine entsprechende Warnung an.

- Kaspersky Endpoint Security für Windows der Versionen 12.11–14.1 unterstützt die folgenden Telemetrieereignisse von EDR Expert (On-Premises) nicht:

  - Änderung des LDAP-Attributs

  - GPO-Änderung

- Abweichende lokale SCCM-Konfiguration
- Änderung der SCCM-Konfiguration
- SCCM-Bereitstellungsaufgabe
- SMB-Verbindung geöffnet

Ab Version 14.2 unterstützt Kaspersky Endpoint Security alle diese Telemetrieereignisse von EDR Expert (On-Premises) mit Ausnahme von Änderung des LDAP-Attributs.

Andere Einschränkungen

- Windows-Betriebssysteme ab Version 11 24H2 unterstützen die Technologie UDP Receive Segment Coalescing Offload (URO). Diese Technologie ist standardmäßig aktiviert, wenn auf dem Computer eine kompatible Netzwerkkarte und kompatible Treiber installiert sind. Wenn URO auf dem Benutzercomputer deaktiviert wird, kann die Leistung des Programms erheblich sinken.
- Kaspersky Endpoint Security unterstützt das WSL-Subsystem (Windows-Subsystem für Linux) mit Einschränkungen:
  - WSL 1. Das Programm überwacht den Netzwerkverkehr und erkennt Bedrohungen über HTTP/HTTPS. Da Kaspersky Endpoint Security ein eigenes Zertifikat verwendet, um sichere HTTPS-Verbindungen zu untersuchen, wird der Betrieb einiger Drittanbieter-Programme möglicherweise unterbrochen.
  - WSL 2. Das Programm unterstützt WSL 2 nicht.
- Wenn im Programm Fehler auftreten oder das Programm hängen bleibt, kann sich das Programm automatisch neu starten. Treten bei der Ausführung des Programms wiederholt Fehler auf, aufgrund derer das Programm beendet wird, führt das Programm die folgenden Aktionen aus:
  1. Deaktivierung der Schutz- und Überwachungsfunktionen (die Verschlüsselungsfunktion bleibt aktiv).
  2. Benachrichtigung des Benutzers über die Deaktivierung der Funktionen.
  3. Versuch der Wiederherstellung der Funktionsfähigkeit nach Updates der Antiviren-Datenbanken und der Übernahme von Updates der Programm-Module.
- Webadressen, die der Liste der vertrauenswürdigen Adressen hinzugefügt werden, werden möglicherweise nicht korrekt verarbeitet.
- In der Konsole von Kaspersky Security Center können Sie eine Datei aus dem Ordner **Erweitert** → **Datenverwaltung** → **Aktive Bedrohungen** nicht auf der Festplatte speichern. Um die Datei speichern zu können, müssen Sie die infizierte Datei desinfizieren. Bei der Desinfektion speichert die App eine Kopie der Datei im Backup. Jetzt können Sie die Datei aus dem Ordner **Erweitert** → **Datenverwaltung** → **Backup** auf der Festplatte speichern.
- Die Vererbung von Einstellungen für die Datenübertragung an den Administrationsserver (**Allgemeine Einstellungen** → **Berichte und Speicher** → **Datenübertragung an den Administrationsserver**) unterscheidet sich von der Vererbung anderer Einstellungen. Wenn Sie in der Richtlinie das Ändern der Datenübertragungseinstellungen erlaubt haben (das „Schloss“ ist geöffnet), werden diese Einstellungen in den Eigenschaften des lokalen Computers in der Konsole auf die Standardwerte zurückgesetzt, falls sie nicht bereits definiert waren. Wenn diese Einstellungen bereits definiert waren, werden ihre Werte wiederhergestellt. Beim Löschen einer Richtlinie werden die Einstellungen auf die gleiche Weise vererbt. In diesen Fällen erbt die Richtlinie andere Einstellungen in den Eigenschaften des lokalen Computers.

- Kaspersky Endpoint Security überwacht den HTTP-Datenverkehr, der den Standards RFC 2616, RFC 7540, RFC 7541 und RFC 7301 entspricht. Wenn Kaspersky Endpoint Security ein anderes Übertragungsformat im HTTP-Datenverkehr erkennt, sperrt die Anwendung diese Verbindung, um einen Download von bösartigem Code aus dem Internet zu verhindern.

- Kaspersky Endpoint Security verhindert die Kommunikation über das QUIC-Protokoll. Browser verwenden das Standard-Transportprotokoll (TLS oder SSL) unabhängig davon, ob die QUIC-Unterstützung im Browser aktiviert ist oder nicht.

- TLS-Verbindungsfehler können auftreten, wenn Drittanbieter-Software die Libcurl-Bibliothek verwendet. Dies kann mit dem Kaspersky-Zertifikat zusammenhängen, das Kaspersky Endpoint Security verwendet, um verschlüsselte Verbindungen zu untersuchen. Um dieses Problem zu umgehen, können Sie die Zertifikatverifizierung für Drittanbieter-Software deaktivieren (nicht empfohlen) oder eine Kaspersky-Zertifizierungsstelle zum cURL-Zertifikatspeicher hinzufügen. Ausführliche Informationen finden Sie in der Kaspersky-Wissensdatenbank.

- Wenn Kaspersky Endpoint Security für Windows zum ersten Mal gestartet wird, kann es vorkommen, dass ein digital signiertes Programm vorübergehend in die falsche Gruppe verschoben wird. Der digital signierte Antrag wird später in die richtige Gruppe gestellt.

- Bei einer erneuten Untersuchung eines bösartigen Objekts, das durch Software von Drittanbietern blockiert wurde, wird der Benutzer nicht benachrichtigt, wenn die Bedrohung erneut erkannt wird. Das Ereignis des erneuten Bedrohungsfundes wird im Anwendungsbericht und im Bericht für Kaspersky Security Center angezeigt.

- Der Kaspersky Security Center-Bericht über die Geräteverschlüsselung enthält keine Informationen über Geräte, die mit Microsoft-BitLocker auf Serverplattformen oder auf Arbeitsstationen verschlüsselt wurden, auf denen die Komponente „Gerätekontrolle“ nicht installiert ist.

- Es ist nicht möglich, die Anzeige aller Berichtseinträge in der „Kaspersky Security Center Web Console“ zu aktivieren. In der „Web Console“ können Sie nur die Anzahl der Einträge ändern, die in Berichten angezeigt werden. „Kaspersky Security Center Web Console“ zeigt standardmäßig 1.000 Berichtseinträge an. Die Anzeige aller Berichtseinträge können Sie in der Verwaltungskonsole (MMC) aktivieren.

- Es ist nicht möglich, in der „Kaspersky Security Center Web Console“ die Anzeige von mehr als 1.000 Berichtseinträgen festzulegen. Wenn Sie einen höheren Wert als 1.000 angeben, zeigt die Kaspersky Security Center-Konsole nur 1.000 Berichtseinträge an.

- Bei Verwendung einer Richtlinienhierarchie sind die Einstellungen des Abschnitts „Verschlüsselung von Wechseldatenträgern“ in einer untergeordneten Richtlinie zur Bearbeitung zugänglich, wenn die übergeordnete Richtlinie die Änderung dieser Einstellungen verbietet.

- Sie müssen die Anmeldungsüberwachung in den Betriebssystemeinstellungen aktivieren, um das ordnungsgemäße Funktionieren der Ausnahmen für den Schutz von freigegebenen Ordnern vor externer Verschlüsselung zu gewährleisten.

- Wenn der Schutz gemeinsamer Ordner aktiviert ist, versucht Kaspersky Endpoint Security für Windows, gemeinsame Ordner für jede Remote-Zugriffssitzung zu verschlüsseln, die vor dem Start von Kaspersky Endpoint Security für Windows gestartet wurde, auch wenn der Computer, von dem die Remote-Zugriffssitzung gestartet wurde, zu den Ausnahmen hinzugefügt wurde. Wenn Sie nicht möchten, dass Kaspersky Endpoint Security für Windows Versuche zur Verschlüsselung von freigegebenen Ordnern für Remote-Zugriffssitzungen überwacht, die von einem Computer gestartet wurden, der zu den Ausnahmen hinzugefügt wurde und der vor dem Start von Kaspersky Endpoint Security für Windows gestartet wurde, beenden Sie die Remote-Zugriffssitzung und bauen Sie sie wieder auf oder starten Sie den Computer neu, auf dem Kaspersky Endpoint Security für Windows installiert ist.

- Wenn die Aktualisierungsaufgabe mit den Berechtigungen eines bestimmten Benutzerkontos ausgeführt wird, werden Produkt-Patches nicht heruntergeladen, sofern die Aktualisierung von einer Quelle erfolgt, die eine Autorisierung erfordert.

- Der Start des Programms kann aufgrund unzureichender Systemleistung fehlschlagen. Um dieses Problem zu beheben, verwenden Sie die Option Ready Boot oder erhöhen Sie die Zeitüberschreitung des Betriebssystems für den Start von Diensten.

- Das Programm kann im abgesicherten Modus von Windows nicht ausgeführt werden.

- Wir können nicht garantieren, dass die Audiosteuerung beim ersten Neustart nach der Installation des Programms funktioniert.

- In der Verwaltungskonsole (MMC) ist in den Einstellungen der „Programm-Überwachung“ im Konfigurationsfenster für die Anwendungsberechtigungen die Schaltfläche **Entfernen** nicht verfügbar. Verwenden Sie das Kontextmenü der Anwendung, wenn Sie eine Anwendung aus einer Sicherheitsgruppe entfernen möchten.

- In der lokalen Schnittstelle der Anwendung sind in den Einstellungen der „Programm-Überwachung“ die Anwendungsberechtigungen und geschützten Ressourcen nicht zur Anzeige verfügbar, wenn der Computer mit einer Richtlinie verwaltet wird. Bildlauffunktion, Suche, Filterung und andere Steuerungsfenster sind nicht verfügbar. Die Anwendungsberechtigungen können Sie in den Richtlinieneigenschaften in der Kaspersky Security Center-Konsole ansehen.

- Wenn rotierende Ablaufverfolgungsdateien aktiviert sind, werden keine Ablaufverfolgungen für die AMSI-Komponente und das Outlook-Plug-in erstellt.

- Leistungsspuren können in Windows Server 2008 nicht manuell erfasst werden.

- Leistungsspuren für den Spurentyp „Neustart“ werden nicht unterstützt.

- Die Dump-Protokollierung wird für Pico-Prozesse nicht unterstützt.

- Wenn Sie die Option **Externe Steuerung von Systemdiensten deaktivieren** deaktivieren, können Sie den Dienst des Programms, das mit dem Parameter `AMPPL=1` installiert wurde, nicht beenden (der Parameterwert steht ab Betriebssystemversion Windows 10RS2 standardmäßig auf `1`). Der Parameter `AMPPL` mit einem Wert von `1` ermöglicht die Verwendung der Schutzprozess-Technologie für den Produktservice.

- Um eine benutzerdefinierte Untersuchung eines Ordners auszuführen, muss der Benutzer, der die benutzerdefinierte Untersuchung startet, über die Berechtigungen zum Lesen der Attribute dieses Ordners verfügen. Andernfalls ist die Untersuchung des benutzerdefinierten Ordners nicht möglich und endet mit einem Fehler.

- Wenn eine in einer Richtlinie definierte Untersuchungsregel einen Pfad ohne das Zeichen `\` am Ende enthält (z. B. `C:\folder1\folder2`), wird die Untersuchung für den Pfad `C:\folder1\` ausgeführt.

- Wenn Sie Richtlinien zur Softwareeinschränkung (Softwareeinschränkungsrichtlinien, SRP) verwenden, kann der Computer möglicherweise nicht gestartet werden (schwarzer Bildschirm). Zur Vermeidung von Fehlfunktionen müssen Sie die Verwendung von Programmbibliotheken in den SRP-Eigenschaften zulassen. Fügen Sie in den SRP-Eigenschaften die Regel mit der Sicherheitsstufe **Unrestricted** für die Datei khkum.dll hinzu (Menüeintrag **Neue Hash-Regel**). Die Datei befindet sich im Ordner `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. Wenn Sie diese Methode ausgewählt haben, müssen Sie zusätzlich das Kontrollkästchen **Updates für Programm-Module herunterladen** deaktivieren, das sich in den Einstellungen der *Update*-Aufgabe für Kaspersky Endpoint Security befindet. Details zur Verwendung von SRP finden Sie in der Microsoft-Dokumentation.

  Sie können SRP auch deaktivieren und die Kaspersky Endpoint Security-Komponente Programmkontrolle verwenden, um die App-Nutzung zu steuern.

- Wenn der Computer zu einer Domäne gehört, für die ein Windows-Gruppenrichtlinienobjekt (Gruppenrichtlinienobjekt, GPO) gilt, und der Parameter DriverLoadPolicy den Wert 8 (Nur gut) hat, verursacht ein Neustart des Computers, auf dem Kaspersky Endpoint Security installiert ist, einen BSOD. Um einen Fehler zu verhindern, muss der Parameter Antischadsoftware für frühen Start (ELAM) in der Gruppenrichtlinie den Wert 1 (Gut und unbekannt) besitzen. ELAM-Einstellungen befinden sich in der Richtlinie unter: **Computer Configuration → Administrative Templates → System → Early Launch Antimalware**.

- Die Verwaltung von Outlook-Plug-in-Einstellungen über Rest API wird nicht unterstützt.

- Aufgabenablaufeinstellungen für einen bestimmten Benutzer können nicht über eine Konfigurationsdatei zwischen Geräten übertragen werden. Nachdem die Einstellungen aus einer Konfigurationsdatei übernommen wurden, geben Sie den Benutzernamen und das Kennwort manuell an.

- Nach der Installation eines Updates funktioniert die Aufgabe der Integritätsprüfung erst, wenn das System neu gestartet wird, um das Update anzuwenden.

- Wenn die rotierende Ablaufverfolgungsebene über das Ferndiagnose-Dienstprogramm geändert wird, zeigt Kaspersky Endpoint Security für Windows fälschlicherweise einen leeren Wert für die Ablaufverfolgungsebene an. Ablaufverfolgungsdateien werden jedoch entsprechend der korrekten Ablaufverfolgungsebene geschrieben. Wenn die rotierende Ablaufverfolgungsebene über die lokale Programmoberfläche geändert wird, wird die Ablaufverfolgungsebene korrekt geändert, aber das Ferndiagnose-Dienstprogramm zeigt fälschlicherweise die Ablaufverfolgungsebene an, die zuletzt vom Dienstprogramm definiert wurde. Dies kann dazu führen, dass der Administrator nicht über aktuelle Informationen für die aktuelle Ablaufverfolgungsebene verfügt und dass in den Protokollen relevante Informationen fehlen, wenn ein Benutzer die Ablaufverfolgungsebene manuell über die lokalen Programmoberfläche ändert.

- Auf der lokalen Benutzeroberfläche verhindern die Kennwortschutz-Einstellungen das Ändern des Namens des Administratorkontos (standardmäßig KLAdmin). Um den Namen des Administratorkontos zu ändern, müssen Sie den Kennwortschutz deaktivieren, dann den Kennwortschutz aktivieren und einen neuen Namen für das Administratorkonto angeben.

- Wenn Kaspersky Endpoint Security auf einem Server mit Windows Server 2019 installiert ist, ist die Anwendung inkompatibel mit Docker. Die Bereitstellung von Docker-Containern auf einem Computer mit Kaspersky Endpoint Security führt zu einem Absturz (BSOD).

- Wenn Kaspersky Endpoint Security auf einem Server des SQL Server-DBMS installiert ist, sendet das Programm Anfragen an die Instanz des Servers. Dies ist erforderlich, um die Aufträge des SQL Server-Agenten zu untersuchen und die Ausführung bösartiger Aufträge zu verhindern. Kaspersky Endpoint Security verwendet das SQL Server-Benutzerkonto, um Aufträge zu untersuchen. Das Programm sendet bei der Untersuchung des Systemspeichers und nach dem Update der Antiviren-Datenbanken Anfragen an den Server.

- Die Kompatibilität von Kaspersky Endpoint Security und Secret Net Studio ist eingeschränkt:

  - Die Anwendung Kaspersky Endpoint Security ist nicht mit der Antivirus-Komponente von Secret Net Studio kompatibel.

    Die Anwendung kann nicht auf einem Computer installiert werden, auf dem Secret Net Studio mit der Antivirus-Komponente bereitgestellt ist. Um die Interoperabilität zu ermöglichen, müssen Sie die Antivirus-Komponente aus Secret Net Studio entfernen.

  - Die Anwendung Kaspersky Endpoint Security ist nicht mit der Komponente für den Festplattenschutz und die vollständige Festplattenverschlüsselung von Secret Net Studio kompatibel.

    Die Anwendung kann nicht auf einem Computer installiert werden, auf dem Secret Net Studio mit der Komponente für den Festplattenschutz und die vollständige Festplattenverschlüsselung bereitgestellt ist. Um die Interoperabilität zu ermöglichen, müssen Sie die Komponente für den Festplattenschutz und die vollständige Festplattenverschlüsselung aus Secret Net Studio entfernen.

  - Secret Net Studio ist nicht mit der Kaspersky Endpoint Security-Komponente „Verschlüsselung von Dateien“ (FLE) kompatibel.

    Wenn Sie Kaspersky Endpoint Security mit der Komponente „Verschlüsselung von Dateien“ (FLE) installieren, funktioniert Secret Net Studio möglicherweise fehlerhaft. Um die Interoperabilität zu gewährleisten, müssen Sie die Komponente „Verschlüsselung von Dateien“ (FLE) aus Kaspersky Endpoint Security entfernen.

- Wenn Regeln für die Überwachung der Systemintegrität importiert werden, überprüft die App die ID und den Namen der Regel. Wenn die Regel-IDs identisch sind, ersetzt Kaspersky Endpoint Security die vorhandenen Regeln durch die neue Regel. Wenn Regeln exportiert werden, vergibt die App automatisch IDs. Regeln mit identischen IDs können beispielsweise vorkommen, wenn Sie exportierte XML-Dateien mit Regeln manuell bearbeitet haben. Sind die Regel-IDs einmalig, die Regelnamen sind jedoch identisch, fügt Kaspersky Endpoint Security dem Namen der Regel den Zusatz `(1)` und so weiter hinzu.

- Ab Kaspersky Endpoint Security für Windows Version 12.11 können die Einstellungen einer übergeordneten Richtlinie, die in einer untergeordneten Gruppe geöffnet ist, nicht mehr in der Web Console angezeigt werden. Zusätzlich zeigt die Web Console eine Warnung an: *Diese Richtlinie ist geerbt. Sie können ihre Einstellungen nur in der Administrationsgruppe bearbeiten, in der sie erstellt wurde*.

- Pop-up-Benachrichtigungen, die länger als 256 Zeichen sind, werden in der Verwaltungskonsole (MMC) nicht angezeigt.

- Die Komponenten können in der Richtlinie und im Installationspaket unterschiedliche Namen haben. Endpoint Detection and Response Expert (on-premises) kann beispielsweise die folgenden Namen haben: Endpoint Detection and Response (KATA), Endpoint Detection and Response Expert (on-premises) oder Kaspersky Anti Targeted Attack Platform Integration. Die Namen der Komponenten können sich auch je nach Programmversion unterscheiden.

Glossar

Administrationsagent

Programmkomponente von Kaspersky Security Center, welche für die Interaktion zwischen dem Administrationsserver und den Kaspersky-Programmen verantwortlich ist, die auf einem konkreten Netzwerkknoten (Workstation oder Server) installiert sind. Die vorliegende Komponente ist einheitlich für alle Programme von Kaspersky, die unter dem Betriebssystem Windows laufen. Für die Programme, die unter anderen Betriebssystemen laufen, sind spezielle Versionen des Administrationsagenten vorgesehen.

Administrationsgruppe

Eine Reihe von Geräten, die anhand der auszuführenden Funktionen und der auf ihnen installierten Kaspersky-Programme zusammengefasst wurden. Die Gruppierung dient zur vereinfachten Verwaltung der Geräte als geschlossene Einheit. Zu einer Gruppe können weitere Gruppen gehören. Für jede in der Gruppe installierte Anwendung können Gruppenrichtlinien angelegt und Gruppenaufgaben erstellt werden.

Aktiver Schlüssel

Schlüssel, der momentan für das Programm verwendet wird.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die Kaspersky im Moment der Veröffentlichung der Antiviren-Datenbanken bekannt sind. Die Einträge der Antiviren-Datenbanken ermöglichen es, bösartigen Code in untersuchten Objekten zu finden. Die Antiviren-Datenbanken werden von den Kaspersky-Spezialisten gepflegt und stündlich aktualisiert.

Archiv

Eine oder mehrere Dateien, die in komprimierter Form in eine Datei aufgenommen wurden. Für die Archivierung und zum Entpacken von Daten ist ein spezielles Archivierungsprogramm erforderlich.

Aufgabe

Funktionen, die die Kaspersky-App als Aufgaben ausführt, zum Beispiel: Echtzeitschutz für Dateien, Vollständige Untersuchung des Geräts und Datenbanken-Update.

Authentifizierungsagent

Schnittstelle, welche nach der Verschlüsselung einer bootfähigen Festplatte die Authentifizierung für den Zugriff auf verschlüsselte Festplatten und für das Laden des Betriebssystems ermöglicht.

Cloud Discovery

Cloud Discovery verwaltet den Benutzerzugriff auf Cloud-Dienste. Solche Cloud-Dienste sind beispielsweise Microsoft Teams, Salesforce und Microsoft Office 365. Cloud-Dienste sind in Kategorien angeordnet, z. B. *Filehosting-Anbieter*, *Messenger* und *E-Mail*.

Datenbank für bösartige 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 für 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

Situation, in der eine virenfreie Datei von der Kaspersky-Anwendung als infiziert eingestuft wird, da ihr Code Ähnlichkeit mit einem Virus aufweist.

Infizierte Datei

Datei, die schädlichen Code enthält (bei der Untersuchung der Datei wurde der Code eines bekannten bedrohlichen Programms gefunden). Die Kaspersky-Spezialisten warnen davor, mit solchen Dateien zu arbeiten, da dies zur Infektion Ihres Computers führen kann.

Integrationsserver

Die Komponente "Kaspersky Endpoint Security for Virtualization Light Agent". Realisiert die Interaktion zwischen den Komponenten von Kaspersky Endpoint Security und der virtuellen Infrastruktur.

IOC

Kompromittierungsindikator. Ein Datensatz, der sich auf ein schädliches Objekt oder eine schädliche Aktivität bezieht.

IOC-Datei

Eine Datei, die eine Reihe von Kompromittierungsindikatoren (IOCs) enthält, mit denen die Anwendung nach Übereinstimmungen sucht. Die Erkennungswahrscheinlichkeit kann sich erhöhen, wenn eine Untersuchung genaue Übereinstimmungen mit mehreren IOC-Dateien für das Objekt ergibt.

Kerberos-Authentifizierung

Methode zur gegenseitigen Authentifizierung von Client und Server, bevor eine Verbindung zur Kommunikation über unsichere Netzwerke hergestellt wird. Die Methode basiert auf einem Ticket, das der Benutzer von einem vertrauenswürdigen Authentifizierungszentrum erhält.

Light Agent

Die Komponente "Kaspersky Endpoint Security for Virtualization Light Agent". Wird auf jede virtuelle Maschine, die geschützt werden soll, installiert.

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.

Maske

Aus allgemeinen Zeichen bestehender Platzhalter für Dateinamen und -erweiterungen.

Zum Erstellen einer Dateimaske können alle für Dateinamen zulässigen Symbole einschließlich folgender Sonderzeichen verwendet werden:

- 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` funktioniert nicht. Die Maske ** ist nur für die Erstellung von Untersuchungsausnahmen verfügbar.

- 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.

Normalisierte Form der Adresse einer Webressource

Als normalisierte Form der Adresse einer Webressource gilt die Textdarstellung der Adresse einer Webressource, die durch eine Normalisierung erreicht wird. *Bei der Normalisierung wird die Textdarstellung einer Webadresse nach bestimmten Regeln verändert (z. B. Ausschluss von Benutzername, Kennwort und Verbindungsport aus der Textdarstellung der Webadresse, Umwandlung von in der Webadresse vorkommenden Großbuchstaben in Kleinbuchstaben).*

Im Kontext der Schutzkomponenten besteht das Ziel einer Normalisierung der Adressen von Webressourcen darin, syntaktisch unterschiedliche, physisch jedoch äquivalente Adressen von Webadressen nur einmal zu untersuchen.

Beispiel:
Nicht normalisierte Form einer Adresse: www.Example.com\.
Normalisierte Form einer Adresse: www.example.com.

OLE-Objekt

Datei, die an eine andere Datei angehängt oder darin eingebettet ist. Die Programme von Kaspersky gestatten es, OLE-Objekte auf Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel® in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

OpenIOC

Offener Standard für die Beschreibungen von Kompromittierungsindikatoren (IOC), auf XML basierend, mit über 500 verschiedenen Kompromittierungsindikatoren.

Portabler Dateimanager

Programm, das eine Schnittstelle für die Verwendung verschlüsselter Dateien auf Wechseldatenträgern bietet, wenn die Verschlüsselungsfunktionalität auf einem Computer nicht verfügbar ist.

Potenziell infizierbare Datei

Datei, die aufgrund ihrer Struktur oder ihres Formats von einem Angreifer als „Container“ benutzt werden kann, um Schadcode zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Für solche Dateien ist das Risiko, dass bösartiger Code eindringt, relativ hoch.

Schutzbereich

Objekte, die permanent von der Komponente für den Basisschutz untersucht werden. Der Schutzbereich besitzt je nach Komponente unterschiedliche Eigenschaften.

SVM

Eine Secure Virtual Machine (SVM) ist eine spezielle virtuelle Maschine, auf welcher der Dienst "scanserver" (Dienst des Schutzservers als Komponente von Kaspersky Security for Virtualization Light Agent) installiert ist.

Trusted Platform Module

Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten.

Untersuchungsbereich

Objekte, die im Rahmen einer Untersuchungsaufgabe von Kaspersky Endpoint Security untersucht werden.

Zertifikataussteller

Zertifizierungsstelle, die das Zertifikat ausgestellt hat

Anhänge

Die Informationen in diesem Abschnitt ergänzen den allgemeinen Text des Dokuments.

Anhang 1. Programmeinstellungen

Sie können eine Richtlinie, Aufgaben oder die Programmoberfläche verwenden, um Kaspersky Endpoint Security zu konfigurieren. Ausführliche Informationen über die Programmkomponenten finden Sie in den entsprechenden Unterabschnitten.

Schutz vor bedrohlichen Dateien

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.

Einstellungen der Komponente „Schutz vor bedrohlichen Dateien“

Einstellung	Beschreibung
Sicherheitsstufe *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Zum Schutz vor bedrohlichen Dateien kann Kaspersky Endpoint Security verschiedene Gruppen von Einstellungen (Einstellungssätze) anwenden. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Auf dieser Sicherheitsstufe für Dateien kontrolliert die Komponente „Schutz vor bedrohlichen Dateien“ alle Dateien, die geöffnet, gespeichert und gestartet werden, mit höchster Genauigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht alle Dateitypen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Untersucht werden außerdem Archive, Installationspakete und eingebettete OLE-Objekte. • **Empfohlen**. Diese Sicherheitsstufe für Dateien wird von Kaspersky-Experten empfohlen. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien bestimmter Formate auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht Archive oder Installationspakete nicht. • **Niedrig**. Diese Sicherheitsstufe für Dateien bietet eine maximale Untersuchungsgeschwindigkeit. Die Komponente „Schutz vor bedrohlichen Dateien“ untersucht nur Dateien mit bestimmten Erweiterungen auf allen Festplatten, Wechseldatenträgern und Netzlaufwerken des Computers. Zusammengesetzte Dateien werden von der Komponente „Schutz vor bedrohlichen Dateien“ nicht untersucht.

Einstellung	Beschreibung
Dateitypen *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	**Alle Dateien**. Bei Auswahl dieser Option untersucht Kaspersky Endpoint Security ausnahmslos alle Dateien (unabhängig von Format und Erweiterung). **Dateien nach Format untersuchen**. 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. **Dateien nach Erweiterung untersuchen**. Bei Auswahl dieser Option untersucht das Programm nur potenziell infizierbare Dateien. Das Dateiformat wird auf Basis der Dateierweiterung ermittelt.
Untersuchungsbereich	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.
Machine Learning und Signaturanalyse *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Bei der Untersuchungsmethode Maschinelles Lernen und Signaturanalyse werden die Datenbanken von Kaspersky Endpoint Security verwendet, die Beschreibungen bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten. Die Verwendung dieser Untersuchungsmethode gewährleistet die minimal zulässige Sicherheitsstufe. Aufgrund von Empfehlungen der Kaspersky-Experten ist die Untersuchungsmethode Maschinelles Lernen und Signaturanalyse immer aktiviert.
Heuristische Analyse *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Aktion beim Fund einer Bedrohung	**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**. Wenn diese Option ausgewählt ist, versucht das Programm automatisch, die gefundene infizierte Datei zu desinfizieren. Wenn die Desinfektion fehlschlägt, wird die Datei durch die Anwendung blockiert. **Blockieren**. Wenn diese Option ausgewählt ist, wird die infizierte Datei automatisch durch die Anwendung blockiert und es erfolgt kein Desinfektionsversuch. Bevor versucht wird, eine infizierte Datei zu desinfizieren oder zu löschen, erstellt das Programm eine Backup-Kopie der Datei für den Fall, dass Sie die Datei wiederherstellen müssen oder wenn sie in Zukunft desinfiziert werden kann.
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.
Archive untersuchen	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Programmpakete untersuchen	Verteilungspakete für Drittanbieter-Programme untersuchen.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Dateien in E-Mail-Formaten untersuchen	Untersucht Dateien im E-Mail-Format. Die App untersucht MSG- und EML-Dateien. E-Mail-Format-Dateien enthalten auch OLE-Objekte und MHT-Dateien. Dateien im E-Mail-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch Kaspersky Endpoint Security untersucht.

Einstellung	Beschreibung
Große zusammengesetzte Dateien nicht entpacken	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.
Zusammengesetzte Dateien im Hintergrund entpacken	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.
Untersuchungsmodus *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Kaspersky Endpoint Security untersucht Dateien, auf die der Benutzer, das Betriebssystem oder ein Programm, das unter dem Benutzerkonto des Benutzers läuft, zugreift. **Intelligenter Modus**. In diesem Untersuchungsmodus untersucht die „Schutz vor bedrohlichen Dateien"-Funktion ein Objekt auf Basis einer Analyse von Vorgängen, die mit ihm ausgeführt werden. Wird beispielsweise mit einem Microsoft-Office-Dokument gearbeitet, so untersucht Kaspersky Endpoint Security die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen. **Bei Zugriff und Veränderungen**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien" Objekte jedes Mal untersucht, wenn versucht wird, diese zu öffnen oder zu bearbeiten. **Bei Zugriff**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien" nur dann Objekte untersucht, wenn versucht wird, sie zu öffnen. **Bei Ausführung**. Untersuchungsmodus, in dem die Funktion „Schutz vor bedrohlichen Dateien" nur dann Objekte untersucht, wenn versucht wird, sie zu starten.
iSwift-Technologie verwenden *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iSwift ist eine Weiterentwicklung der iChecker-Technologie für das NTFS-Dateisystem.
iChecker-Technologie verwenden *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Eine Technologie, die eine Steigerung der Untersuchungsgeschwindigkeit erlaubt, indem bestimmte Dateien ausgeschlossen werden. Dateien werden nach einem speziellen Algorithmus von der Untersuchung ausgeschlossen. Dabei werden das Erscheinungsdatum der Datenbanken von Kaspersky Endpoint Security, das Datum der letzten Untersuchung einer Datei und Veränderungen der Untersuchungseinstellungen berücksichtigt. Die Technologie iChecker besitzt folgende Einschränkungen: Sie funktioniert nicht mit umfangreichen Dateien und kann nur auf Dateien angewendet werden, deren Struktur dem Programm bekannt ist (z. B. auf Dateien der Formate EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

Einstellung	Beschreibung
Schutz vor bedrohlichen Dateien anhalten *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Diese Option hält die Ausführung der Funktion „Schutz vor bedrohlichen Dateien“ zu den angegebenen Zeiten oder beim Start der angegebenen Programme vorübergehend automatisch an.
Untersuchung von Dateivorgängen, die in Windows-Containern ausgeführt werden	Wenn in einem Container eine Bedrohung gefunden wird, wendet das Programm die Aktion an, die für die Komponente Schutz vor bedrohlichen Dateien ausgewählt wurde. **Container anhalten, wenn 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. **Dateivorgänge, die in Windows-Containern ausgeführt werden, nicht untersuchen**. Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm den Container nur beim Starten des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.

Schutz vor Web-Bedrohungen

Die Komponente „Schutz vor Web-Bedrohungen“ verhindert den Download schädlicher Dateien aus dem Internet und blockiert außerdem Verbindungen zu schädlichen Websites und Phishing-Websites. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken, des Cloud-Dienstes Kaspersky Security Network und der heuristischen Analyse.

Kaspersky Endpoint Security untersucht den HTTP-, HTTPS- und FTP-Datenverkehr. Kaspersky Endpoint Security untersucht URL- und IP-Adressen.

Um den Schutz vor Web-Bedrohungen zu verwenden, müssen Sie die Erstkonfiguration des Programms abschließen:

- Aktivieren Sie für die Kontrolle des HTTPS-Datenverkehrs die Untersuchung verschlüsselter Verbindungen (standardmäßig aktiviert).
- Wählen Sie die Ports aus, die Kaspersky Endpoint Security überwachen soll (standardmäßig überwacht das Programm alle Ports).
- Wählen Sie die Programme aus, deren Datenverkehr durch Kaspersky Endpoint Security überwacht werden soll. Die meisten Browser stehen bereits auf der Liste der von Kaspersky empfohlenen Programme. Wenn Ihr Browser nicht auf der Liste steht, fügen Sie ihn manuell hinzu.
- Wir empfehlen, ein Webseiten-Interaktionsskript in den Web-Datenverkehr einzubinden (die Skript-Injektion ist standardmäßig deaktiviert). Dieses Skript ermöglicht die Registrierung von Ereignissen des Schutzes vor Web-Bedrohungen im Ereignisprotokoll des Programms, im Ereignisprotokoll des Betriebssystems und in Berichten.

Wenn ein Benutzer versucht, eine schädliche Website oder eine Phishing-Website zu öffnen, blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an.

Einstellung	Beschreibung
Sicherheitsstufe *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Für den „Schutz vor Web-Bedrohungen" sind im Programm verschiedene Gruppen von Einstellungen (Einstellungssätze) verfügbar. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Auf dieser Sicherheitsstufe untersucht die Komponente „Schutz vor Web-Bedrohungen" den Web-Datenverkehr, den ein Computer über HTTP und FTP empfängt, mit höchster Genauigkeit. Der Schutz vor Web-Bedrohungen untersucht alle Objekte des Web-Datenverkehrs ausführlich, verwendet die vollständigen Programm-Datenbanken und führt zusätzlich eine heuristische Analyse mit maximaler Tiefe aus. • **Empfohlen**. Diese Sicherheitsstufe bietet ein optimales Gleichgewicht zwischen der Leistung des Programms und der Sicherheit für den Web-Datenverkehr. Die Komponente „Schutz vor Web-Bedrohungen" führt eine heuristische Analyse auf der mittleren Genauigkeitsebene aus. Diese Sicherheitsstufe für den Web-Datenverkehr wird von den Kaspersky-Experten empfohlen. • **Niedrig**. Diese Sicherheitsstufe für den Web-Datenverkehr gewährleistet maximale Geschwindigkeit bei der Untersuchung des Web-Datenverkehrs. Die Komponente „Schutz vor Web-Bedrohungen" führt die heuristische Analyse auf der Stufe „Oberflächlich" aus.
Aktion beim Fund einer Bedrohung	**Blockieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so blockiert die Komponente „Schutz vor Web-Bedrohungen" den Zugriff auf das Objekt und zeigt im Browser eine Benachrichtigung an. **Informieren**. Ist diese Variante ausgewählt und im Web-Datenverkehr wird ein infiziertes Objekt gefunden, so erlaubt Kaspersky Endpoint Security den Download dieses Objekts auf den Computer und fügt Informationen über das infizierte Objekt zur Liste der aktiven Bedrohungen hinzu.
Webadresse mit der Datenbank für bösartige Webadressen untersuchen *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Es wird überprüft, ob Links in der Datenbank für bösartige Webadressen vorhanden sind. Das ermöglicht den Schutz vor Websites, die auf der Deny-Liste stehen. Die Datenbank für schädliche Webadressen wird von den Kaspersky-Fachleuten angelegt, gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Heuristische Analyse verwenden *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Wenn der Datenverkehr auf Viren und sonstige bedrohliche Programme untersucht wird, führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Webadresse mit der Datenbank für Phishing-Webadressen untersuchen *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Die Datenbank für Phishing-Webadressen enthält die Webadressen der gegenwärtig bekannten Websites, die für Phishing-Angriffe benutzt werden. Kaspersky ergänzt diese Datenbank von Phishing-Links mit Adressen, die es von der internationalen Organisation, der sogenannten Anti-Phishing Working Group, erhalten hat. Die Datenbank für Phishing-Webadressen gehört zum Lieferumfang des Programms und wird beim Datenbank-Update von Kaspersky Endpoint Security aktualisiert.
Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen	Ist diese Option ausgewählt, so untersucht die Komponente „Schutz vor Web-Bedrohungen" den Inhalt von Webseiten/Websites nicht, deren Adressen auf der Liste der vertrauenswürdigen Webadressen stehen. Sie können zur Liste der vertrauenswürdigen Webadressen entweder die konkrete Adresse einer Webseite/Website hinzufügen oder eine Adressmaske für eine Webseite/Website. Außerdem können Sie eine allgemeine Liste mit Ausnahmen für verschlüsselte Verbindungen erstellen. 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.

Schutz vor E-Mail-Bedrohungen

Die Komponente „Schutz vor E-Mail-Bedrohungen" untersucht, ob in den Anlagen der ein- und ausgehenden E-Mail-Nachrichten Viren und andere bedrohliche Programme enthalten sind. 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. Die Anwendung unterstützt POP3, SMTP, IMAP und NNTP in den folgenden E-Mail-Clients:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

Um den Datenverkehr in den E-Mail-Clients Mozilla Thunderbird, MyOffice Mail und R7-Office Organizer zu untersuchen, müssen Sie ein Kaspersky-Zertifikat zum Zertifikatspeicher hinzufügen und den Speicher für eigene Zertifikate auswählen.

Der „Schutz vor E-Mail-Bedrohungen“ unterstützt keine anderen Protokolle und E-Mail-Clients.

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 bietet der „Schutz vor E-Mail-Bedrohungen“ eine Erweiterung für Microsoft Office Outlook. Mit dieser Erweiterung können Nachrichten auf der *Ebene des E-Mail-Clients* untersucht werden. Die Erweiterung für den Schutz vor E-Mail-Bedrohungen unterstützt die 32-Bit- und 64-Bit-Versionen von Outlook 2010, 2013, 2016, 2019, 2021, 2024 und 365. Auf Arm-basierten Computern unterstützt die Erweiterung für den Schutz vor E-Mail-Bedrohungen die 32-Bit- und 64-Bit-Versionen von Outlook 2016, Outlook 2021, Outlook 2024 und Outlook 365 für Arm64.

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 der Komponente „Schutz vor E-Mail-Bedrohungen“

Einstellung	Beschreibung
Sicherheitsstufe *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Für den Schutz vor E-Mail-Bedrohungen sind im Programm verschiedene Gruppen von Einstellungen verfügbar. Diese Einstellungsgruppen, die im Programm gespeichert sind, werden *Sicherheitsstufen* genannt: • **Hoch**. Auf dieser E-Mail-Sicherheitsstufe kontrolliert die Komponente „Schutz vor E-Mail-Bedrohungen“ die Nachrichten mit höchster Genauigkeit. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mails und führt eine tiefe heuristische Analyse durch. Die E-Mail-Sicherheitsstufe „Hoch“ wird für Umgebungen mit hohem Risiko empfohlen. Als Beispiel für eine gefährliche Umgebung kann eine Verbindung des Computers mit einem kostenlosen Mailanbieter dienen, wenn die Verbindung aus einem lokalen Netzwerk ohne zentralisierten E-Mail-Schutz erfolgt. • **Empfohlen**. Diese E-Mail-Sicherheitsstufe bietet ein optimales Gleichgewicht zwischen der Leistung des Programms und der Sicherheit für E-Mails. Die Komponente „Schutz vor E-Mail-Bedrohungen“ untersucht ein- und ausgehende E-Mail-Nachrichten und führt eine heuristische Analyse mit mittlerer Tiefe aus. Diese E-Mail-Sicherheitsstufe wird von den Kaspersky-Experten empfohlen. • **Niedrig**. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ nur eingehende E-Mail-Nachrichten, führt eine oberflächliche heuristische Analyse aus und scannt die an Nachrichten angehängten Archive nicht. Auf dieser E-Mail-Sicherheitsstufe untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ E-Mail-Nachrichten mit maximaler Geschwindigkeit und beansprucht die Betriebssystemressourcen minimal. Die E-Mail-Sicherheitsstufe „Niedrig“ ist für die Arbeit in einer gut geschützten Umgebung geeignet. Ein Beispiel für eine solche Umgebung ist ein LAN eines Unternehmens mit zentralisiertem E-Mail-Schutz.

Einstellung	Beschreibung
Aktion beim Fund einer Bedrohung	**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 Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, wird das infizierte Objekt gelöscht. Das Programm fügt Informationen über die ausgeführte Aktion zum Nachrichtenbetreff hinzu, z. B. *[Die Nachricht wurde verarbeitet.] <Nachrichtenbetreff>*. **Desinfizieren – Blockieren, wenn Desinfektion fehlschlägt**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, versucht das Programm, das gefundene Objekt zu desinfizieren. Der Benutzer erhält Zugriff auf die Nachricht mit der desinfizierten Anlage. Wenn das Objekt nicht desinfiziert werden kann, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. 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**. Wird in einer eingehenden Nachricht ein infiziertes Objekt gefunden, fügt das Programm dem Nachrichtenbetreff eine Warnung hinzu. Der Benutzer erhält Zugriff auf die Nachricht mit der ursprünglichen Anlage. Wird in einer ausgehenden Nachricht ein infiziertes Objekt gefunden, blockiert das Programm das Senden der Nachricht und der Mail-Client meldet einen Fehler.
Schutzbereich *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Der *Schutzbereich* umfasst die Objekte, welche die Komponente während ihrer Ausführung untersucht: ein- und ausgehende Nachrichten oder nur eingehende Nachrichten. Um den Schutz Ihrer Computer sicherzustellen, müssen Sie nur die eingehenden Nachrichten untersuchen. Die Untersuchung ausgehender Nachrichten kann aktiviert werden, um zu verhindern, dass infizierte Dateien in Form von Archiven versendet werden. Außerdem kann die Untersuchung ausgehender Nachrichten aktiviert werden, um zu verhindern, dass Dateien bestimmter Formate wie Audio- und Videodateien versendet werden.
POP3-, SMTP-, NNTP- und IMAP-Datenverkehr untersuchen	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	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. Erfolgt die E-Mail-Untersuchung mithilfe der Erweiterung für Microsoft Outlook, so wird empfohlen, den Exchange-Cache-Modus zu verwenden (Use Cached Exchange Mode). Ausführlichere Informationen über den Exchange-Cache-Modus und Tipps zu seiner Verwendung finden Sie in der Microsoft Knowledge Base.
Heuristische Analyse *(nur in der Verwaltungskonsole (MMC) und in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar)*	Technologie zum Erkennen von Bedrohungen, die nicht mithilfe der aktuellen Version der Datenbanken für Programme von Kaspersky festgestellt werden können. Ermöglicht die Erkennung von Dateien, die einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten. Während der Untersuchung der Dateien auf bösartigen Code führt die heuristische Analyse die Anweisungen in den ausführbaren Dateien aus. Die Anzahl der Anweisungen, die von der heuristischen Analyse ausgeführt werden, sind von der für die heuristische Analyse festgelegten Ebene abhängig. Die Ebene der heuristischen Analyse regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach neuen Bedrohungen, der Belastungsstufe der Betriebssystemressourcen und der Dauer der heuristischen Analyse.
Angehängte Archive untersuchen	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs). Falls das Programm während der Untersuchung im Nachrichtentext ein Kennwort für ein Archiv findet, wird dieses Kennwort verwendet, um den Inhalt des Archivs auf Schadsoftware zu untersuchen. Das Kennwort wird in diesem Fall nicht gespeichert. Ein Archiv wird während der Untersuchung entpackt. Wenn während des Entpackungsvorgangs ein Anwendungsfehler auftritt, können Sie die unter dem folgenden Pfad gespeicherten entpackten Dateien manuell löschen: %systemroot%\temp. Diese Dateien besitzen das Präfix PR.
Angehängte Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Archive nicht untersuchen, wenn größer als n MB	Ist das Kontrollkästchen aktiviert, so schließt die Komponente „Schutz vor E-Mail-Bedrohungen“ die Archive, die an E-Mail-Nachrichten angehängt sind, von der Untersuchung aus, falls sie die festgelegte Größe überschreiten. Ist das Kontrollkästchen deaktiviert, so untersucht die Komponente „Schutz vor E-Mail-Bedrohungen“ die an E-Mail-Nachrichten angehängten Archive unabhängig von deren Größe.

Einstellung	Beschreibung
Untersuchungsdauer für Archive beschränken auf n Sekunden	Wenn dieses Kontrollkästchen aktiviert ist, wird die Untersuchungsdauer für Archive, die an E-Mail-Nachrichten angehängt sind, auf die festgelegte Dauer beschränkt.
Anlagenfilterung	Die Anlagenfilterung funktioniert nicht für ausgehende E-Mail-Nachrichten. **Filterung deaktivieren**. Bei Auswahl dieser Variante werden Dateien, die an E-Mail-Nachrichten angehängt sind, von der Komponente „Schutz vor E-Mail-Bedrohungen“ nicht gefiltert. **Anlagen der ausgewählten Typen umbenennen**. Wenn Sie diese Option auswählen, ersetzt der Schutz vor E-Mail-Bedrohungen das letzte Zeichen der Erweiterung angehängter Dateien bestimmter Typen mit einem Unterstrich (z. B. attachment.doc_). Der Benutzer muss die Datei dann zunächst umbenennen, um sie öffnen zu können. **Anlagen der ausgewählten Typen löschen**. Bei Auswahl dieser Variante löscht die Komponente „Schutz vor E-Mail-Bedrohungen“ aus E-Mail-Nachrichten die angehängten Dateien der angegebenen Typen. Die Typen der angehängten Dateien, die umbenannt und aus E-Mail-Nachrichten gelöscht werden sollen, können Sie in der Liste der Dateimasken festlegen.

Schutz vor Netzwerkbedrohungen

Die Komponente *Schutz vor Netzwerkbedrohungen* (auch Intrusion Detection System oder IDS genannt) überwacht den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe charakteristisch sind. Wenn das Programm einen Netzwerkangriff auf den Benutzercomputer erkennt, sperrt es die Netzwerkverbindung mit dem angreifenden Computer. Beschreibungen der derzeit bekannten Arten von Netzwerkangriffen und entsprechende Abwehrmethoden sind in den Programm-Datenbanken enthalten. Die Liste der Netzwerkangriffe, die von der Komponente „Schutz vor Netzwerkbedrohungen“ erkannt werden, wird beim Update der Datenbanken und Programm-Module aktualisiert.

Einstellungen für die Komponente „Schutz vor Netzwerkbedrohungen“

Einstellung	Beschreibung
Port-Scanning und Netzwerk-Flooding als Angriffe betrachten	*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. 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. 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.
Angreifende Geräte sperren für n 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. Die Sperrliste können Sie im Fenster Netzwerkmonitor ansehen. Kaspersky Endpoint Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ geändert werden.

Einstellung	Beschreibung
Ausnahmen	Die Liste enthält IP-Adressen, von denen die Komponente „Schutz vor Netzwerkbedrohungen“ keine Netzwerkangriffe blockiert. Sie können eine IP-Adresse mit angegebenem Port und Protokoll hinzufügen. Informationen über Netzwerkangriffe von den IP-Adressen, die zur Ausnahmeliste gehören, werden vom Programm nicht in den Bericht aufgenommen.
MAC-Spoofing-Schutz	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

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*.

Der Administrationsagent wird für die Interaktion mit Kaspersky Security Center verwendet. Die Firewall erstellt automatisch Netzwerkregeln, die für die ordnungsgemäße Funktion des Programms und des Administrationsagenten erforderlich sind. Dadurch bedingt öffnet die Firewall bestimmte Ports auf dem Computer. Welche Ports geöffnet werden, hängt von der Rolle des Computers ab (z. B. Verteilungspunkt). Weitere Informationen zu den Ports, die auf dem Computer geöffnet werden, finden Sie in der Hilfe zu Kaspersky Security Center.

Netzwerkregeln

Sie können die Netzwerkregeln auf folgenden Ebenen anpassen:

- *Regeln für Netzwerkpakete*. Sie dienen zur Definition von Beschränkungen für die Netzwerkpakete, wobei das Programm keine Rolle spielt. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Kaspersky Endpoint Security hat vordefinierte Netzwerkregeln für Pakete mit Lösungen, die von den Kaspersky-Experten empfohlen werden.

- *Netzwerkregeln für das Programm*. Sie dienen zur Definition von Beschränkungen der Netzwerkaktivität eines konkreten Programms. Dabei werden nicht nur die Merkmale des Netzwerkpakets berücksichtigt, sondern auch das konkrete Programm, an das dieses Netzwerkpaket adressiert ist oder welches das Senden dieses Netzwerkpakets initiiert hat.

Die Komponente „Programm-Überwachung“ kontrolliert mithilfe von *Programmrechten* den Zugriff auf Betriebssystemressourcen, Prozesse und persönliche Daten.

Wenn ein Programm zum ersten Mal gestartet wird, führt die „Firewall“ folgende Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.
2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Firewall“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.
3. Platziert das Programm in einer der Vertrauensgruppen: *Vertrauenswürdig*, *Schwach beschränkt*, *Stark beschränkt*, *Nicht vertrauenswürdig*.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

   Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

   Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung” aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.
4. Blockiert abhängig von der Sicherheitsgruppe die Netzwerkaktivität des Programms. Für Programme aus der Sicherheitsgruppe „*Stark beschränkt*“ sind beispielsweise alle Netzwerkverbindungen verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde das Programm nicht verändert, so wendet die Komponente die aktuellen Netzwerkregeln darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Prioritäten der Netzwerkregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, desto höher ist ihre Priorität. Wenn eine Netzwerkaktivität in mehreren Regeln vorkommt, reguliert die „Firewall“ die Netzwerkaktivität nach der Regel mit der höchsten Priorität.

Netzwerkregeln für Pakete besitzen eine höhere Priorität als Netzwerkregeln für Programme. Sind für eine Art der Netzwerkaktivität gleichzeitig Netzwerkregeln für Pakete und Netzwerkregeln für Programme vorhanden, wird diese Netzwerkaktivität nach den Netzwerkregeln für Pakete verarbeitet.

Netzwerkregeln für Programme funktionieren auf besondere Weise. Die Netzwerkregel für Programme enthält Zugriffsregeln basierend auf dem Netzwerkstatus: *Öffentliches Netzwerk*, *Lokales Netzwerk*, *Vertrauenswürdiges Netzwerk*. Zum Beispiel ist für die Sicherheitsgruppe „*Stark beschränkt*“ standardmäßig jede Netzwerkaktivität eines Programms in Netzwerken mit beliebigem Status verboten. Wenn für ein bestimmtes Programm (übergeordnetes Programm) eine Netzwerkregel vorliegt, werden die untergeordneten Prozesse anderer Programme gemäß der Netzwerkregel des übergeordneten Programms ausgeführt. Gibt es keine Netzwerkregel für ein Programm, so werden die untergeordneten Prozesse gemäß der Regel für den Zugriff auf Netzwerke der Sicherheitsgruppe des Programms ausgeführt.

Beispiel: Sie haben jede Netzwerkaktivität aller Programme für Netzwerke mit beliebigem Status verboten, unter Ausnahme von Browser X. Wenn Browser X (übergeordnetes Programm) die Installation von Browser Y startet (untergeordneter Prozess), erhält Browser Y Zugriff auf das Netzwerk und lädt die erforderlichen Dateien herunter. Nach der Installation sind für Browser Y alle Netzwerkverbindungen verboten, wobei die Einstellungen der Firewall gelten. Um dem Installationsprogramm von Browser Y die Netzwerkaktivität als untergeordneter Prozess zu verbieten, muss eine Netzwerkregel für das Installationsprogramm von Browser Y hinzugefügt werden.

Arten von Netzwerkverbindungen

Bei der Kontrolle der Netzwerkaktivität kann die „Firewall“ den Typ einer Netzwerkverbindung berücksichtigen. Den Typ der Netzwerkverbindung erhält Kaspersky Endpoint Security vom Betriebssystem des Computers. Den Typ einer Netzwerkverbindung im Betriebssystem legt der Benutzer beim Einrichten der Verbindung fest. Sie können den Typ der Netzwerkverbindung in den Einstellungen von Kaspersky Endpoint Security ändern. Dann kontrolliert die Firewall die Netzwerkaktivität anhand des Netzwerktyps, der in den Einstellungen von Kaspersky Endpoint Security angegeben ist, nicht anhand des Typs aus dem Betriebssystem.

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.

  Das Internet erhält von der Firewall standardmäßig den Typ *Öffentliches Netzwerk*. Der Typ des Internets kann nicht geändert werden.

- **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 im Rahmen dieses Netzwerks jede beliebige Netzwerkaktivität.

Einstellungen für die Komponente „Firewall“

Einstellung	Beschreibung
Paketregeln	Tabelle der Netzwerkregeln für Pakete. Netzwerkregeln für Pakete werden verwendet, um Netzwerkpakete unabhängig von Programmen einzuschränken. Diese Regeln beschränken die ein- und ausgehende Netzwerkaktivität anhand bestimmter Ports für ausgewählte Datenübertragungsprotokolle. Die Tabelle enthält vordefinierte Netzwerkregeln für Pakete, die von Kaspersky zum optimalen Schutz des Netzwerkverkehrs für Computer mit dem Betriebssystem Microsoft Windows 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	Diese Tabelle enthält Informationen über Netzwerkverbindungen, welche die Firewall auf dem Benutzercomputer gefunden hat. Das Internet besitzt standardmäßig den Status *Öffentliches Netzwerk*. Der Status des Internets kann nicht geändert werden.

Einstellung	Beschreibung
Regeln für Programme	**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.

Schutz vor modifizierten USB-Geräten

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.

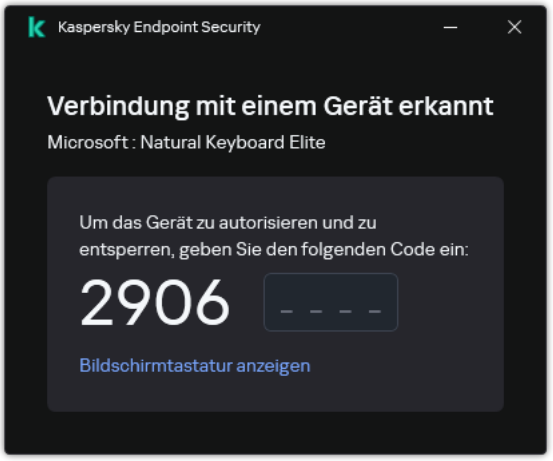
Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (sofern verfügbar) einen vom Programm generierten Code einzugeben (siehe folgende Abbildung). Dieser Vorgang 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.

Wurde der digitale Code falsch eingegeben, so generiert das Programm einen neuen Code. 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.



Autorisierung der Tastatur

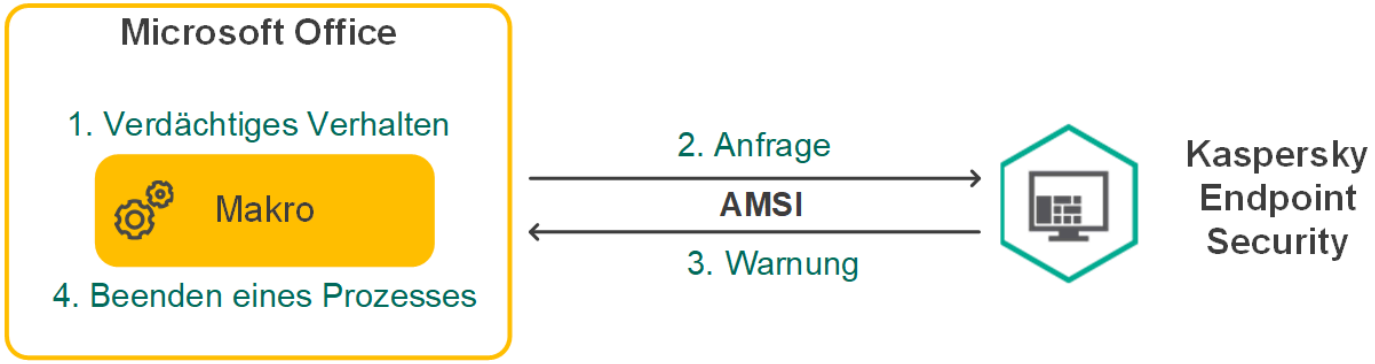
Einstellungen für die Komponente „Schutz vor modifizierten USB-Geräten"

Einstellung	Beschreibung
Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten	Wenn der Schalter aktiviert ist, verbietet das Programm die Verwendung einer Bildschirmtastatur für die Autorisierung eines USB-Geräts, von dem aus der Autorisierungscode nicht eingegeben werden kann.
Verwendung eines Strichcodes zur Autorisierung von USB-Geräten verbieten	Wenn der Schalter aktiviert ist, zeigt das Programm in der Benachrichtigung zur Authentifizierung des Barcode-Scanners keinen Strichcode an.
Maximale Anzahl der Autorisierungsversuche für USB-Geräte	Automatisches Blockieren des USB-Gerätes, wenn der Autorisierungscode zu oft falsch eingegeben wird. Mögliche Werte: 1 bis 10. Wenn Sie beispielsweise fünf Eingabeversuche für den Autorisierungscode erlauben, sperrt das Programm das USB-Gerät nach dem fünften erfolglosen Versuch. Kaspersky Endpoint Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie erneut fünf Versuche, den Autorisierungscode einzugeben.
Timeout beim Erreichen der maximalen Anzahl von Versuchen	Dauer, für die das USB-Gerät gesperrt wird, nachdem die festgelegte Anzahl erfolgloser Eingabeversuche für den Autorisierungscode erreicht wurde. Mögliche Werte: 1 bis 180 (Minuten).

AMSI-Schutz

Die Komponente "AMSI-Schutz" dient der Unterstützung des Antimalware Scan Interface von Microsoft. Mithilfe *Schnittstelle für Antimalware Scan Interface (AMSI)* können Dritthersteller-Anwendungen, die AMSI unterstützen, Objekte (z. B. PowerShell-Skripte) für eine zusätzliche Untersuchung an Kaspersky Endpoint Security senden und Untersuchungsergebnisse für diese Objekte erhalten. Dritthersteller-Anwendungen können z. B. Microsoft-Office-Programme sein (siehe folgende Abb.). Details über die AMSI-Schnittstelle finden Sie in der Microsoft-Dokumentation.

Die Funktion von „AMSI-Schutz“ ist darauf beschränkt, eine Bedrohung zu erkennen und eine Drittanbieterprogramm über die gefundene Bedrohung zu benachrichtigen. Nachdem eine Dritthersteller-Anwendung über eine Bedrohung benachrichtigt wurde, verhindert diese die schädlichen Aktionen (z. B. beendet die Aktion).



Beispiel für die Funktionsweise von AMSI

Die Komponente „AMSI-Schutz“ kann die Anfrage eines Drittanbieterprogramms zurückweisen. Dies ist beispielsweise möglich, wenn dieses Programm die maximale Anzahl von Anfragen innerhalb des festgelegten Zeitraums erreicht hat. Kaspersky Endpoint Security sendet Informationen über die Ablehnung der Anfrage einer Dritthersteller-Anwendung an den Administrationsserver. Die Komponente „AMSI-Schutz“ weist Anfragen von Drittanbieter-Programmen nicht zurück, wenn für diese die kontinuierliche Integration mit der „AMSI-Schutz“-Komponente aktiviert ist.

„AMSI-Schutz“ ist für die folgenden Betriebssysteme für Workstations und Server verfügbar:

- Windows 10 Home / Pro / Pro für Workstations / Education / Enterprise / Enterprise Multi-Session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise Multi-Session
- Windows Server 2016 Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2019 Essentials / Standard / Datacenter (einschließlich Server Core-Modus)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (einschließlich Server Core-Modus)
- Windows Server 2025 Standard / Datacenter

Einstellungen für den AMSI-Schutz

Einstellung	Beschreibung
Archive untersuchen	Untersuchung von ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE und anderen Archiven. Das Programm untersucht Archive nicht nur nach Erweiterungen, sondern auch nach Format. Bei der Untersuchung von Archiven führt die App das Entpacken rekursiv durch. Dadurch können Bedrohungen in mehrstufigen Archiven erkannt werden (Archive innerhalb eines Archivs).
Programmpakete untersuchen	Verteilungspakete für Drittanbieter-Programme untersuchen.
Dateien in Microsoft Office-Formaten untersuchen	Untersucht Microsoft Office-Dateien (DOC, DOCX, XLS, PPT und andere Microsoft-Erweiterungen). Office-Format-Dateien enthalten auch OLE-Objekte. Dateien im Office-Format, die kleiner als 1 MB sind, werden unabhängig vom Status dieses Kontrollkästchens durch die App untersucht.
Große zusammengesetzte Dateien nicht entpacken	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.

Exploit-Prävention

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.

Einstellungen der Komponente „Exploit-Prävention”

Einstellung	Beschreibung
Wenn ein Exploit erkannt wird	**Blockieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, blockiert Kaspersky Endpoint Security die Aktivitäten dieses Exploits und erstellt einen Berichtseintrag, der Informationen über diesen Exploit enthält. **Informieren**. Wenn dieses Element ausgewählt ist und ein Exploit gefunden wird, erstellt Kaspersky Endpoint Security einen Berichtseintrag, der Informationen über den Exploit enthält, und fügt Informationen über diesen Exploit zur Liste der aktiven Bedrohungen hinzu.
Schutz für den Arbeitsspeicher von Systemprozessen aktivieren	Ist dieser Schalter aktiviert, so blockiert Kaspersky Endpoint Security Drittanbieter-Prozesse, die versuchen, auf den Arbeitsspeicher von Systemprozessen zuzugreifen.

Verhaltensanalyse

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.

Einstellungen der Komponente „Verhaltensanalyse”

Einstellung	Beschreibung
Aktion, wenn Schadsoftware-Aktivität erkannt wird	**Löschen**. Ist diese Variante ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Endpoint Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an. **Blockieren**. Ist diese Variante ausgewählt, so beendet Kaspersky Endpoint Security beim Fund einer schädlichen Programmaktivität die betreffende Anwendung. **Informieren**. Ist diese Variante ausgewählt und es wird eine schädliche Programmaktivität erkannt, so beendet Kaspersky Endpoint Security dieses Programm nicht und fügt Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.

Programm-Überwachung

Die Komponente „Programm-Überwachung“ (HIPS, Host Intrusion Prevention System) hindert Programme daran, systemgefährdende Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und persönliche Daten. Die Komponente schützt den Computer mithilfe der Antiviren-Datenbanken und des Cloud-Dienstes Kaspersky Security Network

Die Komponente kontrolliert Programme mithilfe von *Programmrechten*. Programmrechte beinhalten die folgenden Zugriffseinstellungen:

- Zugriff auf Betriebssystemressourcen (z. B. Autostart-Einstellungen und Registrierungsschlüssel)
- Zugriff auf persönliche Daten (z. B. auf Dateien und Programme)

Die Netzwerkaktivität von Programmen wird von der Komponente Firewall mithilfe von *Netzwerkregeln* kontrolliert.

Wenn ein Programm zum ersten Mal gestartet wird, führt die Komponente „Programm-Überwachung“ die folgenden Aktionen aus:

1. Die Sicherheit des Programms wird mithilfe der geladenen Antiviren-Datenbanken untersucht.
2. Die Sicherheit des Programms wird in Kaspersky Security Network untersucht.

   Um die Effektivität der Komponente „Programm-Überwachung“ zu erhöhen, wird die Teilnahme an Kaspersky Security Network empfohlen.

3. Platziert das Programm in einer der Vertrauensgruppen: *Vertrauenswürdig*, *Schwach beschränkt*, *Stark beschränkt*, *Nicht vertrauenswürdig*.

   Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme verwendet. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

   Kaspersky Endpoint Security weist das Programm einer Sicherheitsgruppe für die Komponenten „Firewall“ und „Programm-Überwachung“ zu. Es ist nicht möglich, die Sicherheitsgruppe nur für die „Firewall“ oder nur für die „Programm-Überwachung“ zu ändern.

   Wenn Sie die Teilnahme an KSN abgelehnt haben oder keine Internetverbindung besteht, wählt Kaspersky Endpoint Security die Sicherheitsgruppe für das Programm anhand der Einstellungen der Komponente „Programm-Überwachung“ aus. Wenn später Daten über die Reputation des Programms aus KSN empfangen werden, kann die Sicherheitsgruppe automatisch geändert werden.

4. Blockiert abhängig von der Sicherheitsgruppe die Aktionen des Programms. Für Programme aus der Sicherheitsgruppe „*Stark beschränkt*“ ist beispielsweise der Zugriff auf Module des Betriebssystems verboten.

Beim nächsten Programmstart untersucht Kaspersky Endpoint Security die Programmintegrität. Wurde ein Programm nicht verändert, so wendet die Komponente die aktuellen Rechte für Programme darauf an. Wurde das Programm verändert, so untersucht Kaspersky Endpoint Security das Programm erneut wie beim ersten Start.

Einstellungen der Komponente „Programm-Überwachung"

Einstellung	Beschreibung
Rechte für Programme	Tabelle der Programme, die von der Komponente „Programm-Überwachung" kontrolliert werden. Die Programme sind auf Sicherheitsgruppen verteilt. Die Sicherheitsgruppe legt die Rechte fest, die Kaspersky Endpoint Security für die Aktivitätskontrolle für Programme 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. Die folgenden Tabellen enthalten die Zugriffsrechte von Programmen: • **Dateien und Systemregistrierung**. Tabelle mit Zugriffsrechten für Betriebssystemressourcen und persönliche Daten für Programme, die zu der Sicherheitsgruppe gehören. • **Rechte**. Tabelle mit Zugriffsrechten für Prozesse und Betriebssystemressourcen für Programme, die zu der Sicherheitsgruppe gehören. • **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.
Geschützte Ressourcen	Die Tabelle enthält Computerressourcen, die nach Kategorien angeordnet sind. Die Komponente „Programm-Überwachung" kontrolliert den Zugriff anderer Programme auf die Ressourcen aus dieser Tabelle. Eine Ressource kann sein: Registrierungskategorie, Datei, Ordner oder Registrierungsschlüssel.
Sicherheitsgruppe für Programme, die vor Kaspersky Endpoint Security gestartet werden	Sicherheitsgruppe, in die Kaspersky Endpoint Security die Programme verschiebt, die vor Kaspersky Endpoint Security gestartet werden.
Regeln für bisher unbekannte Programme aus KSN aktualisieren	Ist das Kontrollkästchen aktiviert, so aktualisiert die Komponente „Programm-Überwachung" die Rechte von bisher unbekannten Programmen unter Verwendung der Datenbank von Kaspersky Security Network.
Programmen mit digitaler Signatur vertrauen	Ist dieses Kontrollkästchen aktiviert, so weist die Komponente „Programm-Überwachung" die Programme, die eine digitale Signatur eines vertrauenswürdigen Herstellers besitzen, der Gruppe „*Vertrauenswürdig*" zu. *Vertrauenswürdige Hersteller* sind Softwareanbieter, denen Kaspersky vertraut. Sie können ein Herstellerzertifikat auch manuell zum Speicher für vertrauenswürdige Zertifikate hinzufügen. Ist das Kontrollkästchen deaktiviert, so stuft die Komponente „Programm-Überwachung" solche Programme nicht als vertrauenswürdig ein und weist sie anhand anderer Kriterien zu den Sicherheitsgruppen zu.
Regeln für Programme löschen, wenn nicht gestartet seit über n Tagen	Ist das Kontrollkästchen aktiviert, so löscht Kaspersky Endpoint Security automatisch die Informationen über das Programm (Sicherheitsgruppe, Zugriffsrechte), wenn die folgenden Bedingungen erfüllt sind: • Sie haben das Programm einer Sicherheitsgruppe zugeordnet oder die Zugriffsrechte manuell angepasst. • Das Programm wurde innerhalb des festgelegten Zeitraums nicht gestartet. Wenn die Sicherheitsgruppe und die Programmrechte automatisch festgelegt wurden, löscht Kaspersky Endpoint Security die Informationen über dieses Programm nach 30 Tagen. Es ist nicht möglich, die Speicherdauer für Informationen über ein Programm zu ändern oder das automatische Löschen zu deaktivieren. Wenn dieses Programm zum nächsten Mal gestartet wird, untersucht Kaspersky Endpoint Security das Programm wie beim ersten Start.
Sicherheitsgruppe für Programme, die nicht zu anderen Gruppen gehören	Mit den Elementen dieser Dropdown-Liste wird festgelegt, welcher Sicherheitsgruppe Kaspersky Endpoint Security ein unbekanntes Programm zuordnen soll. Sie können eines der folgenden Elemente wählen: • **Schwach beschränkt**. • **Stark beschränkt**. • **Nicht vertrauenswürdig**.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Endpoint Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem verarbeitet Kaspersky Endpoint Security folgende Typen von schädlicher Programmaktivität:

- **Dateiaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht ausführbare Dateien, die von Schadsoftware erstellt wurden (auf allen Datenträgern, außer auf Netzlaufwerken).
  - löscht ausführbare Dateien, die von Programmen erstellt wurden, in welche Schadsoftware eingedrungen ist.
  - stellt Dateien wieder her, die von Schadsoftware verändert oder gelöscht wurden.

  Die Funktionalität zur Wiederherstellung von Dateien besitzt bestimmte Beschränkungen.

- **Aktivität der Registrierung**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - löscht Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden.
  - stellt Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden, nicht wieder her.

- **Systemaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - beendet Prozesse, die von Schadsoftware gestartet wurden.
  - beendet Prozesse, in die Schadsoftware eingedrungen ist.
  - stellt Prozesse, die von Schadsoftware beendet wurden, nicht wieder her.

- **Netzwerkaktivität**

  Kaspersky Endpoint Security führt die folgenden Aktionen aus:

  - verbietet die Netzwerkaktivität von Schadsoftware.
  - verbietet die Netzwerkaktivität von Prozessen, in die Schadsoftware eingedrungen ist.

Ein Rollback von Schadsoftware-Aktionen kann entweder von der Komponente Schutz vor bedrohlichen Dateien, Verhaltensanalyse oder bei einer Schadsoftware-Untersuchung gestartet werden.

Das Rollback der Aktionen schädlicher Programme betrifft lediglich eine eng eingeschränkte Auswahl an Daten. Ein Rollback hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und die Integrität der Daten auf Ihrem Computer.

Kaspersky Security Network

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Endpoint Security die von Benutzern aus aller Welt empfangenen Daten. Für den Empfang dieser Daten ist Kaspersky Security Network vorgesehen.

Die KSN-Funktionalität ist im Programm in den USA möglicherweise nicht verfügbar

Kaspersky Security Network (KSN) ist eine Infrastruktur von Cloud-Diensten, die Zugriff auf eine ständig aktualisierte Kaspersky-Wissensdatenbank bietet. Diese Datenbank enthält Informationen zur Reputation von Dateien, Internet-Ressourcen und Programmen. Durch die Nutzung von Daten aus Kaspersky Security Network wird die Reaktion von Kaspersky Endpoint Security auf unbekannte Bedrohungen beschleunigt und die Leistungsfähigkeit bestimmter Schutzkomponenten erhöht. Außerdem reduziert sich das Risiko von Fehlalarmen. 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 Konfiguration des Zugriffs auf KSN 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.

Ausführliche Informationen darüber, welche statistischen Informationen, die während der Teilnahme an KSN generiert werden, an Kaspersky gesendet werden und wie solche Informationen gespeichert und gelöscht werden, finden Sie in der Erklärung zu Kaspersky Security Network und auf der Kaspersky-Website. 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 Arbeit mit Kaspersky-Reputationsdatenbanken:

- 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.

Die Übertragung von Daten aus dem Land ihres Standorts oder aus dem Unternehmens-LAN ist rechtlich oder durch Unternehmenssicherheitsrichtlinien untersagt.

Einstellung	Beschreibung
Erweiterten KSN-Modus aktivieren	Im *erweiterten KSN-Modus* überträgt Kaspersky Endpoint Security zusätzliche Daten an Kaspersky. Unabhängig vom Zustand des Schalters verwendet Kaspersky Endpoint Security KSN für die Erkennung von Bedrohungen.
Cloud-Modus aktivieren	*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. Ist der Schalter aktiviert, so verwendet Kaspersky Endpoint Security eine eingeschränkte Version der Antiviren-Datenbanken. Dadurch werden die Betriebssystemressourcen entlastet. Nachdem das Kontrollkästchen aktiviert wurde, lädt Kaspersky Endpoint Security beim nächsten Update eine eingeschränkte Version der Antiviren-Datenbanken herunter. Ist der Schalter deaktiviert, so 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 *(nur in der Konsole von Kaspersky Security Center verfügbar)*	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 *(nur in der Konsole von Kaspersky Security Center verfügbar)*	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.
Kaspersky Security Network-Server verwenden, wenn kein KSN-Proxyserver verfügbar *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Ist das Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security die KSN-Server, wenn der KSN Proxy-Dienst nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird).

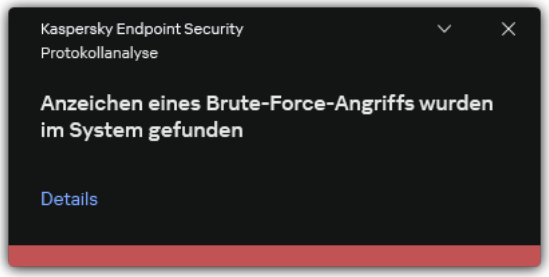
Protokollanalyse

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 „Protokollanalyse“ überwacht die Integrität der geschützten Umgebung basierend auf der Windows-Ereignisprotokollanalyse. Wenn das Programm ungewöhnliche Verhaltensmerkmale im System erkennt, wird der Administrator informiert, da solches Verhalten auf einen versuchten Cyberangriff hinweisen kann.

Kaspersky Endpoint Security analysiert Windows-Ereignisprotokolle und erkennt Verstöße gemäß den Regeln. Die Komponente enthält vordefinierte Regeln. Vordefinierte Regeln basieren auf einer heuristischen Analyse. Sie können auch Ihre eigenen Regeln hinzufügen (benutzerdefinierte Regeln). Wenn eine Regel ausgelöst wird, erstellt das Programm ein Ereignis mit dem Status *Kritisch* (siehe Abbildung unten).

Wenn Sie die Protokollanalyse verwenden möchten, stellen Sie sicher, dass die Sicherheitseinstellungen der Audit-Richtlinie konfiguriert sind und das System die relevanten Ereignisse protokolliert (Einzelheiten finden Sie auf der Website des technischen Supports von Microsoft).



Protokollanalysebenachrichtigung

Protokollanalyseeinstellungen

Einstellung	Beschreibung
Vordefinierte Regeln	Liste der Protokollanalyseregeln. Vordefinierte Regeln enthalten Vorlagen für anormale Aktivitäten auf dem geschützten Computer. Abnormale Aktivität kann auf einen versuchten Angriff hindeuten.
Benutzerdefinierte Regeln	Liste der vom Benutzer hinzugefügten Protokollanalyseregeln. Sie können Ihre eigenen Auslösekriterien für die Protokollanalyseregel festlegen. Dazu müssen Sie eine Ereignis-ID eingeben und eine Ereignisquelle auswählen. Sie können eine Ereignisquelle aus den Standardprotokollen auswählen: *Application*, *Security* oder *System*. Sie können auch das Protokoll eines Drittanbieterprogramms angeben.

Schutz vor Verschlüsselung

Die Komponente „Schutz vor Verschlüsselung“ analysiert die Aktivität in freigegebenen Ordnern. 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.

Kaspersky Endpoint Security schützt nur jene Dateien vor ferngesteuerten Verschlüsselungsversuchen, die sich auf Datenträgern mit NTFS-Dateisystem befinden und nicht mit einem EFS-System verschlüsselt wurden.

Einstellung	Beschreibung
Ausnahmen nach Name oder IP-Adresse	**Ausnahmen nach Name oder IP-Adresse**. Liste der Computer, deren Verschlüsselungsversuche für gemeinsame Ordner nicht überwacht werden. Damit die Ausnahmeliste funktioniert, mit der Computer aus dem Schutz gemeinsamer Ordner vor externer Verschlüsselung ausgeschlossen werden, muss die Überwachung von Anmeldeereignissen am System in der Windows-Sicherheitsüberwachungsrichtlinie aktiviert werden. Die Überwachung von Anmeldeereignissen am System ist standardmäßig deaktiviert. Details über die Windows-Sicherheitsüberwachungsrichtlinie finden Sie auf der Microsoft-Website. **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. Beispielsweise kann die „Verhaltensanalyse“ Fehlalarme auslösen, wenn der Benutzer in einem gemeinsamen Ordner Dateien mit der Erweiterung ENC verwendet. Diese Aktivität gleicht einem Verhaltensmuster, das für externe Verschlüsselung charakteristisch ist. Wenn Sie zu Datenschutzzwecken verschlüsselte Dateien in einem gemeinsamen Ordner ablegen, fügen Sie diesen Ordner den Ausnahmen hinzu. 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` funktioniert nicht. • 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	• **Informieren**. Wenn diese Option ausgewählt ist und Kaspersky Endpoint Security einen Versuch zur Änderung von Dateien in freigegebenen Ordnern erkennt, fügt das Programm Informationen über diesen Versuch zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über eine erkannte schädliche Aktivität an Kaspersky Security Center. • **Verbindung blockieren für (Min.) n Minuten**. Ist diese Option ausgewählt und Kaspersky Endpoint Security erkennt einen Versuch, Dateien in gemeinsamen Ordnern zu ändern, so blockiert die App den Zugriff auf die Dateiänderung für die Sitzung, die die schädliche Aktivität initiiert hat, und erstellt Backup-Kopien der veränderten Dateien. Ist die Komponente „Rollback von schädlichen Aktionen“ aktiviert und die Option **Verbindung blockieren für (Min.) n Minuten** ausgewählt, so werden die veränderten Dateien aus den Backup-Kopien wiederhergestellt.
Schutzbereich	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.

Web-Kontrolle

Die „Web-Kontrolle“ verwaltet den Zugriff durch Benutzer auf Webressourcen. Dadurch lässt sich Datenverkehr einsparen und die zweckentfremdete Nutzung der Arbeitszeit reduzieren. Wenn ein Benutzer versucht, eine Website zu öffnen, auf den die „Web-Kontrolle“ den Zugriff beschränkt, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Warnung an (siehe folgende Abb.).

Um die Web-Kontrolle zu verwenden, müssen Sie die Erstkonfiguration des Programms abschließen:

- Aktivieren Sie für die Kontrolle des HTTPS-Datenverkehrs die Untersuchung verschlüsselter Verbindungen (standardmäßig aktiviert).
- Wählen Sie die Ports aus, die Kaspersky Endpoint Security überwachen soll (standardmäßig überwacht das Programm alle Ports).
- Wählen Sie die Programme aus, deren Datenverkehr durch Kaspersky Endpoint Security überwacht werden soll. Die meisten Browser stehen bereits auf der Liste der von Kaspersky empfohlenen Programme. Wenn Ihr Browser nicht auf der Liste steht, fügen Sie ihn manuell hinzu.
- Wir empfehlen, ein Webseiten-Interaktionsskript in den Web-Datenverkehr einzubinden (die Skript-Injektion ist standardmäßig deaktiviert). Dieses Skript ermöglicht die Registrierung von Web-Kontrolle-Ereignissen für die Ereignisanzeige des Programms, die Ereignisanzeige des Betriebssystems und Berichte.

Methoden zur Verwaltung des Zugriffs auf Websites

Mithilfe der „Web-Kontrolle“ kann der Zugriff auf Websites wie folgt angepasst werden:

- **Website-Kategorie**. 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). So können Sie z. B. den Benutzerzugriff auf die Kategorie „*Soziale Netzwerke*“ oder auf andere Kategorien beschränken.
- **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. festlegen, dass der Zugriff auf den Datentyp *Dateien für Office-Programme* nur für die Website-Kategorie *Web-E-Mail* beschränkt werden soll.

Regeln für den Zugriff auf Websites

Die „Web-Kontrolle“ verwaltet den Zugriff von Benutzern auf Websites mithilfe von *Zugriffsregeln*. Sie können eine Regel für den Zugriff auf Websites wie folgt zusätzlich anpassen:

- Benutzer, für welche die Regel gilt.

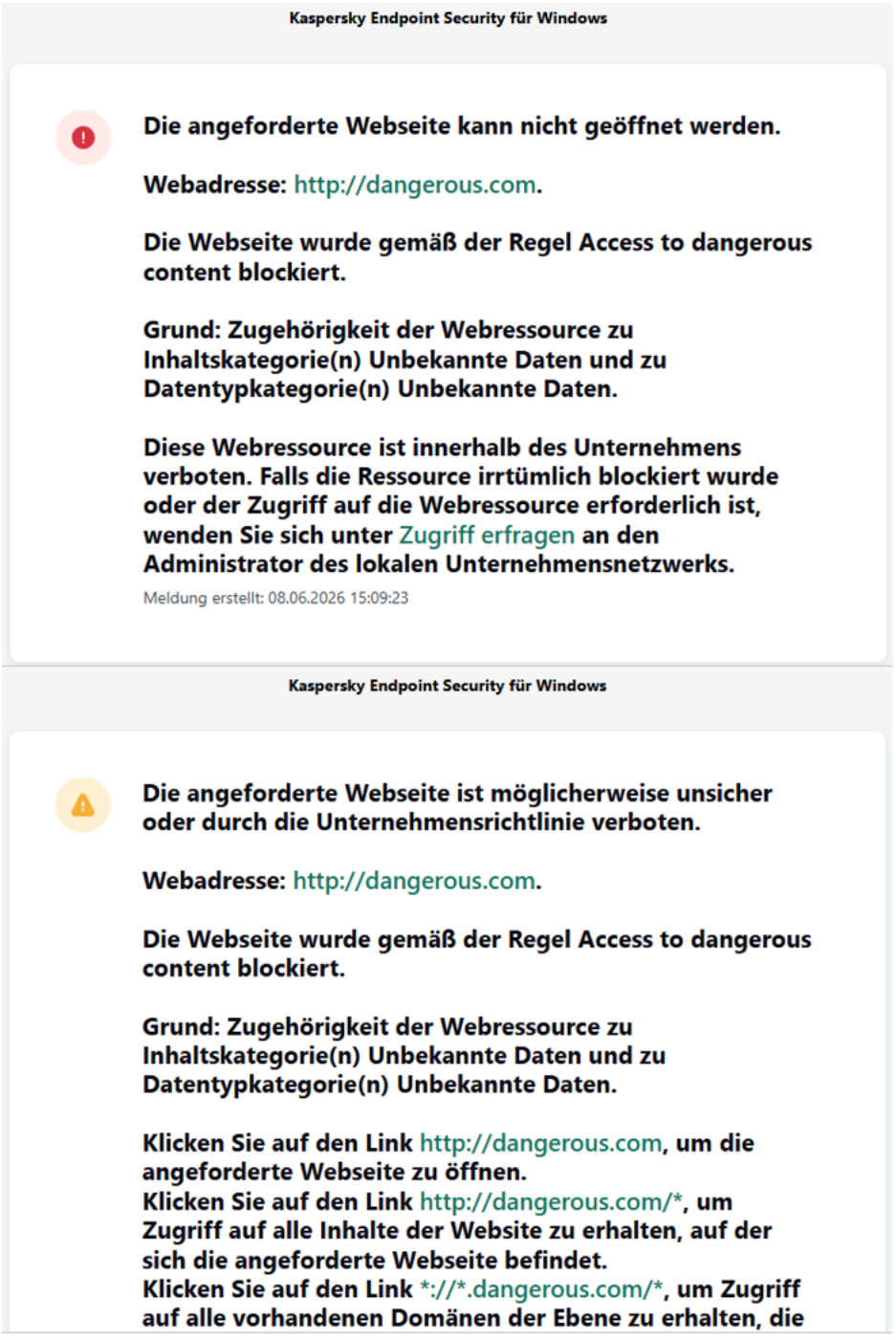
  Sie können beispielsweise den Internetzugriff über einen Browser für alle Unternehmensmitarbeiter beschränken, aber die IT-Abteilung ausnehmen.

- Zeitplan für die Regel.

  Sie können beispielsweise den Internetzugriff über einen Browser nur während der Arbeitszeit beschränken.

Prioritäten für Zugriffsregeln

Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, 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. Es kann beispielsweise vorkommen, dass Kaspersky Endpoint Security ein Unternehmensportal als soziales Netzwerk betrachtet. Um den Zugriff auf soziale Netzwerke zu beschränken und Zugriff auf das Web-Portal des Unternehmens zu gewähren, erstellen Sie zwei Regeln: eine Verbotsregel für die Website-Kategorie „*Soziale Netzwerke*“ und eine Erlaubnisregel für das Unternehmens-Web-Portal. Die Zugriffsregel für das Unternehmens-Web-Portal muss eine höhere Priorität haben als die Zugriffsregel für soziale Netzwerke.



Benachrichtigungen der „Web-Kontrolle“

Einstellung	Beschreibung
Regeln für den Zugriff auf Webressourcen	Liste der Zugriffsregeln für Webressourcen. Jede Regel besitzt eine Priorität. Je weiter oben eine Regel auf der Liste steht, 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.
Standardregel	Eine *Standardregel* ist eine Regel für den Zugriff auf Webressourcen, für die keine der Regeln gilt. Folgende Varianten stehen zur Auswahl: • **Alle erlauben, die nicht in der Regelliste angegeben sind**, auch bekannt als Denylist-Modus für verbotene Websites. • **Alle verbieten, die nicht in der Regelliste angegeben sind**, die auch als Allowlist-Modus für erlaubte Websites bekannt ist.
Aktive Browsersitzungen des Benutzers beenden, nachdem die Regel angewendet wurde	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.
Vorlagen	**Warnung**. Das Eingabefeld enthält eine Vorlage für die Meldung, die erscheint, wenn eine Regel ausgelöst wird, die vor einem Zugriffsversuch auf eine nicht empfehlenswerte Webressource warnt. **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 der Nachricht, die an den Administrator des lokalen Netzwerks gesendet wird, wenn der Zugriff nach Meinung des Benutzers irrtümlich blockiert wurde. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Zugriffsverbot auf Webseite**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse. Zum Erstellen von Nachrichtenvorlagen stehen spezielle Variablen zur Verfügung (z. B. `%USER_NAME%`). Wenn Sie Variablen verwenden, kann ein und dieselbe Nachrichtenvorlage für verschiedene Computer genutzt werden.
Das Öffnen erlaubter Seiten protokollieren	Kaspersky Endpoint Security protokolliert Daten über den Besuch aller Websites, einschließlich erlaubter Websites. Kaspersky Endpoint Security sendet Ereignisse an Kaspersky Security Center, an den lokalen Bericht für Kaspersky Endpoint Security, an das Windows-Ereignisprotokoll. 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.

Gerätekontrolle

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.

Wenn die Gerätekontrolle aktiviert ist, leitet das Programm Informationen über angeschlossene Geräte an Kaspersky Security Center weiter. Die Liste der verbundenen Geräte können Sie in Kaspersky Security Center im Ordner **Erweitert** → **Datenverwaltung** → **Hardware** ansehen.

Ebenen für den Zugriff auf Geräte

Die „Gerätekontrolle“ verwaltet den Zugriff auf folgenden Ebenen:

- **Gerätetyp**. Beispielsweise Drucker, Wechseldatenträger, CD/DVD-Laufwerke.

  Sie können den Zugriff auf Geräte wie folgt anpassen:

  - Erlauben – .
  - Blockieren – .
  - Nach Regeln (nur Drucker und tragbare Geräte) – .
  - Von Verbindungsschnittstelle abhängig (außer WLAN) – .
  - Verbieten mit Ausnahmen (nur WLAN) – .

- **Schnittstellen**. Mithilfe einer *Verbindungsschnittstelle* können Geräte mit einem Computer verbunden werden (z. B. via USB oder FireWire). Wenn der Modus **Von Verbindungsschnittstelle abhängig** für den Gerätetyp ausgewählt ist, erlaubt oder verbietet die App den Zugriff auf das Gerät abhängig von der Verbindungsschnittstelle (z. B. USB).

  Sie können den Zugriff auf Geräte wie folgt anpassen:

  - Erlauben – .
  - Blockieren – .

- **Vertrauenswürdige Geräte**. *Vertrauenswürdige Geräte* sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

  Sie können vertrauenswürdige Geräte mithilfe der folgenden Daten hinzufügen:

  - **Geräte nach 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.
  - **Geräte nach Modell**. Jedes Gerät besitzt eine Vendor ID (VID) und eine 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.

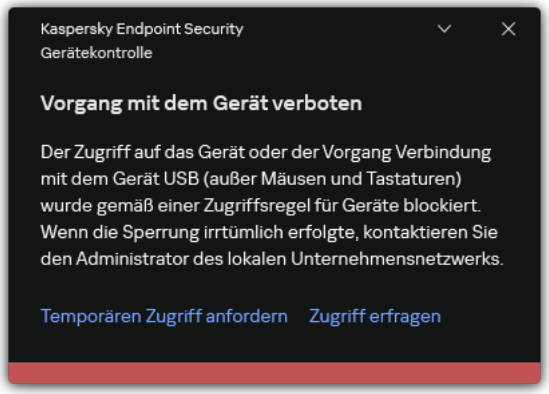
- **Geräte nach ID-Maske**. Wenn Sie mehrere Geräte mit ähnlichen IDs verwenden, können Sie Masken verwenden, um die Geräte zur Liste der vertrauenswürdigen Geräte hinzuzufügen. Das Zeichen `*` steht als Platzhalter für eine beliebige Zeichenkombination. Das Zeichen `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `WDC_C*`.

- **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 `?` wird bei der Angabe einer Maske von Kaspersky Endpoint Security nicht unterstützt. Beispiel: `VID_05AC&PID_*`.

Die „Gerätekontrolle“ verwendet *Zugriffsregeln*, um den Zugriff von Benutzern auf Geräte zu regulieren. Außerdem kann die „Gerätekontrolle“ Ereignisse über die Verbindung/Trennung von Geräten speichern. Damit Ereignisse gespeichert werden, müssen Sie in der Richtlinie das Senden von Ereignissen anpassen.

Falls der Zugriff auf das Gerät von der Schnittstelle abhängig ist (Status), werden Ereignisse über die Verbindung/Trennung des Geräts nicht von Kaspersky Endpoint Security gespeichert. Damit das Programm Kaspersky Endpoint Security Ereignisse über die Verbindung/Trennung des Geräts speichert, erlauben Sie den Zugriff auf den entsprechenden Gerätetyp (Status) oder fügen Sie das Gerät zur Liste der vertrauenswürdigen Geräte hinzu.

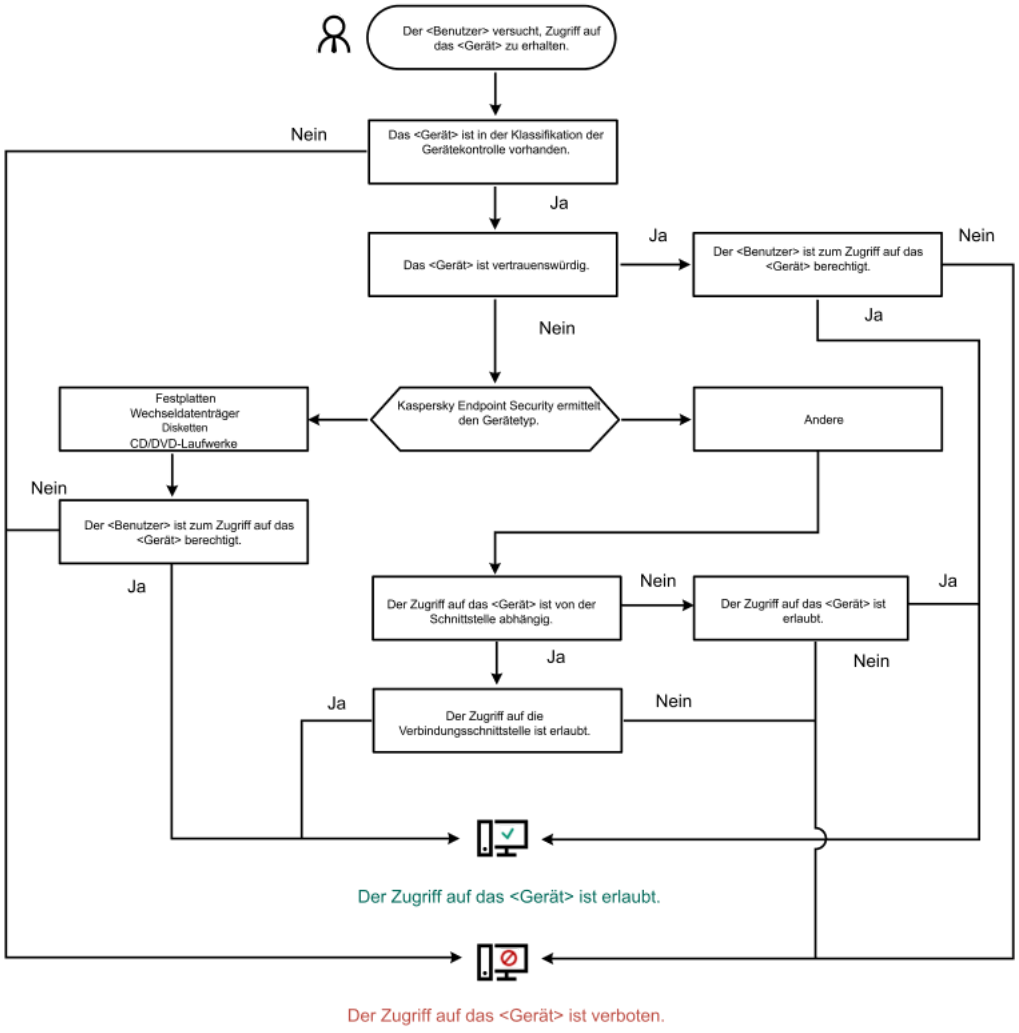
Wird mit dem Computer ein Gerät verbunden, auf das der Zugriff von der „Gerätekontrolle“ verboten ist, so blockiert Kaspersky Endpoint Security den Zugriff und zeigt eine Benachrichtigung an (s. Bild unten).



Benachrichtigung der „Gerätekontrolle“

Algorithmus der „Gerätekontrolle"

Kaspersky Endpoint Security entscheidet über den Zugriff auf ein Gerät, sobald dieses vom Benutzer an den Computer angeschlossen wird (s. folgende Abb.).



Algorithmus der „Gerätekontrolle"

Wenn ein Gerät verbunden ist und der Zugriff erlaubt ist, können Sie die Zugriffsregel ändern und den Zugriff verbieten. Wenn das nächste Mal auf das Gerät zugegriffen wird (Anzeige der Ordnerstruktur, Lesen, Schreiben), blockiert Kaspersky Endpoint Security den Zugriff. Geräte ohne Dateisystem werden erst blockiert, wenn sie zum nächsten Mal mit dem Computer verbunden werden.

Wenn der Benutzer eines Computers, auf dem das Programm Kaspersky Endpoint Security installiert ist, den Zugriff auf ein Gerät angefordert hat, das seiner Meinung nach irrtümlicherweise blockiert wurde, so übermitteln Sie ihm eine Anleitung für die Zugriffsanforderung.

Einstellung	Beschreibung
Anfragen auf temporären Zugriff erlauben *(nur in der Konsole von Kaspersky Security Center verfügbar)*	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.
Geräte und WLAN-Netzwerke	Tabelle mit allen verfügbaren Gerätetypen nach der Klassifikation der Komponente „Gerätekontrolle" und dem entsprechenden Zugriffsstatus.
Verbindungsschnittstellen	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.
Vertrauenswürdige Geräte	Liste der vertrauenswürdigen Geräte und Benutzer, denen der Zugriff auf diese Geräte erlaubt ist.
Bei Vererbung Werte zusammenführen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dadurch wird die Liste der vertrauenswürdigen Geräte in den übergeordneten und untergeordneten Richtlinien von Kaspersky Security Center zusammengeführt. Um Listen zusammenzuführen, muss die untergeordnete Richtlinie so konfiguriert werden, dass sie die Einstellungen der übergeordneten Richtlinie von Kaspersky Security Center erbt. Wenn das Kontrollkästchen aktiviert ist, werden Listenelemente aus der übergeordneten Richtlinie von Kaspersky Security Center in untergeordneten Richtlinien angezeigt. Auf diese Weise können Sie z. B. eine konsolidierte Liste der vertrauenswürdigen Geräte für das gesamte Unternehmen erstellen. Vererbte Listenelemente in einer untergeordneten Richtlinie können nicht gelöscht oder bearbeitet werden. Elemente in der Liste der vertrauenswürdigen Geräte, die während der Vererbung zusammengeführt werden, können nur in der übergeordneten Richtlinie gelöscht und bearbeitet werden. Sie können Listenelemente in untergeordneten Richtlinien hinzufügen, bearbeiten oder löschen. Wenn Elemente auf Listen der untergeordneten und übergeordneten Richtlinie übereinstimmen, werden diese Elemente als dasselbe Element der übergeordneten Richtlinie angezeigt. Wenn das Kontrollkästchen deaktiviert ist, werden die Elemente der Listen mit vertrauenswürdigen Geräten bei der Vererbung der Einstellungen der Richtlinien für Kaspersky Security Center nicht zusammengefasst. Mit dieser Funktionalität können Listen auch in Richtlinienprofilen zusammengeführt werden. Um Listen im Profil mit der höchsten Priorität zusammenzuführen, aktivieren Sie die Vererbung der Einstellungen aus einem Profil mit niedrigerer Priorität. Details über die Prioritäten von Richtlinienprofilen finden Sie in der Hilfe zu Kaspersky Security Center.
Anti-Bridging	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.
Vorlagen für Nachrichten	**Nachricht beim Blockieren**. 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. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Zugriffsverbot auf Gerät**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

Programmkontrolle

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 „Programmkontrolle“ wird mit folgenden Schritten angepasst:

1. Programmkategorien erstellen

   Der Administrator erstellt Kategorien für die Programme, die er verwalten möchte. Die Programmkategorien gelten unabhängig von der Administrationsgruppe für alle Computer des Unternehmensnetzwerks. Um eine Kategorie zu erstellen, können Sie beispielsweise folgende Kriterien verwenden: KL-Kategorie (z. B. *Browser* oder another category), Datei-Hash und Programmhersteller.

2. Programmkontrolle-Regeln erstellen.

   Der Administrator erstellt Regeln der „Programmkontrolle“ in der Richtlinie für die Administrationsgruppe. Eine Regel enthält Programmkategorien und einen Startstatus für die Programme aus diesen Kategorien: verboten oder erlaubt. 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.

3. Modus der „Programmkontrolle“ auswählen.

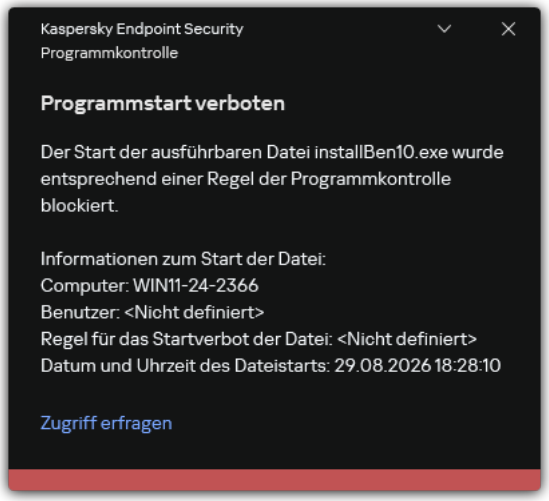
   Der Administrator wählt einen Modus für die Arbeit mit den Programmen aus, die zu keiner Regel gehören: Denyliste und Allowliste.

Wenn der Benutzer versucht, ein verbotenes Programm zu starten, blockiert Kaspersky Endpoint Security den Programmstart und zeigt eine Benachrichtigung an (s. Abb. unten).

Die Einstellungen der „Programmkontrolle“ können im *Testmodus* überprüft werden. In diesem Modus führt Kaspersky Endpoint Security die folgenden Aktionen aus:

- Der Start von Programmen (auch von verbotenen Programmen) wird erlaubt.
- Beim Start eines verbotenen Programms wird eine entsprechende Benachrichtigung angezeigt und Informationen werden zum Bericht auf dem Benutzercomputer Informationen hinzugefügt.

- Daten über den Start verbotener Programme werden an Kaspersky Security Center gesendet.



Benachrichtigung der „Programmkontrolle"

Modi der „Programmkontrolle"

Die Komponente „Programmkontrolle" bietet zwei Modi:

- **Deny-Liste**. In diesem Modus erlaubt die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" verboten sind.

  Dieser Modus ist für die Programmkontrolle standardmäßig ausgewählt.

- **Allow-Liste**. In diesem Modus verbietet die „Programmkontrolle" den Benutzern den Start beliebiger Programme, unter Ausnahme von Programmen, die durch Regeln der „Programmkontrolle" erlaubt und nicht verboten sind.

  Wenn eine extrem genaue Erlaubnisregel für die Programmkontrolle erstellt wurde, verbietet die Komponente den Start aller neuen Programme, die noch nicht vom Administrator des lokalen Unternehmensnetzwerks überprüft wurden, gewährleistet dabei aber die Funktionsfähigkeit des Betriebssystems und der bereits untersuchten Programme, die von Benutzern für dienstliche Zwecke benötigt werden.

  Beachten Sie die Tipps für die Anpassung von Regeln der Programmkontrolle im Allowlist-Modus.

Diese Modi für die Programmkontrolle können sowohl auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security als auch mithilfe von Kaspersky Security Center angepasst werden.

Allerdings verfügt Kaspersky Security Center über Tools, die auf der lokalen Benutzeroberfläche von Kaspersky Endpoint Security nicht verfügbar sind und für folgende Aufgaben dienen:

- Programmkategorien erstellen

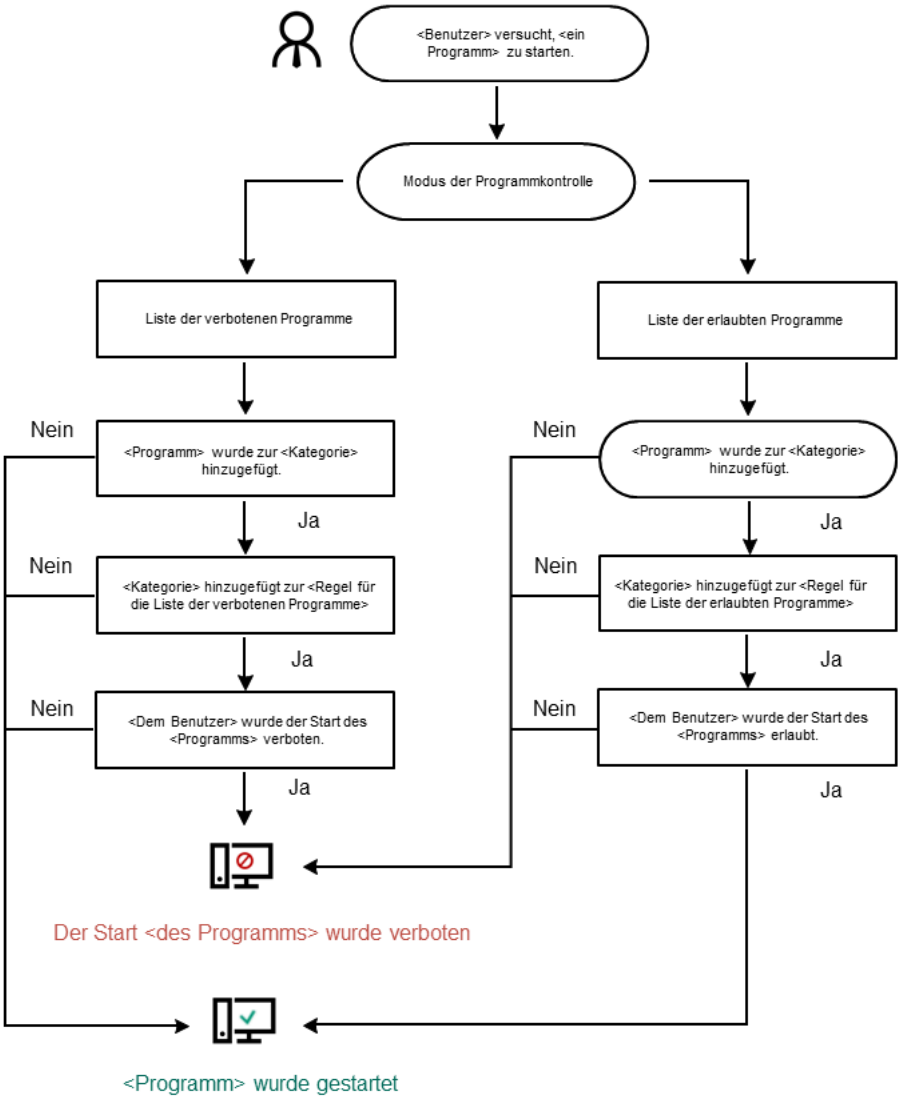
  Die Regeln der Programmkontrolle, die in der Verwaltungskonsole von Kaspersky Security Center erstellt wurden, beruhen auf den von Ihnen erstellten Programmkategorien, und nicht wie in der lokalen Benutzeroberfläche von Kaspersky Endpoint Security auf ein- und ausschließenden Bedingungen.

- Empfang von Informationen über die Programme, die auf den Computern des lokalen Unternehmensnetzwerks installiert sind

Deshalb wird empfohlen, die Komponente „Programmkontrolle" mithilfe von Kaspersky Security Center anzupassen.

Algorithmus der „Programmkontrolle”

Kaspersky Endpoint Security verwendet einen Algorithmus, um über den Start eines Programms zu entscheiden (s. Abb. unten).



Algorithmus der „Programmkontrolle”

Einstellung	Beschreibung
Aktion beim Start von Programmen, die durch Regeln blockiert werden	**Regeln anwenden**. Kaspersky Endpoint Security verwaltet den Programmstart gemäß dem ausgewählten Modus. **Regeln testen**. Kaspersky Endpoint Security erlaubt den Start des Programms, das im aktuellen Modus der Programmkontrolle verboten ist, und protokolliert Informationen über den Programmstart.
Modus „Kontrolle des Programmstarts"	Sie können zwischen folgenden Varianten wählen: • **Deny-Liste**. Bei Auswahl dieser Variante erlaubt die Programmkontrolle allen Benutzern den Start beliebiger Anwendungen. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Verbotsregeln der Programmkontrolle erfüllt sind. • **Allow-Liste**. Bei Auswahl dieser Variante verbietet die Programmkontrolle allen Benutzern den Start beliebiger Anwendungen. Als Ausnahmen gelten Fälle, in denen die Bedingungen von Erlaubnisregeln der Programmkontrolle erfüllt sind. Bei Auswahl des Modus **Allow-Liste** werden automatisch zwei Regeln für die Programmkontrolle erstellt: • **Goldene Kategorie**. • **Vertrauenswürdige Programme mit Update-Funktionen**. Automatisch erstellte Regeln können nicht geändert oder gelöscht werden. Sie können diese Regeln aktivieren oder deaktivieren.
Laden von DLL-Modulen überwachen	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.
Strenge Überprüfung von digitalen Signaturen verwenden	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.
Vorlagen für Nachrichten über Programmblockierung	**Nachricht beim Blockieren**. 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. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über Verbot des Programmstarts**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

Adaptive Kontrolle von Anomalien

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Die Komponente „Adaptive Kontrolle von Anomalien" überwacht und blockiert Aktionen, die für Computer des Unternehmensnetzwerks untypisch sind. Zur Überwachung von untypischen Aktionen verwendet die „Adaptive Kontrolle von Anomalien" eine Auswahl von Regeln (z. B. die Regel *Start von Windows PowerShell aus einem Office-Programm*). Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für schädliche Aktivitäten erstellt. Sie können ein Verhalten der „Adaptiven Kontrolle von Anomalien" für jede einzelne Regeln auswählen und beispielsweise den Start von PowerShell-Skripten erlauben, um die Lösung von Unternehmensaufgaben zu automatisieren. Kaspersky Endpoint Security aktualisiert den Regelsatz aus den Programm-Datenbanken. Die Aktualisierung des Regelsatzes muss manuell bestätigt werden.

„Adaptive Kontrolle von Anomalien" anpassen

Die Anpassung der „Adaptiven Kontrolle von Anomalien" umfasst folgende Schritte:

1. Training der „Adaptiven Kontrolle von Anomalien".

   Nachdem die „Adaptive Kontrolle von Anomalien" aktiviert ist, funktionieren die Regeln im *Lernmodus*. Im Verlauf des Trainings überwacht die „Adaptive Kontrolle von Anomalien" die Auslösung von Regeln und sendet Auslöseereignisse an Kaspersky Security Center. Jede Regel hat eine eigene Dauer für den Lernmodus. Die Dauer des Lernmodus wird von den Kaspersky-Experten vorgegeben. Gewöhnlich dauert der Lernmodus 2 Wochen.

   Wenn eine Regel während des Trainings nie ausgelöst wurde, betrachtet die „Adaptive Kontrolle von Anomalien" die mit dieser Regel verbundenen Aktionen als untypisch. Kaspersky Endpoint Security blockiert alle Aktionen, die mit dieser Regel zusammenhängen.

   Wenn während des Trainings eine Regel ausgelöst wurde, protokolliert Kaspersky Endpoint Security die Ereignisse im Bericht über ausgelöste Regeln und in der Datenverwaltung **Auslöser der Regel im Smart-Training-Status**.

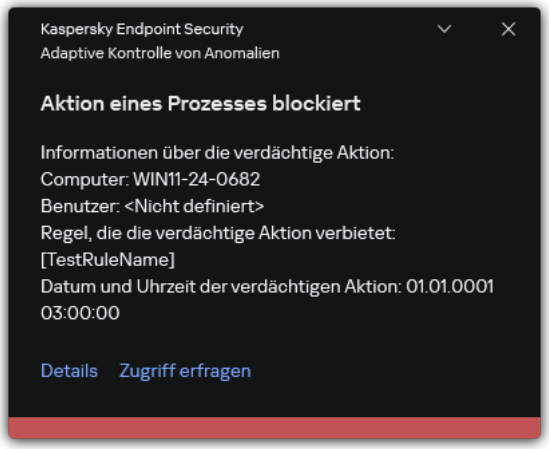
2. Analyse des Berichts über ausgelöste Regeln.

   Der Administrator analysiert den Bericht über ausgelöste Regeln oder den Inhalt der Datenverwaltung **Auslöser der Regel im Smart-Training-Status**. Anschließend kann der Administrator das Verhalten der „Adaptiven Kontrolle von Anomalien" bei einer Auslösung der Regel festlegen: blockieren oder erlauben. Außerdem kann der Administrator die Regelauslösung weiterhin überwachen und die Dauer des Lernmodus für das Programm verlängern. Ergreift der Administrator keine Maßnahmen, so läuft das Programm ebenfalls im Lernmodus weiter. Die Dauer des Lernmodus beginnt von vorne.

Die Adaptive Kontrolle von Anomalien über die folgenden Kanäle in Echtzeit konfiguriert werden:

- Die „Adaptive Kontrolle von Anomalien“ beginnt automatisch, jene Aktionen zu blockieren, die mit Regeln zusammenhängen, die im Lernmodus nicht ausgelöst wurden.
- Kaspersky Endpoint Security fügt neue Regeln hinzu oder löscht veraltete Regeln.
- Der Administrator analysiert den Bericht über ausgelöste Regeln und den Inhalt des Repositorys **Auslöser der Regel im Smart-Training-Status** und konfiguriert anschließend die „Adaptive Kontrolle von Anomalien“. Es wird empfohlen, den Bericht über ausgelöste Regeln und den Inhalt des Speichers **Auslöser der Regel im Smart-Training-Status** zu überprüfen.

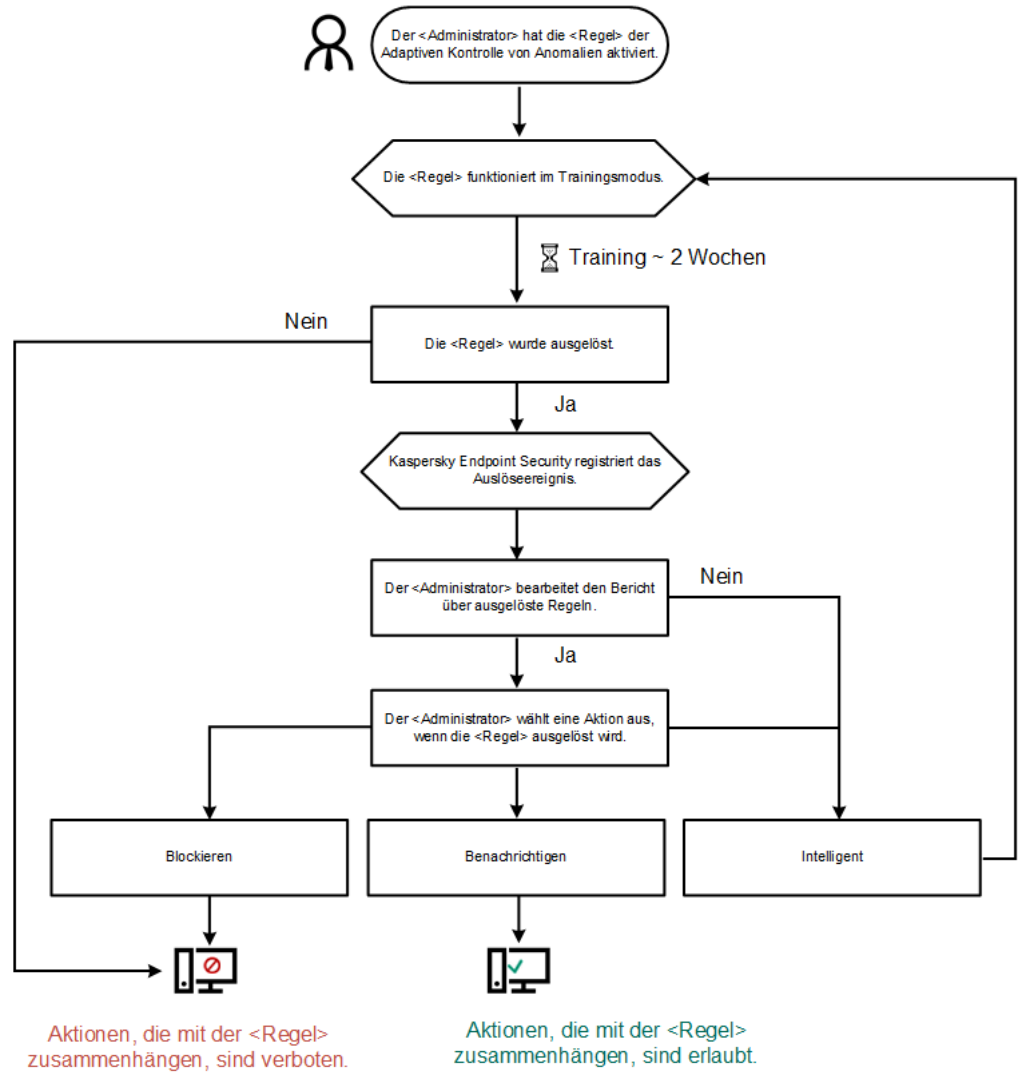
Wenn ein Schadprogramm versucht, eine Aktion auszuführen, blockiert Kaspersky Endpoint Security die Aktion und zeigt eine Benachrichtigung an (siehe Abbildung unten).



Benachrichtigung der „Adaptiven Kontrolle von Anomalien“

Algorithmus der „Adaptiven Kontrolle von Anomalien"

Um über die Ausführung einer Aktion, die mit einer Regeln verbunden ist, zu entscheiden, nutzt Kaspersky Endpoint Security den folgenden Algorithmus (siehe Abbildung unten).



Algorithmus der „Adaptiven Kontrolle von Anomalien"

Einstellungen der Komponente „Adaptive Kontrolle von Anomalien"

Einstellung	Beschreibung
Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien" *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dieser Bericht enthält Informationen zum Status der Erkennungsregeln der „Adaptiven Kontrolle von Anomalien" (z. B. *Deaktiviert* oder *Blockieren*). Der Bericht wird für alle Administrationsgruppen erstellt.
Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien" *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dieser Bericht enthält Informationen über untypische Aktionen, die mithilfe der „Adaptiven Kontrolle von Anomalien" erkannt wurden. Der Bericht wird für alle Administrationsgruppen erstellt.

Einstellung	Beschreibung
Regeln	Tabelle der Regeln der „Adaptiven Kontrolle von Anomalien“. Die Regeln wurden von den Kaspersky-Spezialisten auf Basis typischer Szenarien für schädliche Aktivitäten erstellt.
Vorlagen	**Nachricht beim Blockieren**. Vorlage der Nachricht an den Benutzer. Diese Nachricht wird angezeigt, wenn eine Regel der „Adaptiven Kontrolle von Anomalien“ ausgelöst wird, die eine untypische Aktion blockiert. **Nachricht an den Administrator**. Vorlage der Nachricht, die an den Administrator des lokalen Unternehmensnetzwerks gesendet wird, wenn eine Aktion nach Meinung des Benutzers irrtümlich blockiert wurde. Nachdem der Benutzer den Zugriff anfragt, sendet Kaspersky Endpoint Security ein Ereignis an Kaspersky Security Center: **Nachricht an den Administrator über das Verbot einer Programmaktion**. Die Ereignisbeschreibung enthält eine Nachricht an den Administrator mit ersetzten Variablen. Sie können diese Ereignisse in der Kaspersky Security Center-Konsole mithilfe der vordefinierten Ereignisauswahl **Benutzeranfragen** ansehen. Wenn Kaspersky Security Center in Ihrem Unternehmen nicht bereitgestellt wird oder keine Verbindung zum Administrationsserver besteht, sendet die App dem Administrator eine Nachricht an die angegebene E-Mail-Adresse.

Überwachung der Systemintegrität

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.

Ab Version 12.6 wird in Kaspersky Endpoint Security für Windows die Komponente „Überwachung der Datei-Integrität“ durch die Komponente „Überwachung der Systemintegrität“ ersetzt. Die Überwachung der Systemintegrität enthält alle Funktionen der Überwachung der Dateiintegrität und ermöglicht zusätzlich die Überwachung von Registrierungsänderungen und angeschlossenen Geräten.

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.

Echtzeitüberwachung der Systemintegrität

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.

Prüfung der Systemintegrität auf Befehl

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.

Einstellung	Beschreibung
Funktionsmodus für Sperr-Regeln	• **Verbieten**. In diesem Modus blockiert die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis. • **Informieren**. In diesem Modus erlaubt die Überwachung der Systemintegrität Aktionen, die mit Dateien und Registrierungsschlüsseln aus dem Überwachungsbereich erfolgen, und generiert ein entsprechendes Ereignis.
Echtzeitüberwachung der Systemintegrität	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.
Geräte überwachen	Die Überwachung der Systemintegrität überwacht das Verbinden und Trennen externer Geräte.
Dateien und Registrierung überwachen	Die Überwachung der Systemintegrität überwacht Änderungen an Dateien, Ordnern und der Registrierung.
Prüfung der Systemintegrität	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.

Endpoint Sensor

In Kaspersky Endpoint Security 11.4.0 ist die Komponente Endpoint Sensor nicht im Programm enthalten.

„Endpoint Sensor“ können Sie über die „Kaspersky Security Center Web Console“ und über die Verwaltungskonsole für Kaspersky Security Center verwalten. Endpoint Sensor kann nicht im Programm Kaspersky Security Center Cloud Console verwaltet werden.

Endpoint Sensor dient der Interaktion mit 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“.

Für die Verwaltung von Endpoint Sensor gelten die folgenden Besonderheiten:

- Wenn auf dem Computer das Programm Kaspersky Endpoint Security Versionen 11.0.0 – 11.3.0 installiert ist, können Sie die Einstellungen von Endpoint Sensor mithilfe einer Richtlinie anpassen. Weitere Informationen zum Anpassen der „Endpoint Sensor“-Einstellungen mithilfe einer Richtlinie finden Sie in der Hilfe für die vorhergehenden Versionen von Kaspersky Endpoint Security.
- Wenn auf dem Computer das Programm Kaspersky Endpoint Security Version 11.4.0 oder höher installiert ist, können die Einstellungen von Endpoint Sensor nicht mithilfe einer Richtlinie angepasst werden.

„Endpoint Sensor“ wird auf den Client-Computern installiert. Auf diesen Computern überwacht die Komponente permanent Prozesse, geöffnete Netzwerkverbindungen und veränderte Dateien. Endpoint Sensor überträgt Informationen an den KATA-Server.

Die Funktionalität der Komponente ist für die folgenden Betriebssysteme verfügbar:

- Windows 7 Service Pack 1 Home / Professional / Enterprise
- Windows 8.1.1 Professional / Enterprise
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-Bit)
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-Bit)

Ausführliche Informationen über die Funktionsweise von KATA finden Sie in der Hilfe zu „Kaspersky Anti Targeted Attack Platform“.

Sandbox

Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten zur Integration mit der Lösung Kaspersky Sandbox. 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.

Kaspersky Endpoint Security für Windows unterstützt ab Version 12.7 die Sandbox-Komponente, die Teil der Lösung Kaspersky Anti Targeted Attack Platform ist. Im Gegensatz zur Kaspersky Sandbox-Lösung können Dateien in der KATA Sandbox-Komponente nur manuell über das Kontextmenü einer Datei untersucht werden.

KATA Sandbox erfordert die Bereitstellung von Kaspersky Anti Targeted Attack Platform 7.0 höher.

Die Komponente kann nur über die „Kaspersky Security Center Web Console“ verwaltet werden. Sie können diese Komponente nicht mit der Verwaltungskonsole (MMC) verwalten.

Einstellungen der Komponente „Sandbox“

Einstellung	Beschreibung
Integrationsmodus	**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**.
Einstellungen der Serververbindung	**Timeout (ms)**. 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.
Verbindung mit Sandbox-Servern	**Kaspersky Sandbox**. Verbindungseinstellungen für die „Sandbox“-Server. Die Server verwenden bereitgestellte virtuelle Abbilder von Microsoft Windows-Betriebssystemen, um die zu untersuchenden Objekte auszuführen. Sie können eine IP-Adresse (IPv4 oder IPv6) oder einen vollständig qualifizierten Domänennamen angeben. **KATA Sandbox**. Einstellungen der Verbindung zum Central Node-Server. Central Node wählt die optimalen Untersuchungseinstellungen und verteilt die Last zwischen den Sandbox-Servern.
Aktion beim Fund einer Bedrohung	**Kopie in die Quarantäne verschieben, Objekt löschen**. Wenn diese Option ausgewählt ist, löscht Kaspersky Endpoint Security das auf dem Computer gefundene schädliche Objekt. Bevor das Objekts gelöscht wird, erstellt Kaspersky Endpoint Security eine Backup-Kopie für den Fall, dass das Objekt später wiederhergestellt werden muss. 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. Kaspersky Endpoint Security untersucht standardmäßig den Kernel-Speicher, die laufenden 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	**Bereiche mit kritischen Dateien**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security nur kritische Dateibereiche des Computers auf IOCs. Dazu zählen Kernel-Speicher und Bootsektoren. **Dateibereiche auf dem Systemlaufwerk des Computers**. Wenn diese Option ausgewählt ist, untersucht Kaspersky Endpoint Security das Systemlaufwerk des Computers auf IOCs.
IOC-Untersuchungsaufgabe ausführen	**Manuell**. In diesem Ausführungsmodus können Sie die Aufgabe *IOC-Untersuchung* zu einem geeigneten Zeitpunkt manuell starten. **Automatisch**. Ausführungsmodus, in dem Kaspersky Endpoint Security die Aufgabe *IOC-Untersuchung* automatisch ausführt, nachdem eine Bedrohung erkannt wurde. **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.

Managed Detection and Response

Kaspersky Endpoint Security für Windows 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“.

Einstellungen von Managed Detection and Response

Einstellung	Beschreibung
MDR-Konfigurationsdatei	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

Kaspersky Endpoint Security für Windows enthält einen integrierten Agenten für die Lösung Kaspersky Endpoint Detection and Response Optimum (im Folgenden auch „EDR Optimum“). Ab Version 11.8.0 enthält Kaspersky Endpoint Security für Windows einen integrierten Agenten für die Lösung Kaspersky Endpoint Detection and Response Expert (im Folgenden auch „EDR Expert“). *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. Im Vergleich zu „EDR Optimum“ bietet „EDR Expert“ eine erweiterte Funktionalität zur Überwachung von und zur Reaktion auf Bedrohungen. Einzelheiten zu diesen Lösungen finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

„Kaspersky Endpoint Detection and Response“ prüft und analysiert, wie sich eine Bedrohung entwickelt, und versorgt die *Sicherheitsabteilung* oder den *Administrator* mit Informationen über den möglichen Angriff, um eine rechtzeitige Reaktion zu ermöglichen. Kaspersky Endpoint Detection and Response (EDR) zeigt Alarm-Details in einem separaten Fenster an. Ein *Alarm* ist ein Ereignis in der Unternehmens-IT-Infrastruktur, das von der App als ungewöhnlich oder verdächtig eingestuft wurde und möglicherweise eine Sicherheitsbedrohung für die IT-Infrastruktur des Unternehmens darstellt. *Alarm-Details* ist ein Tool, mit dem alle über eine erkannte Bedrohung gesammelten Informationen angezeigt werden können. Zu den Alarm-Details gehört beispielsweise der Verlauf der auf dem Computer angezeigten Dateien. Einzelheiten zur Verwaltung der Alarm-Details finden Sie in der Hilfe zu „Kaspersky Endpoint Detection and Response Optimum“ und in der Hilfe zu „Kaspersky Endpoint Detection and Response Expert“.

Sie können die Komponente Endpoint Detection and Response Optimum in der Web Console und Cloud Console konfigurieren. Die Einstellungen der Komponente Endpoint Detection and Response Expert (cloud) sind nur in der Cloud Console verfügbar.

Einstellung	Beschreibung
Erweiterte Protokollierung der Systemaktivität aktivieren	Die erweiterte Telemetrie verbessert die Genauigkeit der IOC-Erkennung, erfordert jedoch mehr Computerressourcen. Für retrospektive IOC-Untersuchungen wird empfohlen die erweiterte Telemetrie auf dem Computer zu aktivieren. Die *retrospektive IOC-Untersuchung* ist ein Modus der Aufgabe *IOC-Untersuchung*. Dabei sucht Kaspersky Endpoint Security innerhalb eines bestimmten Zeitraums nach Kompromittierungsindikatoren. Dieser Modus ist für die Suche nach Kompromittierungsindikatoren anhand der Telemetrie des geschützten Computers vorgesehen (z. B. Netzwerkaktivität, Prozesse, Dateien und andere Telemetriedaten). Wenn die erweiterte Telemetrie deaktiviert ist, kann Kaspersky Endpoint Security die Informationen über gefundene Kompromittierungsindikatoren rotieren.
Netzwerkisolation	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 von Kaspersky Endpoint Security-Diensten initiiert werden. • Verbindungen, die vom Kaspersky Security Center-Administrationsagenten initiiert werden.
Isolation eines Geräts automatisch beenden nach (Std.)	Die Netzwerkisolation kann automatisch nach einem bestimmten Zeitraum deaktiviert werden oder manuell. Kaspersky Endpoint Security deaktiviert die Netzwerkisolation standardmäßig 5 Stunden nach Beginn der Isolierung.
Ausnahmen für die Netzwerkisolation	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	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 Ausführungsverhinderung unterstützt eine Reihe von Office-Dateierweiterungen und Skriptinterpretern. Um die Komponente Ausführungsprävention zu verwenden, müssen Sie die Regeln für die Ausführungsprävention hinzufügen. 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.
Aktion beim Ausführen oder Öffnen eines verbotenen Objekts	**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 die Anwendung im Windows-Ereignisprotokoll und im Kaspersky Security Center-Ereignisprotokoll ein Ereignis über Versuche, Objekte auszuführen oder Dokumente zu öffnen. **Dem Ereignisprotokoll hinzufügen**. In diesem Modus veröffentlicht Kaspersky Endpoint Security im Windows-Ereignisprotokoll 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. Standardmäßig ist dieser Modus ausgewählt.
Regeln zur Ausführungsprävention	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.

Einstellung	Beschreibung
Cloud Sandbox	Mit der Technologie *Cloud Sandbox* können Sie komplexe Bedrohungen auf einem Computer erkennen. Kaspersky Endpoint Security leitet erkannte Dateien automatisch zur Analyse an „Cloud Sandbox“ weiter. „Cloud Sandbox“ führt diese Dateien in einer isolierten Umgebung aus, um bösartige Aktivität zu erkennen, und entscheidet dann über ihre Reputation. 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. Die Technologie „Cloud Sandbox“ ist ständig aktiviert und steht allen Benutzern von Kaspersky Security Network zur Verfügung, unabhängig vom Typ der genutzten Lizenz. Wenn dieses Kontrollkästchen aktiviert ist, aktiviert Kaspersky Endpoint Security den Indikator für Bedrohungen, die mithilfe von „Cloud Sandbox“ erkannt wurden. Der Indikator befindet sich im Programmhauptfenster unter **Technologien zur Erkennung**. Kaspersky Endpoint Security verweist auch in Programmereignissen und im *Bericht über Bedrohungen* in der Kaspersky Security Center-Konsole auf die „Cloud Sandbox“-Bedrohungserkennungstechnologie.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security für Windows unterstützt die Integration in die Lösung Kaspersky Endpoint Detection and Response Expert (on-premises). *Kaspersky Endpoint Detection and Response Expert (on-premises)* ist eine Cybersicherheits-Lösung für Unternehmen. Mit den darin enthaltenen Kaspersky-Programmen kann sich ein Unternehmen vor den meisten Arten von Cyber-Risiken schützen und die wichtigsten Verbreitungsszenarien für Bedrohungen abdecken. Die Komponenten von EDR Expert (on-premises) werden auf der Open Single Management Platform (OSMP) bereitgestellt. Diese Plattform führt plattformübergreifende Szenarien auf einer einzigen Benutzeroberfläche aus und ermöglicht die Integration von Kaspersky-Programmen in Drittherstellerprogramme, um ein umfassendes Sicherheitssystem zu gestalten.

Eines der zentralen Elemente dieser Lösung ist *SIEM*. SIEM verfolgt Ereignisse, die von allen Komponenten stammen, und stellt mithilfe von Herstellerregeln und benutzerdefinierten Regeln Zusammenhänge zwischen diesen Ereignissen her. EDR Expert (on-premises) 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-premises) erfassten Ereignisse kombiniert, einschließlich der Ereignisse aus Kaspersky-Programmen und Informationssicherheitsprodukten von Drittanbietern.

Zur Reaktion auf komplexe Vorfälle verwendet EDR Expert (on-premises) vordefinierte und benutzerdefinierte Szenarien. Sie können auch Reaktionen aus Drittanbieter-Programmen sowie Reaktionsszenarien verwenden, an denen mehrere Programme beteiligt sind.

Endpoint Detection and Response (KATA)

Kaspersky Endpoint Security für Windows unterstützt die Arbeit mit der Komponente Kaspersky Endpoint 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.

Einstellungen für Endpoint Detection and Response Expert (on-premises)

Einstellung	Beschreibung
Verbindung mit Telemetrie-Erfassungsservern	Ein *Telemetrie-Erfassungsserver* ist Teil einer SIEM-Lösung, die Informationen über auf dem Computer auftretende Ereignisse sammelt, normalisiert, korreliert, analysiert und speichert. Konfigurieren Sie die folgenden Einstellungen, um eine Verbindung mit den Telemetrie-Erfassungsservern (KUMA) herzustellen: • **Timeout (Sek.)**. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden. • **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers 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. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Nachdem Sie die Server-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.
Adresse und **Port** (Telemetrie-Erfassungsserver)	Einstellungen für die Verbindung mit Telemetrie-Erfassungsservern. Sie können eine IP-Adresse eingeben (IPv4 oder IPv6). Sie können mehrere Adressen für 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.
Telemetrie an Telemetrie-Erfassungsserver senden	Mit dieser Funktionalität können Sie das Senden von Telemetriedaten an den KATA-Server vollständig deaktivieren. 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**. 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.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden. • **Anzahl der Ereignispakete pro Übertragung beschränken**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse. Mit dieser Funktion können Sie die Pufferung von Ereignissen vor der Synchronisierung mit dem Server deaktivieren.

Einstellung	Beschreibung
Anforderungsbegrenzung aktivieren	Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Konfigurieren Sie die Telemetrie-Einstellungen: • **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen. • **Prozentsatz für die Überschreitung des Ereignislimits**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.
Synchronisierungsanfrage an Server senden alle (Min.)	Häufigkeit der an den Server gesendeten Synchronisierungsanfragen. Während der Synchronisierung sendet Kaspersky Endpoint Security Informationen über geänderte Einstellungen und Aufgaben der App.
Verbindung mit Reaktionsservern	Ein *Reaktionsserver* ist ein Server, der Daten empfängt und sendet, das Verhalten von Objekten analysiert und die Ergebnisse solcher Untersuchungen veröffentlicht. Konfigurieren Sie die folgenden Einstellungen für die Verbindung zu Reaktionsservern: • **Timeout (Sek.)**. Maximales Timeout für den Reaktionsserver. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Server zu verbinden. • **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Server. Sie können ein TLS-Zertifikat von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Herstellen einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Servers 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. Sie können einen Krypto-Container von der Open Single Management Plattform abrufen (siehe Anweisungen in der Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises)). Nachdem Sie die Server-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden.
Adresse und **Port** (Reaktionsserver)	Einstellungen für die Verbindung mit Reaktionsservern. Sie können eine IP-Adresse eingeben (IPv4 oder IPv6). Sie können mehrere Adressen für 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.

Einstellung	Beschreibung
Synchronisierungsanfrage an Server senden alle (Min.)	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	Konfigurieren Sie die folgenden Einstellungen für die Verbindung zum Central Node-Server: • **Timeout (Sek.)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden. • **Serverzertifikat**. TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem Central Node-Server. Ein TLS-Zertifikat können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). • **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Endpoint Security und dem Central Node-Server. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen des Central Node-Servers aktivieren, dann einen Krypto-Container anfordern und ein Kennwort festlegen, um den Krypto-Container zu schützen. Ein *Krypto-Container* ist ein PFX-Archiv mit einem Zertifikat und einem privaten Schlüssel. Einen Krypto-Container können Sie in der Konsole von Kaspersky Anti Targeted Attack Platform anfordern (siehe Anleitung in der Hilfe zu Kaspersky Anti Targeted Attack Platform). Nachdem Sie die Central Node-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung in den Einstellungen von Kaspersky Endpoint Security aktivieren und einen kennwortgeschützten Krypto-Container laden. Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.
Adresse und **Port** (KATA-Server)	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.
Telemetriedaten an KATA senden	Mit dieser Funktionalität können Sie das Senden von Telemetriedaten an den KATA-Server vollständig deaktivieren. 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. Konfigurieren Sie die Telemetrie-Einstellungen: • **Maximale Verzögerung der Ereignisübertragung (Sek.)**. Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden. • **Maximale Anzahl der Ereignispakete**. Das Programm synchronisiert sich mit dem Server, wenn sich genügend Ereignisse im Puffer befinden. Der Standardwert beträgt 1.024 Ereignisse.
Anforderungsbegrenzung aktivieren	Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. Wenn die Anzahl der Ereignisse die festgelegten Grenzwerte überschreitet, beendet Kaspersky Endpoint Security das Senden von Ereignissen. Konfigurieren Sie die Telemetrie-Einstellungen: • **Maximale Anzahl von Ereignissen pro Stunde**. Die App analysiert den Telemetriedatenstrom und schränkt das Senden von Ereignissen ein, wenn der Ereignisstrom das festgelegte Limit für Ereignisse pro Stunde überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen nach einer Stunde fort. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen. • **Prozentsatz für die Überschreitung des Ereignislimits**. Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

Network Detection and Response (KATA)

Kaspersky Endpoint Security für Windows 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.

Einstellungen für Network Detection and Response (KATA)

Einstellung	Beschreibung
Einstellungen der Serververbindung	**Timeout (Sek)**. Maximale Zeitüberschreitung für die Antwort von Central Node. Nach Ablauf des Timeouts versucht Kaspersky Endpoint Security, sich mit einem anderen Central Node-Server zu verbinden. **TLS-Zertifikat des Servers**. 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.
Adresse und **Port**	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.

Einstellung	Beschreibung
Synchronisierungsanfrage an NDR-Server senden alle (Min.)	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.)	Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
Anforderungsbegrenzung aktivieren	Durch diese Funktion wird die Auslastung des Computers optimiert. Wenn diese Funktion aktiviert ist, schränkt das Programm die Ereignisübertragung ein. 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. Die Standardeinstellung ist 3.000 Ereignisse pro Stunde. Wenn die App auf einem Server installiert ist, ist der Telemetrie-Datenstrom höher. Für Server wird empfohlen, den Wert auf 60.000 Ereignisse pro Stunde zu erhöhen.
Prozentsatz für die Überschreitung des Ereignislimits	Die App sortiert Ereignisse nach Typ (z. B. Ereignisse des Typs „Änderungen in der Registrierung“) und schränkt die Übertragung von Ereignissen ein, wenn das Verhältnis von Ereignissen desselben Typs zur Gesamtzahl von Ereignissen den in Prozent festgelegten Grenzwert überschreitet. Kaspersky Endpoint Security setzt das Senden von Ereignissen fort, wenn das Verhältnis der anderen Ereignisse zur Gesamtzahl der Ereignisse wieder dem Grenzwert entspricht. Die Standardeinstellung ist 15%.

KUMA-Integration

Kaspersky Endpoint Security für Windows 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.

Einstellungen der KUMA-Integration

Einstellung	Beschreibung
Maximale Verzögerung beim Versenden von Ereignissen (Sek.)	Die App synchronisiert sich mit dem Server, um Ereignisse nach Ablauf des Synchronisierungsintervalls zu senden. Der Standardwert ist 30 Sekunden.
Verbindung mit KUMA-Servern	**Timeout (Sek.)**. Die maximale Wartezeit auf eine Antwort vom KUMA-Server (standardmäßig beträgt der Wert 5 Sekunden). 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. Sie können ein TLS-Zertifikat in der Konsole von Kaspersky Unified Monitoring and Analysis Platform abrufen (siehe Anleitung in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). Um eine vertrauenswürdige Verbindung herzustellen, müssen Sie in der KUMA-Konsole in den TCP-Konnektor-Einstellungen den TLS-Modus **With verification** auswählen (siehe Einstellungen für den TCP-Konnektor in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). **Zwei-Wege-Authentifizierung verwenden**. Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen KES und KUMA. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie in der KUMA-Konsole in den Konnektor-Einstellungen den TLS-Modus **Custom PFX with client authentication** auswählen (siehe Konnektor-Einstellungen in der Hilfe zu Kaspersky Unified Monitoring and Analysis Platform). Anschließend müssen Sie ein Serverzertifikat herunterladen und ein Kennwort zum Schutz des Krypto-Containers festlegen. Der Krypto-Container muss kennwortgeschützt sein. Ein Krypto-Container mit einem leeren Passwort kann nicht hinzugefügt werden.
KUMA-Server	Einstellungen der Verbindung mit den Servern von Kaspersky Unified Monitoring and Analysis Platform. Sie können eine IP-Adresse eingeben (IPv4 oder IPv6). Sie können mehrere Adressen für KUMA-Server 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.

Vollständige Festplattenverschlüsselung

Sie können ein Verschlüsselungsverfahren auswählen: Kaspersky-Festplattenverschlüsselung oder BitLocker-Laufwerkverschlüsselung (im Folgenden auch „BitLocker“ genannt).

Kaspersky-Festplattenverschlüsselung

Die Kaspersky-Festplattenverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

Nach der Verschlüsselung von Systemfestplatten und einem nachfolgenden Neustart des Computers, sind der Zugriff auf die Festplatten und das Laden des Betriebssystems erst möglich, nachdem der Benutzer sich mithilfe des Authentifizierungsagenten authentifiziert hat. Dazu ist entweder die Eingabe des Kennworts für den Token oder die Smartcard, die mit dem Computer verbunden sind, oder die Eingabe des Namens und Kennworts für das Authentifizierungsagenten-Benutzerkonto erforderlich, das vom Systemadministrator des lokalen Unternehmensnetzwerks mithilfe der Aufgabe *Authentifizierungsagenten-Konten verwalten* erstellt wurde. Diese Konten basieren auf den Benutzerkonten von Microsoft Windows, mit denen sich die Benutzer im Betriebssystem anmelden. Sie können auch die Technologie Single Sign-On (SSO) verwenden. Diese ermöglicht eine automatische Anmeldung im Betriebssystem mit dem Benutzernamen und dem Kennwort des Authentifizierungsagenten-Benutzerkontos.

Es gibt zwei Methoden, mit denen sich der Benutzer im Authentifizierungsagenten authentifizieren kann:

- Durch Eingabe von Name und Kennwort eines Benutzerkontos für den Authentifizierungsagenten, wenn das Benutzerkonto vom Administrator des lokalen Unternehmensnetzwerks mit Mitteln von Kaspersky Security Center erstellt wurde.
- Durch Eingabe des Kennworts für einen Token oder eine Smartcard, die mit dem Computer verbunden sind.

  Ein Token oder eine Smartcard kann nur verwendet werden, wenn die Festplatten des Computers mithilfe des AES256-Verschlüsselungsalgorithmus verschlüsselt sind. Sind die Festplatten des Computers mithilfe des AES56-Verschlüsselungsalgorithmus verschlüsselt, so kann dem Befehl keine elektronische Zertifikatdatei hinzugefügt werden.

BitLocker-Laufwerkverschlüsselung

BitLocker ist eine integrierte Verschlüsselungstechnologie des Windows-Betriebssystems.
Kaspersky Endpoint Security ermöglicht es, BitLocker mithilfe der Infrastruktur von Kaspersky Next zu kontrollieren und zu verwalten. BitLocker verschlüsselt ein logisches Volume. Wechseldatenträger können mithilfe von BitLocker nicht verschlüsselt werden. Details über BitLocker finden Sie in der Microsoft-Dokumentation.

Wenn der Datenträger verschlüsselt wird, legt BitLocker den Bootloader und andere Hilfsdateien in der system partition ab. Diese Partition ist nicht verschlüsselt. Die Systempartition wird vom Betriebssystem automatisch während der Windows-Installation erstellt. Wenn die Festplatte vor der Windows-Installation vollständig partitioniert ist, kann das Betriebssystem keine Systempartition erstellen. In diesem Fall werden Sie beim

Starten der BitLocker-Festplattenverschlüsselung vom Betriebssystem aufgefordert, das Laufwerk neu zu partitionieren und eine Systempartition zu erstellen. Nachdem eine Systempartition erstellt wurde, startet das Betriebssystem die BitLocker-Verschlüsselung.

Die Sicherheit beim Speichern von Zugriffsschlüsseln gewährleistet BitLocker mithilfe von Trusted Platform Module. *Trusted Platform Module* (TMP) ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Ein Trusted Platform Module wird normalerweise auf der Hauptplatine des Computers installiert und interagiert mit allen anderen Systemkomponenten über die Hardwareschnittstelle. Die Verwendung des TPM ist die sicherste Art, BitLocker-Zugriffsschlüssel zu speichern, da das TPM eine Überprüfung der Systemintegrität vor dem Systemstart ermöglicht. Auf Computern ohne TPM können Sie Laufwerke verschlüsseln. Dabei wird der Zugriffsschlüssel mit einem Kennwort verschlüsselt. BitLocker verwendet die folgenden Authentifizierungsmethoden:

- TPM.
- TPM und PIN-Code.
- Kennwort.

Nachdem die Systemfestplatte verschlüsselt wurde, von der das Betriebssystem gestartet wird, muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach der Authentifizierung erlaubt BitLocker dem Benutzer die Anmeldung. Die Single-Sign-On-Technologie (SSO) wird von BitLocker nicht unterstützt.

Nach der Laufwerkverschlüsselung erstellt BitLocker einen Wiederherstellungsschlüssel. Kaspersky Endpoint Security sendet den Wiederherstellungsschlüssel an Kaspersky Security Center, damit Sie den Zugriff auf das Laufwerk wiederherstellen können (beispielsweise wenn ein Benutzer sein Kennwort vergessen hat).

Wenn ein Benutzer ein Laufwerk mithilfe von BitLocker verschlüsselt, sendet Kaspersky Endpoint Security den Wiederherstellungsschlüssel und Informationen über die Festplattenverschlüsselung an Kaspersky Security Center.

Wenn Sie Gruppenrichtlinien für Windows verwenden, deaktivieren Sie die BitLocker-Verwaltung in den Richtlinieneinstellungen. Es kann sein, dass die Windows-Richtlinieneinstellungen den Richtlinieneinstellungen von Kaspersky Endpoint Security widersprechen. Bei einer Laufwerksverschlüsselung könnten deshalb Fehler auftreten.

Einstellungen der Komponente „Kaspersky-Festplattenverschlüsselung"

Einstellung	Beschreibung
Verschlüsselungsmodus	**Alle Festplatten verschlüsseln**. Ist diese Option ausgewählt und die Richtlinie wird übernommen, so verschlüsselt das Programm alle Festplatten. Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem das Programm installiert ist. **Alle Festplatten entschlüsseln**. Ist diese Option ausgewählt und die Richtlinie wird übernommen, so entschlüsselt das Programm alle zuvor verschlüsselten Festplatten. **Nicht verändern**. Ist dieses Elements gewählt und die Richtlinie wird übernommen, so verbleiben die Laufwerke in ihrem ursprünglichen Zustand. Wenn das Laufwerk verschlüsselt wurde, bleibt es verschlüsselt. Wenn das Laufwerk entschlüsselt wurde, bleibt es entschlüsselt. Dieses Element ist standardmäßig ausgewählt.
Während der Verschlüsselung die Authentifizierungsagenten-Konten für Windows-Benutzer automatisch erstellen	Wenn dieses Kontrollkästchen aktiviert ist, erstellt das Programm Benutzerkonten des Authentifizierungsagenten basierend auf der Liste der Windows-Benutzerkonten auf dem Computer. Kaspersky Endpoint Security verwendet standardmäßig alle lokalen und Domänen-Benutzerkonten, mit denen sich der Benutzer in den letzten 30 Tagen am Betriebssystem angemeldet hat.

Einstellung	Beschreibung
Einstellungen zum Erstellen von Authentifizierungsagenten-Konten	**Alle Benutzerkonten des Computers**. Alle Benutzerkonten auf dem Computer, die zu irgendeinem Zeitpunkt aktiv waren. **Alle Domänenkonten des Computers**. Alle Benutzerkonten auf dem Computer, die zu einer Domäne gehören und die zu irgendeinem Zeitpunkt aktiv waren. **Alle lokalen Benutzerkonten des Computers**. Alle lokalen Benutzerkonten auf dem Computer, die zu irgendeinem Zeitpunkt aktiv waren. **Dienstkonto mit Einmalkennwort**. Das Dienstkonto wird beispielsweise benötigt, um Zugriff auf den Computer zu erhalten, wenn der Benutzer das Kennwort vergisst. Sie können das Dienstkonto auch als Reservekonto verwenden. Sie müssen den Namen des Benutzerkontos eingeben (Standardwert `ServiceAccount`). Kaspersky Endpoint Security erstellt automatisch ein Kennwort. Das Kennwort finden Sie in der Kaspersky Security Center-Konsole. **Lokaler Administrator**. Kaspersky Endpoint Security erstellt ein Authentifizierungsagenten-Konto für den lokalen Administrator des Computers. **Manager des Computers**. Kaspersky Endpoint Security erstellt ein Authentifizierungsagenten-Konto für das Benutzerkonto des Computermanagers. Welches Benutzerkonto die Rolle „Computermanager“ hat, können Sie in den Active Directory-Computereigenschaften nachsehen. Standardmäßig ist die Rolle „Computermanager“ nicht definiert, d. h. diese Rolle entspricht keinem Benutzerkonto. **Aktives Benutzerkonto**. Kaspersky Endpoint Security erstellt automatisch ein Authentifizierungsagenten-Konto für das Benutzerkonto, das zum Zeitpunkt der Festplattenverschlüsselung aktiv ist.
Bei der Anmeldung die Authentifizierungsagenten-Konten für alle Benutzer dieses Computers automatisch erstellen	Wenn dieses Kontrollkästchen aktiviert ist, überprüft das Programm Informationen zu Windows-Benutzerkonten auf dem Computer, bevor der Authentifizierungsagent gestartet wird. Wenn Kaspersky Endpoint Security ein Windows-Benutzerkonto erkennt, das kein Benutzerkonto des Authentifizierungsagenten besitzt, erstellt das Programm ein neues Konto für den Zugriff auf verschlüsselte Laufwerke. Das neue Benutzerkonto des Authentifizierungsagenten verfügt über die folgenden Standardeinstellungen: nur kennwortgeschützte Anmeldung, Kennwortänderung bei der ersten Authentifizierung. Es ist also nicht nötig, für Computer mit bereits verschlüsselten Laufwerken mithilfe der Aufgabe *Authentifizierungsagenten-Konten verwalten* manuell Authentifizierungsagenten-Benutzerkonten hinzuzufügen.
Benutzername speichern, der im Authentifizierungsagenten eingegeben wurde	Wenn das Kontrollkästchen aktiviert ist, speichert das Programm den Namen des Authentifizierungsagenten-Kontos. Wenn im Authentifizierungsagenten das nächste Mal eine Authentifizierung mit demselben Benutzerkonto erfolgt, muss der Benutzername nicht eingegeben werden.
Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt. Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Das Kontrollkästchen ist standardmäßig deaktiviert.

Einstellung	Beschreibung
Legacy USB Support verwenden (nicht empfohlen)	Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktionalität Legacy USB Support. *Legacy USB Support* **ist eine** BIOS-/UEFI-Funktion, die es ermöglicht, USB-Geräte (z. B. ein Token) zu verwenden, wenn der Computer gestartet wird und das Betriebssystem noch nicht gestartet wurde (BIOS-Modus). Nach dem Start des Betriebssystems beeinflusst die Funktion „Legacy USB Support" die Unterstützung von USB-Geräten nicht mehr. Ist das Kontrollkästchen aktiviert, so wird die Unterstützung von USB-Geräten zu Beginn des Startvorgangs des Computers aktiviert. Wenn die Funktion Legacy USB Support aktiviert ist, unterstützt der Authentifizierungsagent im BIOS-Modus die Verwendung von USB-Tokens nicht. Die Funktion sollte nur beim Auftreten von Hardware-Kompatibilitätsproblemen verwendet werden und ausschließlich für jene Computer aktiviert werden, auf welchen das Problem aufgetreten ist.
Einstellungen für Kennwörter	Einstellungen für die Stärke des Kennworts für ein Authentifizierungsagenten-Benutzerkonto Wenn das Verfahren zur Einmalanmeldung verwendet wird, ignoriert der Authentifizierungsagent die Anforderungen an die Kennwortkomplexität, die in Kaspersky Security Center festgelegt sind. Die Anforderungen an die Kennwortkomplexität können Sie in den Betriebssystemeinstellungen festlegen.
Technologie zur Einmalanmeldung (SSO) verwenden	Die Technologie zur Einmalanmeldung erlaubt es, die gleichen Anmeldedaten für den Zugriff auf verschlüsselte Festplatten und für die Anmeldung am Betriebssystem zu verwenden. Ist das Kontrollkästchen aktiviert, so müssen für den Zugriff auf verschlüsselte Festplatten und für die nachfolgende automatische Anmeldung am Betriebssystem die Anmeldedaten für den Zugriff auf die verschlüsselten Datenträger eingegeben werden. Ist das Kontrollkästchen deaktiviert, so müssen für den Zugriff auf verschlüsselte Festplatten und für die nachfolgende Anmeldung am Betriebssystem die Anmeldedaten für den Zugriff auf verschlüsselte Festplatten und die Anmeldedaten des Benutzers im Betriebssystem separat eingegeben werden.
Anmeldedaten von Drittanbietern verpacken	Kaspersky Endpoint Security unterstützt den Drittanbieter für Anmeldeinformationen ADSelfService Plus. Bei der Verwendung von Drittanbietern für Anmeldeinformationen fängt der Authentifizierungsagent das Kennwort ab, bevor das Betriebssystem geladen wird: Der Benutzer muss sein Kennwort also nur ein einziges Mal eingeben, und zwar bei der Windows-Anmeldung. Nach der Anmeldung bei Windows kann der Benutzer die Optionen des Drittanbieters für Anmeldeinformationen nutzen, z. B. für die Anmeldung bei Unternehmensdiensten. Drittanbieter für Anmeldeinformationen bieten Benutzern auch die Möglichkeit, ihre Kennwörter unabhängig zurückzusetzen. In diesem Fall aktualisiert Kaspersky Endpoint Security automatisch das Kennwort für den Authentifizierungsagenten. Wenn Sie einen Drittanbieter für Anmeldeinformationen verwenden, der vom Programm nicht unterstützt wird, sind die Funktionen der Einmalanmeldung möglicherweise eingeschränkt.
Hilfe	**Authentifizierung**. Hilfetext, der im Fenster des Authentifizierungsagenten angezeigt wird, wenn die Anmeldedaten eingegeben werden. **Kennwort ändern**. Hilfetext, der im Fenster des Authentifizierungsagenten angezeigt wird, wenn das Kennwort für das Authentifizierungsagenten-Benutzerkonto geändert wird. **Kennwort wiederherstellen**. Hilfetext, der im Fenster des Authentifizierungsagenten angezeigt wird, wenn das Kennwort für das Authentifizierungsagenten-Benutzerkonto wiederhergestellt wird.

Einstellungen der Komponente „BitLocker-Laufwerkverschlüsselung"

Einstellung	Beschreibung
Verschlüsselungsmodus	**Alle Festplatten verschlüsseln**. Ist diese Option ausgewählt und die Richtlinie wird übernommen, so verschlüsselt das Programm alle Festplatten. Wenn auf dem Computer mehrere Betriebssysteme installiert sind, können Sie nach der Verschlüsselung nur jenes Betriebssystem ausführen, in welchem das Programm installiert ist. **Alle Festplatten entschlüsseln**. Ist diese Option ausgewählt und die Richtlinie wird übernommen, so entschlüsselt das Programm alle zuvor verschlüsselten Festplatten. **Nicht verändern**. Ist dieses Elements gewählt und die Richtlinie wird übernommen, so verbleiben die Laufwerke in ihrem ursprünglichen Zustand. Wenn das Laufwerk verschlüsselt wurde, bleibt es verschlüsselt. Wenn das Laufwerk entschlüsselt wurde, bleibt es entschlüsselt. Dieses Element ist standardmäßig ausgewählt.

Einstellung	Beschreibung
Verwendung der BitLocker-Authentifizierung aktivieren, die Preboot-Tastatureingaben auf Tablets erfordert	Verwendung einer Authentifizierung, die eine Dateneingabe in einer Preboot-Umgebung selbst dann erfordert, wenn die Plattform keine Option zur Preboot-Eingabe bietet (beispielsweise mit Touchscreen-Tastaturen auf Tablets). Das Touchpad von Tablets ist in der Preboot-Umgebung nicht verfügbar. Um die BitLocker-Authentifizierung auf Tablets auszuführen, muss der Benutzer beispielsweise eine USB-Tastatur anschließen. Ist das Kontrollkästchen aktiviert, so wird die Verwendung der Authentifizierung erlaubt, wenn sie eine Preboot-Tastatureingabe erfordert. Es wird empfohlen, diese Einstellung nur für Geräte zu verwenden, die in einer Preboot-Umgebung alternative Dateneingabemethoden anbieten (z. B. eine USB-Tastatur zusätzlich zu einer Touchscreen-Tastatur). Wenn das Kontrollkästchen deaktiviert ist, ist die BitLocker-Laufwerkverschlüsselung auf Tablets nicht möglich.
Hardwareverschlüsselung verwenden (Windows 8 und höher)	Ist das Kontrollkästchen aktiviert, so verwendet das Programm die Hardwareverschlüsselung. Dadurch wird erlaubt, die Verschlüsselung zu beschleunigen und die Auslastung der Computerressourcen zu reduzieren.
Nur belegten Speicherplatz verschlüsseln (Windows 8 und höher)	Das Kontrollkästchen aktiviert/deaktiviert eine Funktion, mit welcher der Verschlüsselungsbereich auf die belegten Sektoren einer Festplatte beschränkt wird. Mit dieser Beschränkung kann die Verschlüsselung beschleunigt werden. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln (reduziert die Verschlüsselungsdauer)** nach dem Start der Verschlüsselung aktiviert oder deaktiviert wird, wird die geänderte Einstellung erst wirksam, wenn die Festplatten entschlüsselt werden. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden. Ist das Kontrollkästchen aktiviert, so wird nur jener Teil einer Festplatte verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist das Kontrollkästchen deaktiviert, so wird die gesamte Festplatte verschlüsselt. Dabei werden auch Fragmente von bereits gelöschten oder geänderten Dateien verschlüsselt. Diese Funktion wird für neue Festplatten empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Verwenden Sie die Verschlüsselung auf einer Festplatte, die bereits benutzt wurde, so sollte die gesamte Festplatte verschlüsselt werden. So sind alle Daten geschützt, selbst gelöschte Daten, die möglicherweise wiederhergestellt werden können. Das Kontrollkästchen ist standardmäßig deaktiviert.

Einstellung	Beschreibung
Authentifizierungsmethode	**Nur Kennwort (Windows 8 und höher)** Bei Auswahl dieser Variante fragt Kaspersky Endpoint Security beim Benutzer das Kennwort ab, wenn auf das verschlüsselte Laufwerk zugegriffen wird. Diese Variante für die Aktion kann gewählt werden, wenn das Trusted Platform Module (TPM) nicht verwendet wird. **Trusted Platform Module (TPM)** Bei Auswahl dieser Variante verwendet BitLocker das Trusted Platform Module (TPM). *Trusted Platform Module* (TMP) ist ein Mikrochip, der grundlegende Sicherheitsfunktionen gewährleistet (z. B. für die Speicherung von Chiffrierschlüsseln). Das Trusted Platform Module wird gewöhnlich auf dem Mainboard des Computers installiert und interagiert über eine Hardwareschnittstelle mit den übrigen Systemkomponenten. Für Computer mit den Betriebssystemen Windows 7 und Windows Server 2008 R2 ist nur die Verschlüsselung unter Verwendung eines TPM-Moduls verfügbar. Wenn kein TPM-Modul installiert ist, ist die BitLocker-Verschlüsselung nicht möglich. Die Verwendung eines Kennworts wird auf diesen Computern nicht unterstützt. Ein Gerät, das mit Trusted Platform Module ausgerüstet ist, kann Chiffrierschlüssel erstellen, die nur seiner Hilfe entschlüsselt werden können. Das Trusted Platform Module verschlüsselt Chiffrierschlüssel mit einem eigenen Storage Root Key. Der Storage Root Key wird im Trusted Platform Module aufbewahrt. Dadurch wird für die Chiffrierschlüssel ein zusätzlicher Schutz vor Angriffsversuchen gewährleistet. Diese Aktion ist standardmäßig ausgewählt. Sie können eine zusätzliche Schutzebene für den Zugriff auf den Chiffrierschlüssel einrichten und den Schlüssel mit einem Kennwort oder einer PIN verschlüsseln: • **PIN für TPM verwenden**. Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer einen PIN-Code verwenden, um auf einen Chiffrierschlüssel zuzugreifen, der im Trusted Platform Module (TPM) aufbewahrt wird. Wenn das Kontrollkästchen deaktiviert ist, ist es dem Benutzer verboten, einen PIN-Code zu verwenden. Um Zugriff auf den Chiffrierschlüssel zu erhalten, verwendet der Benutzer ein Kennwort. • **Trusted Platform Module (TPM) oder Kennwort, falls TPM nicht verfügbar ist**. Wenn diese Option ausgewählt ist, kann der Benutzer mithilfe eines Kennworts Zugriff auf die Chiffrierschlüssel erhalten, falls kein Trusted Platform Module (TPM) verfügbar ist. Wenn das Kontrollkästchen deaktiviert ist und das TPM-Modus nicht verfügbar ist, wird die vollständige Festplattenverschlüsselung nicht gestartet. Die ausgewählte Authentifizierungsmethode muss durch Angabe von Kennwort- oder PIN-Anforderungen konfiguriert werden: • **Mindestlänge der PIN (Zeichen)** (der Standardwert ist 6). • **Mindestlänge des Kennworts (Zeichen)** (der Standardwert ist 8). • **Maximale Anzahl gespeicherter Passwörter/PINs** (der Standardwert ist 5). • **Kennwort/PIN-Gültigkeitsdauer für TPM beschränken (Tage)** (standardmäßig deaktiviert). • **Erweiterte PIN verwenden (Buchstaben und Ziffern)**. Eine *erweiterte PIN* ermöglicht neben der Verwendung numerischer Zeichen auch lateinische Groß- und Kleinbuchstaben, Sonderzeichen und Leerzeichen. Standardmäßig deaktiviert.
Wiederherstellungsschlüssel automatisch neu erstellen (Tage)	Kennwort automatisch aktualisieren, um den Zugriffauf ein BitLocker-geschütztes Laufwerk wiederherzustellen. Wenn das Kontrollkästchen aktiviert ist, geben Sie die Gültigkeitsdauer des Kennworts für den Wiederherstellungsschlüssel an. Dadurch lässt sich eine Wiederverwendung des Kennworts für den Wiederherstellungsschlüssel verhindern.

Verschlüsselung von Dateien

Die Dateiverschlüsselung wird auf Arm-basierten Computern nicht unterstützt.

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Sie können folgende Listen anlegen: Listen mit Dateien nach Erweiterung oder Erweiterungsgruppen, und Listen mit Ordnern, die sich auf lokalen Laufwerken des Computers befinden. Außerdem können Sie Verschlüsselungsregeln für Dateien definieren, die von bestimmten Programmen erstellt werden. Nachdem die Richtlinie übernommen wurde, verschlüsselt und entschlüsselt Kaspersky Endpoint Security die folgenden Dateien:

- Dateien, die einzeln zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
- Dateien, die in Ordnern gespeichert sind, welche zur Verschlüsselungsliste oder Entschlüsselungsliste hinzugefügt wurden
- Dateien, die von bestimmten Programmen erstellt werden

Für die Verschlüsselung von Dateien gelten die folgenden Besonderheiten:

- Kaspersky Endpoint Security verschlüsselt/entschlüsselt die Standardordner nur für die lokalen Benutzerprofile (local user profiles) des Betriebssystems. Kaspersky Endpoint Security verschlüsselt und entschlüsselt die Standardordner nicht für Roaming-Benutzerprofile (roaming user profiles), verbindliche Benutzerprofile (mandatory user profiles), temporäre Benutzerprofile (temporary user profiles) und Ordnerumleitung.
- Für Dateien, deren Veränderung die Funktionsfähigkeit des Betriebssystems und der installierten Programme beeinträchtigen kann, führt Kaspersky Endpoint Security keine Verschlüsselung durch. Zur Liste der Verschlüsselungsausnahmen gehören beispielsweise folgende Dateien und Ordner mit allen untergeordneten Ordnern:
  - %WINDIR%
  - %PROGRAMFILES% und %PROGRAMFILES(X86)%
  - Dateien der Systemregistrierung von Windows

  Die Liste mit Ausnahmen von der Verschlüsselung kann nicht angezeigt oder geändert werden. Dateien und Ordner aus der Liste mit den Verschlüsselungsausnahmen können zur Verschlüsselungsliste hinzugefügt werden; sie werden jedoch bei der Ausführung der Dateiverschlüsselung nicht verschlüsselt.

Einstellungen der Komponente „Dateien verschlüsseln"

Einstellung	Beschreibung
Verschlüsselungsmodus	**Nicht verändern**. Bei Auswahl dieses Elements belässt Kaspersky Endpoint Security die Dateien und Ordner im gleichen Zustand, d.h. sie werden nicht verschlüsselt oder entschlüsselt. **Gemäß den Regeln**. Bei Auswahl dieses Elements geht Kaspersky Endpoint Security wie folgt vor: Dateien und Ordner werden gemäß den Verschlüsselungsregel verschlüsselt, Dateien und Ordner werden gemäß den Entschlüsselungsregel entschlüsselt, und der Zugriff von Programmen auf verschlüsselte Dateien wird nach den Regeln für Programme geregelt. **Alle entschlüsseln**. Bei Auswahl dieses Elements entschlüsselt Kaspersky Endpoint Security alle verschlüsselten Dateien und Ordner.

Einstellung	Beschreibung
Verschlüsselung	Auf dieser Registerkarte werden die Regeln für die Verschlüsselung der Dateien angezeigt, die auf lokalen Laufwerken gespeichert sind. Sie können Dateien wie folgt hinzufügen: • **Standardordner**. Kaspersky Endpoint Security erlaubt es, die folgenden Bereiche hinzuzufügen: **Dokumente**. Dateien im Standardordner *Dokumente* des Betriebssystems, sowie untergeordnete Ordner. **Favoriten**. Dateien im Standardordner *Favoriten* des Betriebssystems, sowie untergeordnete Ordner. **Desktop**. Dateien im Standardordner *Desktop* des Betriebssystems, sowie untergeordnete Ordner. **Temporäre Dateien**. Temporäre Dateien, die mit der Verwendung Programmen zusammenhängen, die auf dem Computer installiert sind. Beispiel: Das Programm Microsoft Office erstellt temporäre Dateien mit Backup-Kopien von Dokumenten. **Outlook-Dateien**. Dateien, die mit der Nutzung des Mail-Clients Outlook zusammenhängen: Datendateien (PST), Offlinedatendateien (OST), Offlineadressbuch-Dateien (OAB) und Dateien für Persönliches Adressbuch (PAB). • **Manuell festgelegter Ordner**. Sie können einen Ordnerpfad eingeben. Beachten Sie folgende Regeln, wenn Sie einen Ordnerpfad hinzufügen: Verwenden Sie eine Umgebungsvariable (z. B. `%FOLDER%\UserFolder\`). Eine Umgebungsvariable kann nur ein Mal und nur am Anfang des Pfads verwendet werden. Verwenden Sie keine relativen Pfade. Verwenden Sie nicht die Zeichen `*` und `?`. Verwenden Sie keine UNC-Pfade. Verwenden Sie `;` oder `,` als Trennzeichen. • **Dateien nach Erweiterung**. Sie können aus der Liste eine Gruppe mit Erweiterungen auswählen, z. B. die Erweiterungsgruppe *Archive*. Außerdem können Sie eine Dateierweiterung manuell hinzufügen.
Entschlüsselung	Auf dieser Registerkarte werden die Entschlüsselungsregeln für Dateien angezeigt, die auf lokalen Laufwerken gespeichert sind.
Regeln für Programme	Auf dieser Registerkarte wird eine Tabelle mit Zugriffsregeln für Programme auf verschlüsselte Dateien und mit Verschlüsselungsregeln für Dateien angezeigt. Die Regeln beziehen sich auf Dateien, die von bestimmten Programmen erstellt und geändert wurden.
Verschlüsselte Archive	Einstellungen für die Kennwortstärke, die beim Erstellen verschlüsselter Archive gelten sollen.

Wechseldatenträger verschlüsseln

Die Verschlüsselung von Wechseldatenträgern wird auf Arm-basierten Computern wird nicht unterstützt.

Diese Komponente ist verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Workstation installiert ist. Diese Komponente ist nicht verfügbar, wenn das Programm Kaspersky Endpoint Security auf einem Computer mit dem Betriebssystem Windows für Server installiert ist.

Kaspersky Endpoint Security unterstützt die Dateiverschlüsselung in FAT32- und NTFS-Dateisystemen. Wenn mit dem Computer ein Wechseldatenträger mit einem nicht unterstützten Dateisystem verbunden ist, wird die Verschlüsselung dieses Wechseldatenträgers mit einem Fehler abgeschlossen und Kaspersky Endpoint Security legt für diesen Wechseldatenträger den Zugriffsstatus „Nur Lesen“ fest.

Um die Daten auf Wechseldatenträgern zu schützen, können Sie folgende Verschlüsselungsmethoden verwenden:

- Full Disk Encryption (FDE).

  Verschlüsselung des gesamten Wechseldatenträgers, einschließlich des Dateisystems.

  Es ist nicht möglich, außerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen. Außerdem ist es nicht möglich, innerhalb des Unternehmensnetzwerks auf die verschlüsselten Daten zuzugreifen, wenn der Computer nicht mit Kaspersky Security Center („Gast-Computer“) verbunden ist.

- File Level Encryption (FLE).

  Nur Dateien auf dem Wechseldatenträger verschlüsseln. Dabei wird das Dateisystem nicht verändert.

  > Die Verschlüsselung von Dateien auf Wechseldatenträgern ermöglicht es, auch außerhalb des Unternehmensnetzwerks auf die Daten zuzugreifen. Dazu dient der *portable Modus*.

Bei der Verschlüsselung erstellt Kaspersky Endpoint Security einen Master-Schlüssel. Kaspersky Endpoint Security speichert den Master-Schlüssel in den folgenden Speichern:

- Kaspersky Security Center.
- Benutzercomputer.

  Der Master-Schlüssel wird mit einem Geheimschlüssel des Benutzers verschlüsselt.
- Wechseldatenträger.

  Der Master-Schlüssel wird mit einem offenen Schlüssel von Kaspersky Security Center verschlüsselt.

Nach der Verschlüsselung sind die Daten auf dem Wechseldatenträger innerhalb des Unternehmensnetzwerks verfügbar, als würde ein gewöhnlicher unverschlüsselter Wechseldatenträger verwendet.

Zugriffserteilung auf verschlüsselte Daten

Wenn eine Wechseldatenträger mit verschlüsselten Daten verbunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

1. Es wird überprüft, ob in der lokalen Datenverwaltung auf dem Benutzercomputer ein Master-Schlüssel vorhanden ist.

   Wenn ein Master-Schlüssel gefunden wird, erhält der Benutzer Zugriff auf die Daten des Wechseldatenträgers.

   Wenn kein Master-Schlüssel gefunden wird, führt Kaspersky Endpoint Security die folgenden Aktionen aus:

   a. Es wird eine Anfrage an Kaspersky Security Center gesendet.

      Daraufhin sendet Kaspersky Security Center eine Antwort mit einem Master-Schlüssel.

   b. Kaspersky Endpoint Security speichert den Master-Schlüssel in der lokalen Datenverwaltung auf dem Benutzercomputer, um ihn künftig für den verschlüsselten Wechseldatenträger zu verwenden.

2. Die Daten werden entschlüsselt.

Besonderheiten bei der Verschlüsselung von Wechseldatenträgern

Für die Verschlüsselung von Wechseldatenträgern gelten die folgenden Besonderheiten:

- Die Richtlinie mit den festgelegten Verschlüsselungseinstellungen für Wechseldatenträger wird für eine bestimmte Gruppe von verwalteten Computern erstellt. Deshalb ist das Ergebnis, das durch das Übernehmen der Richtlinie für Kaspersky Security Center mit angepasster Verschlüsselung/Entschlüsselung von Wechseldatenträgern erreicht wird, davon abhängig, mit welchen Computern ein Wechseldatenträger verbunden ist.

- Für Dateien mit dem Zugriffsstatus „nur Lesen“, die auf Wechseldatenträgern gespeichert sind, führt Kaspersky Endpoint Security keine Dateiverschlüsselung/-entschlüsselung durch.

- Als Wechseldatenträger werden folgende Gerätetypen unterstützt:

  - Datenträger, die über eine USB-Schnittstelle verbunden werden

  - Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

  - SSD-Festplatten, die über die Schnittstellen USB und FireWire angeschlossen werden

Einstellungen der Komponente „Wechseldatenträger verschlüsseln“

Einstellung	Beschreibung
Verschlüsselungsmodus	**Gesamten Wechseldatenträger verschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Wechseldatenträger werden sektorweise verschlüsselt, einschließlich der Dateisysteme der Wechseldatenträger. **Alle Dateien verschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Alle Dateien, die auf Wechseldatenträgern gespeichert sind, werden verschlüsselt. Bereits verschlüsselte Dateien werden von Kaspersky Endpoint Security nicht erneut verschlüsselt. Der Inhalt des Dateisystems von Wechseldatenträgern sowie die Namen verschlüsselter Dateien und die Ordnerstruktur bleiben verfügbar und werden nicht verschlüsselt. **Nur neue Dateien verschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Auf Wechseldatenträgern werden nur jene Dateien verschlüsselt, die hinzugefügt oder geändert wurden, nachdem die Richtlinie für Kaspersky Security Center zum letzten Mal übernommen wurde. Dieser Verschlüsselungsmodus kann praktisch sein, wenn der Benutzer einen Wechseldatenträger sowohl privat als auch geschäftlich nutzt. Der Verschlüsselungsmodus erlaubt es, alle alten Dateien unverändert zu lassen und nur jene Dateien zu verschlüsseln, die der Benutzer auf einem PC erstellt, auf dem Kaspersky Endpoint Security installiert ist und auf dem die Verschlüsselungsfunktion zur Verfügung steht. Dadurch ist ein Zugriff auf persönliche Dateien immer möglich, unabhängig davon, ob das Programm Kaspersky Endpoint Security auf dem Computer installiert ist und ob die Verschlüsselungsfunktion verfügbar ist oder nicht. **Gesamten Wechseldatenträger entschlüsseln**. Ist dieses Element ausgewählt, so geht Kaspersky Endpoint Security wie folgt vor, wenn die Richtlinie mit den angegebenen Verschlüsselungseinstellungen für Wechseldatenträger übernommen wird: Es werden alle verschlüsselten Dateien entschlüsselt, die auf Wechseldatenträgern gespeichert sind, sowie die Dateisysteme der Wechseldatenträger, falls diese verschlüsselt waren. **Nicht verändern**. Ist dieses Elements gewählt und die Richtlinie wird übernommen, so verbleiben die Laufwerke in ihrem ursprünglichen Zustand. Wenn das Laufwerk verschlüsselt wurde, bleibt es verschlüsselt. Wenn das Laufwerk entschlüsselt wurde, bleibt es entschlüsselt. Dieses Element ist standardmäßig ausgewählt.

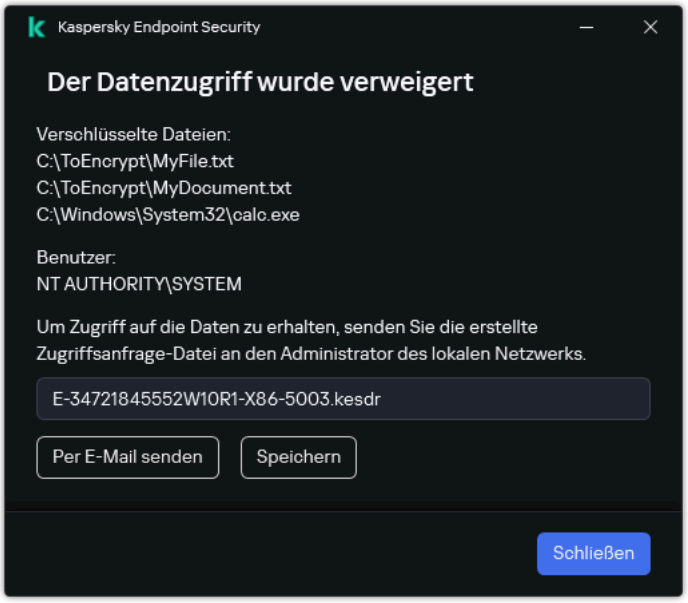
Einstellung	Beschreibung
Portabler Modus	Dieses Kontrollkästchen aktiviert/deaktiviert die Erstellung eines Wechseldatenträgers, der es erlaubt, mit den Dateien, die auf diesem Wechseldatenträger gespeichert sind, auf Computern außerhalb des Unternehmensnetzwerks zu arbeiten. Wenn dieses Kontrollkästchen aktiviert ist und die Richtlinie übernommen wird, fragt Kaspersky Endpoint Security den Benutzer nach dem Kennwort, bevor mit der Verschlüsselung von Dateien auf einem Wechseldatenträger begonnen wird. Dieses Kennwort ist erforderlich, um auf Computern außerhalb des Unternehmensnetzwerks Zugriff auf verschlüsselte Dateien auf dem Wechseldatenträger zu erhalten. Sie können die Kennwortkomplexität anpassen. Der portable Modus ist für die Modi **Alle Dateien verschlüsseln** und **Nur neue Dateien verschlüsseln** verfügbar.
Nur belegten Speicherplatz verschlüsseln	Das Kontrollkästchen aktiviert/deaktiviert einen Verschlüsselungsmodus, bei dem nur die belegten Sektoren eines Laufwerks verschlüsselt werden. Dieser Modus wird für neuen Laufwerke empfohlen, auf denen bisher noch keine Daten geändert oder gelöscht wurden. Ist das Kontrollkästchen aktiviert, so wird nur der Teil eines Laufwerks verschlüsselt, der mit Dateien belegt ist. Neue Daten werden von Kaspersky Endpoint Security automatisch verschlüsselt. Ist dieses Kontrollkästchen deaktiviert, so wird das gesamte Laufwerk verschlüsselt. Dabei werden auch die Bestandteile von bereits gelöschten oder geänderten Dateien verschlüsselt. Die Funktion, bei der nur belegter Speicherplatz verschlüsselt wird, ist nur für den Modus **Gesamten Wechseldatenträger verschlüsseln** verfügbar. Wenn die Funktion **Nur belegten Speicherplatz verschlüsseln** nach dem Start der Verschlüsselung aktiviert/deaktiviert wird, wird diese Einstellung nicht beeinflusst. Diese Einstellung muss vor dem Start der Verschlüsselung aktiviert oder deaktiviert werden.

Benutzerdefinierte Regeln	Tabelle der Geräte, für die individuelle Verschlüsselungsregeln festgelegt sind. Es gibt folgende Möglichkeiten, um Verschlüsselungsregeln für bestimmte Wechseldatenträger zu erstellen:
	• Hinzufügen eines Wechseldatenträgers aus der Liste der vertrauenswürdigen Geräte der „Gerätekontrolle“.
	• Manuelles Hinzufügen eines Wechseldatenträgers:
	  • Nach Geräte-ID (Hardware ID oder HWID)
	  • Nach Gerätemodell: Vendor ID (VID) und Product ID (PID)

Verschlüsselung von Wechseldatenträgern im Offline-Modus erlauben	Ist das Kontrollkästchen aktiviert, so verschlüsselt Kaspersky Endpoint Security die Wechseldatenträger auch dann, wenn keine Verbindung zu Kaspersky Security Center besteht. Die Daten, die zur Entschlüsselung von Wechseldatenträgern erforderlich sind, werden dabei auf der Festplatte des Computers gespeichert, mit dem der Wechseldatenträger verbunden ist, und werden nicht an Kaspersky Security Center übertragen. Wenn dieses Kontrollkästchen deaktiviert ist, verschlüsselt Kaspersky Endpoint Security Wechseldatenträger nicht, wenn keine Verbindung zu Kaspersky Security Center besteht.
Einstellungen für Verschlüsselungskennwörter / Portabler Dateimanager	Einstellungen für die Stärke des Kennworts für den portablen Dateimanager.

Vorlagen (Datenverschlüsselung)

Kaspersky Endpoint Security kann nach der Datenverschlüsselung den Datenzugriff verbieten, beispielsweise wenn sich die Unternehmensinfrastruktur oder der Kaspersky Security Center Administrationsserver geändert hat. Wenn der Benutzer keinen Zugriff auf verschlüsselte Daten hat, kann er beim Administrator den Datenzugriff anfordern. Dazu muss der Benutzer eine Zugriffsanfrage-Datei übermitteln. Dann muss der Benutzer die Antwortdatei, die er vom Administrator erhält, in Kaspersky Endpoint Security laden. In Kaspersky Endpoint Security ist es möglich, den Administrator per E-Mail um Datenzugriff zu bitten (s. Abb. unten).



Anfrage für den Zugriff auf verschlüsselte Daten

Es gibt eine Vorlage für die Nachricht, die über fehlenden Zugriff auf verschlüsselte Daten benachrichtigt. Um es dem Benutzer leichter zu machen, können Sie die folgenden Felder ausfüllen:

- **An**. Geben Sie die E-Mail-Adresse der Administratorengruppe ein, die über Rechte für die Datenverschlüsselungsfunktion verfügt.
- **Betreff**. Geben Sie einen Betreff der Nachricht mit einer Zugriffsanfrage für verschlüsselte Dateien ein. Sie können beispielsweise Tags hinzufügen, um diese Nachrichten zu filtern.
- **Nachricht vom Benutzer**. Ändern Sie bei Bedarf den Nachrichteninhalt. Sie können Variablen verwenden, um die erforderlichen Daten zu erhalten (z. B. die Variable `%USER_NAME%`).

Ausnahmen

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. Ein Administrator kann einem Benutzer auch erlauben, seine eigene lokale vertrauenswürdige Zone für einen bestimmten Computer zu erstellen. Auf diese Weise können Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen.

Ab Kaspersky Endpoint Security 12.5 für Windows können Sie EDR-Telemetrie zur vertrauenswürdigen Zone hinzufügen. Dadurch können die Daten optimiert werden, die das Programm an den Telemetrie-Erfassungsserver für die Lösung Kaspersky Anti Targeted Attack Platform (EDR) sendet.

Ab Kaspersky Endpoint Security 12.6 für Windows gehören Untersuchungsausnahmen und vertrauenswürdige Programme zur vertrauenswürdigen Zone. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme vereinfachen die schnelle Konfiguration von Kaspersky Endpoint Security auf SQL-Servern, Microsoft Exchange-Servern und System Center Configuration Manager. Das bedeutet, dass Sie auf Servern nicht manuell eine vertrauenswürdige Zone für die App einrichten müssen.

Ab Kaspersky Endpoint Security 12.8 für Windows können Sie das Programm im Light Agent-Modus installieren, um virtuelle Umgebungen zu schützen. Mit vordefinierten Untersuchungsausnahmen und vertrauenswürdigen Programmen können Sie Kaspersky Endpoint Security in virtuellen Citrix- und VMware-Umgebungen schnell konfigurieren.

Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Endpoint Security ein Objekt nicht auf Viren und andere bedrohliche Programme. Die Untersuchungsausnahmen ermöglichen es, sicher mit legitimen Programmen zu arbeiten, mit denen Angreifer einen 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.

Derartige Programme können bei der Ausführung von Kaspersky Endpoint Security gesperrt werden. Sie können Untersuchungsausnahmen anpassen, um eine Sperrung von notwendigen Programmen zu verhindern. Dazu muss der vertrauenswürdigen Zone der Name oder eine Namensmaske hinzugefügt werden, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht. Es kann beispielsweise sein, dass Sie häufig mit dem Programm Radmin, zur Remote-Administration von Computern. Eine solche Programmaktivität wird von Kaspersky Endpoint Security als schädlich eingestuft und kann blockiert werden. Um zu verhindern, dass ein Programm gesperrt wird, muss eine Untersuchungsausnahme erstellt werden. In dieser Ausnahme wird ein Name oder eine Namensmaske angegeben, die der Klassifikation der Viren-Enzyklopädie von Kaspersky entspricht.

Ein auf Ihrem Computer installiertes Programm, das Informationen sammelt und zur Verarbeitung weiterleitet, kann von Kaspersky Endpoint Security als schädlich eingestuft werden. Um dies zu vermeiden, können Sie das Programm von der Untersuchung ausschließen. Dazu können Sie Kaspersky Endpoint Security entsprechend anpassen, wie in dieser Dokumentation beschrieben.

Untersuchungsausnahmen können von folgenden Komponenten und Programmaufgaben verwendet werden, die vom Systemadministrator erstellt wurden:

- Verhaltensanalyse.
- Exploit-Prävention.

- Programm-Überwachung.
- Schutz vor bedrohlichen Dateien.
- Schutz vor Web-Bedrohungen.
- Schutz vor E-Mail-Bedrohungen.
- Aufgaben für die *Schadsoftware-Untersuchung*

Liste der vertrauenswürdigen Programme

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.

Untersuchungsausnahmen und vertrauenswürdige Programme unterscheiden sich wie folgt: Bei Ausnahmen untersucht Kaspersky Endpoint Security keine Dateien, während bei vertrauenswürdigen Programmen die initiierten Prozesse nicht kontrolliert werden. Wenn ein vertrauenswürdiges Programm eine schädliche Datei in einem Ordner erstellt, der nicht zu den Untersuchungsausnahmen gehört, erkennt Kaspersky Endpoint Security die Datei und beseitigt die Bedrohung. Wenn der Ordner zu den Ausnahmen gehört, überspringt Kaspersky Endpoint Security diese Datei.

Wenn Sie beispielsweise die Objekte, die von der Standard-App Microsoft-Editor verwendet werden, für ungefährlich halten, vertrauen Sie dieser App und Sie können Microsoft-Editor zur Liste der vertrauenswürdigen Programme hinzufügen, damit die von dieser App verwendeten Objekte nicht überwacht werden. Dadurch wird die Computerleistung erhöht, was bei Verwendung von Serveranwendungen besonders wichtig ist.

Außerdem können spezielle Aktionen, die von Kaspersky Endpoint Security als schädlich klassifiziert werden, im Rahmen bestimmter Programme ungefährlich sein. So ist das Abfangen eines Textes, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (z. B. Punto Switcher) ein normaler Vorgang. Es wird empfohlen, solche Programme in die Liste der vertrauenswürdigen Programme aufzunehmen, um ihre speziellen Funktionen zu berücksichtigen und sie von der Aktivitätskontrolle auszuschließen.

Vertrauenswürdige Programme helfen, Kompatibilitätsprobleme zwischen Kaspersky Endpoint Security und anderen Anwendungen zu vermeiden (z. B. das Problem einer doppelten Untersuchung des Netzwerkverkehrs eines fremden Computers durch Kaspersky Endpoint Security und durch eine andere Antiviren-Anwendung).

Die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms werden jedoch weiterhin auf Viren und andere Schadprogramme untersucht. Verwenden Sie Untersuchungsausnahmen, um ein Programm vollständig von der Untersuchung durch Kaspersky Endpoint Security auszuschließen.

Einstellungen für Ausnahmen

Einstellung	Beschreibung

Typen der zu erkennenden Objekte

Kaspersky Endpoint Security sucht unabhängig von den aktuellen Einstellungen stets nach Viren, Würmern und Trojanern und blockiert diese. Diese Programme können dem Computer erheblichen Schaden zufügen.

- **Viren und Würmer**

  Unterkategorie: Viren und Würmer (Viruses_and_Worms)

  Gefahrenstufe: Hoch

  Klassische Viren und Würmer führen auf einem Computer Aktionen aus, die nicht vom Benutzer erlaubt wurden. Sie können sich selbst kopieren, wobei die Kopien ebenfalls zur Reproduktion fähig sind.

  Klassischer Virus

  Nachdem ein klassischer Virus in ein System eingedrungen ist, infiziert er eine Datei, aktiviert sich darin, führt seine schädlichen Aktionen aus und fügt anderen Dateien Kopien von sich hinzu.

  Ein klassischer Virus vermehrt sich nur auf lokalen Computerressourcen und kann nicht selbständig in andere Rechner eindringen. Er kann nur auf andere Computer gelangen, wenn er seine Kopie einer Datei hinzufügt, die in einem gemeinsamen Ordner oder auf einer eingelegten CD gespeichert wird, oder wenn der Benutzer eine E-Mail-Nachricht verschickt, an welche die infizierte Datei angehängt ist.

  Der Code eines klassischen Virus kann in unterschiedliche Computerbereiche, in das Betriebssystem oder in Programme eindringen. Abhängig vom Milieu werden *Dateiviren*, *Bootviren*, *Skriptviren* und *Makroviren* unterschieden.

  Viren verwenden unterschiedliche Methoden, um Dateien zu infizieren. *Overwriting*-Viren schreiben ihren Code über den Code einer infizierten Datei und zerstören deren Inhalt. Die infizierte Datei funktioniert nicht mehr und kann nicht repariert werden. *Parasitic*-Viren verändern Dateien, wobei diese Dateien vollständig oder teilweise funktionsfähig bleiben. *Companion*-Viren verändern Dateien nicht, sondern legen Duplikate an. Beim Öffnen einer infizierten Datei wird ihr Zwilling gestartet, der ein Virus ist. Außerdem gibt es noch folgende Virentypen: *Link-Viren*, *OBJ-Viren*, *LIB-Viren*, *Quellcode*-Viren so wie viele andere.

  Wurm

  Genau wie ein klassischer Virus dringt auch ein Wurm in einen Computer ein, aktiviert seinen Code und führt schädliche Aktionen aus. Die Bezeichnung Wurm geht darauf zurück, dass er wie ein Wurm von Computer zu Computer „kriechen" und seine Kopien ohne Erlaubnis des Benutzers über verschiedene Datenkanäle verbreiten kann.

  Würmer werden grundsätzlich nach der Art ihrer Verbreitung unterschieden. Die folgende Tabelle klassifiziert die Wurmtypen nach der Verbreitungsmethode.

  Verbreitungsmethoden von Würmern

Typ	Name	Beschreibung
Email-Worm	Email-Worm	Sie verbreiten sich über E-Mails. Eine infizierte E-Mail-Nachricht enthält eine angehängte Datei mit einer Wurmkopie oder einem Link zu einer solchen Datei, die sich auf einer gehackten oder speziell erstellten Website befindet. Wenn Sie die angehängte Datei öffnen, wird der Wurm aktiviert. Wenn Sie auf den Link klicken, die Datei herunterladen und dann öffnen, beginnt der Wurm auch mit seinen bösartigen Aktionen. Danach verbreitet er seine Kopien. Dazu sucht er andere E-Mail-Adressen und schickt infizierte Nachrichten an diese.
IM-Worm	IM-Client-Würmer	Sie verbreiten sich über IM-Clients. Ein IM-Wurm verschickt in der Regel Nachrichten mit einem Link, der zu einer Website mit seiner Kopie führt, an die Adressen der Kontaktliste. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
IRC-Worm	Würmer für Internet-Chats	Sie verbreiten sich über Internet Relay Chats. Dies sind Dienstsysteme, mit denen über das Internet in Echtzeit Gespräche mit anderen Teilnehmern möglich sind. Ein solcher Wurm veröffentlicht im Internet-Chat eine Datei mit seiner Kopie oder einem Link zu einer Datei. Wenn der Benutzer die Datei herunterlädt und öffnet, wird der Wurm aktiviert.
Net-Worm	Netzwürmer (Würmer für Computernetzwerke)	Sie verbreiten sich über Computernetzwerke. Im Unterschied zu anderen Wurmtypen verbreitet sich ein Netzwurm ohne Zutun des Benutzers. Er sucht im lokalen Netzwerk nach Computern, auf denen Programme laufen, die Schwachstellen aufweisen. Zu diesem Zweck schickt er ein spezielles Netzwerkpaket (Exploit), das den Wurmcode oder einen Teil davon enthält. Befindet sich ein „verwundbarer" Computer im Netzwerk, nimmt er das Netzwerkpaket an. Nachdem der Wurm vollständig in den Computer eingedrungen ist, aktiviert er sich.
P2P-Worm	Würmer für Dateitausch-Netzwerke	Sie verbreiten sich über Peer-to-Peer-Netze. Um in ein P2P-Netz einzudringen, kopiert sich der Wurm in einen Ordner, der zum Dateiaustausch verwendet wird und sich gewöhnlich auf einem PC befindet. Das P2P-Netz zeigt Informationen über diese Datei an. Ein Benutzer kann die infizierte Datei wie andere angebotene Dateien im Netzwerk „finden", herunterladen und öffnen. Komplexere Würmer imitieren das Netzwerkprotokoll eines konkreten P2P-Netzes: Sie antworten positiv auf Suchanfragen und bieten ihre Kopien zum Download an.
Wurm	Sonstige Würmer	Zu den sonstigen Netzwürmern zählen: • Würmer, die ihre Kopien in Netzwerkressourcen verbreiten. Unter Verwendung von Betriebssystemfunktionen durchsuchen sie verfügbare Netzwerkordner, bauen Verbindungen zu Computern im globalen Netzwerk auf und versuchen, umfassenden Zugriff auf ihre Laufwerke zu erhalten. Im Unterschied zu den oben beschriebenen Wurmarten verbreiten sich die sonstigen Würmer nicht selbständig weiter, sondern nur, wenn der Benutzer eine Datei mit einer Wurmkopie öffnet. • Würmer, die keine in dieser Tabelle beschriebenen Verbreitungsmethoden verwenden (z. B. Würmer, die sich über Mobiltelefone weiterverbreiten).

- **Trojaner (einschließlich Ransomware)**

  Subkategorie: trojanische Programme (Trojan_programs)

Gefahrenstufe: Hoch

Im Gegensatz zu Würmern und Viren erstellen trojanische Programme keine Kopien von sich. Sie dringen z. B. über E-Mails oder über den Browser in den Computer ein, wenn der Benutzer eine infizierte Webseite besucht. Trojanische Programme werden unter Beteiligung des Benutzers gestartet. Unmittelbar nach ihrem Start beginnen sie mit ihren schädlichen Aktionen.

Jeder Trojaner-Typ zeigt ein individuelles Verhalten auf dem infizierten Computer. Die Hauptfunktionen von trojanischen Programmen sind das Sperren, Verändern oder Vernichten von Informationen sowie das Hervorrufen von Funktionsstörungen in Computern oder Computernetzwerken. Außerdem können trojanische Programme Dateien empfangen oder senden, Dateien ausführen, auf dem Bildschirm Meldungen anzeigen, auf Webseiten zugreifen, Programme herunterladen und installieren, und einen Computer neu starten.

Häufig verwenden Angreifer eine „Kombination" aus unterschiedlichen Trojanerprogrammen.

Die folgende Tabelle unterscheidet die Typen der trojanischen Programme nach ihrem Verhalten.

Typen der trojanischen Programme nach ihrem Verhalten auf einem infizierten Computer

Typ	Name	Beschreibung
Trojan-ArcBomb	Trojanische Programme – „Archivbomben"	Archive. Beim Extrahieren vergrößert sich der Inhalt so stark, dass es auf dem Computer zu Funktionsstörungen kommt. Wenn der Benutzer versucht, ein solches Archiv zu entpacken, kann es sein, dass die Leistung des Computers sinkt, der Computer hängen bleibt oder die Festplatte mit „leeren" Daten überfüllt wird. Eine besondere Gefahr bilden „Archivbomben" für Datei- und Mailserver. Wird auf dem Server ein System zur automatischen Verarbeitung eingehender Daten verwendet, kann eine „Archivbombe" den Server zum Absturz bringen.
Backdoor	Trojanische Programme zur Remote-Administration	Dieser Typ gilt unter den trojanischen Programmen als der gefährlichste. Sie gleichen funktionsmäßig Programmen, die zur Remote-Administration auf einem Computer installiert werden. Diese Programme installieren sich auf dem Computer, ohne dass der Benutzer etwas davon bemerkt, und ermöglichen dem Angreifer die Fernsteuerung des Computers.
Trojan	Trojanische Programme	Dieser Typ umfasst folgende schädlichen Programme: • **Klassische trojanische Programme**. Diese Programme führen nur die Grundfunktionen trojanischer Programme aus: Sperrung, Veränderung oder Zerstörung von Informationen, Störung der Arbeit von Computern oder Computernetzwerken. Sie besitzen keine Zusatzfunktionen, über die andere Trojaner-Typen verfügen, die in dieser Tabelle beschrieben sind. • **„Mehrzweck"-Trojaner**. Sie besitzen Zusatzfunktionen, die gleichzeitig für mehrere Typen trojanischer Programme charakteristisch sind.
Trojan-Ransom	Trojanische Erpressungsprogramme	Sie nehmen die Daten auf einem PC als „Geisel", indem sie diese verändern oder sperren, oder stören die Arbeit des Computers, damit der Benutzer nicht mehr auf seine Daten zugreifen kann. Der Angreifer fordert vom Benutzer ein Lösegeld und verspricht, dafür ein Programm zu liefern, das die Funktionsfähigkeit des Computers und der Daten wiederherstellt.
Trojan-Clicker	Trojanische Clicker-Programme	Diese Programme greifen von einem PC aus auf Webseiten zu: Sie senden entweder selbst Befehle an den Browser oder ersetzen Webadressen, die in Systemdateien gespeichert sind. Mithilfe dieser Programme organisieren Angreifer Netzwerkangriffe oder steigern die Besucherzahlen von Seiten, um die Anzeigehäufigkeit von Werbebannern zu erhöhen.
Trojan-Downloader	Trojanische Download-Programme	Sie greifen auf die Webseite des Eindringlings zu, laden von dort andere bösartige Programme herunter und installieren sie auf dem Computer des Benutzers. Sie können den Dateinamen des böswilligen Programms enthalten, die heruntergeladen oder von der Webseite, auf die zugegriffen wird, empfangen werden soll.
Trojan-Dropper	Trojanische Installationsprogramme	Nachdem sie auf der Computerfestplatte gespeichert wurden, installieren sie andere trojanische Programme, die sich in ihrem Körper befinden. Angreifer können trojanische Installationsprogramme zu folgenden Zwecken verwenden: • um ohne Wissen des Benutzers ein schädliches Programm zu installieren: Trojanische Installationsprogramme zeigen keinerlei Meldungen an oder blenden falsche Meldungen über einen Fehler im Archiv oder eine inkorrekte Version des Betriebssystems ein. • um andere bekannte Schadsoftware vor der Entdeckung zu schützen: Nicht alle Antiviren-Programme können Schadsoftware in trojanischen Installationsprogrammen erkennen.
Trojan-Notifier	Trojanische Benachrichtigungsprogramme	Sie informieren einen Angreifer darüber, dass der infizierte Computer „online" ist und übermitteln folgende Informationen über den Computer: IP-Adresse, Nummer des offenen Ports oder E-Mail-Adresse. Sie nehmen per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise Kontakt mit dem Angreifer auf. Trojanische Benachrichtigungsprogramme werden häufig in Kombination mit unterschiedlichen Trojanerprogrammen eingesetzt. Sie teilen dem Angreifer mit, dass andere trojanische Programme erfolgreich auf einem PC installiert wurden.
Trojan-Proxy	Trojanische Proxy-Programme	Sie ermöglichen es einem Angreifer, über einen PC anonym auf Webseiten zuzugreifen. Sie dienen häufig zum Spam-Versand.
Trojan-PSW	Trojanische Programme zum Kennwortdiebstahl	Trojanische Programme, die Kennwörter stehlen (Password Stealing Ware). Sie berauben Benutzerkonten und stehlen beispielsweise Registrierungsdaten für Softwareprodukte. Solche Trojaner durchsuchen Systemdateien und die Registrierung nach vertraulichen Daten und schicken diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den „Angreifer". Einige dieser trojanischen Programme werden speziellen Typen zugeordnet, die in dieser Tabelle beschrieben sind. Dazu zählen Trojaner, die Bankkonten berauben (Trojan-Banker), Daten von IM-Clients stehlen (Trojan-IM) und Daten aus Netzwerkspielen entwenden (Trojan-GameThief).
Trojan-Spy	Trojanische Spyware-Programme	Sie spionieren den Benutzer aus und sammeln Informationen über die Aktionen, die der Benutzer bei der Arbeit am Computer ausführt. Sie können die Daten abfangen, die der Benutzer über die Tastatur eingibt, Screenshots machen oder Listen aktiver Programme sammeln. Die gesammelten Informationen werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.

Trojan-DDoS	Trojanische Programme für Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung). Häufig werden mehrere Computer von solchen Programmen infiziert, um sie dann gleichzeitig für einen gezielten Angriff auf einen Server zu verwenden. DoS-Programme realisieren einen Angriff von einem Computer aus, wobei der Benutzer davon weiß. DDoS-Programme (Distributed DoS) verwenden eine größere Anzahl von Computern ohne Wissen der Benutzer für verteilte Angriffe.
Trojan-IM	Trojanische Programme zum Diebstahl der Daten von IM-Client-Benutzern	Sie stehlen Nummern und Kennwörter der Benutzer von IM-Clients. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Rootkit	Rootkits	Sie maskieren andere bösartige Programme und deren Aktivität und verlängern so die Persistenz der Programme im Betriebssystem. Sie können auch Dateien, Prozesse im Speicher eines infizierten Computers oder Registrierungsschlüssel, die bösartige Programme ausführen, verbergen. Die Rootkits können den Datenaustausch zwischen Programmen auf dem Computer des Benutzers und anderen Computern im Netzwerk maskieren.
Trojan-SMS	Trojanische Programme für SMS-Nachrichten	Sie infizieren Handys und versenden SMS-Nachrichten an kostenpflichtige Nummern.
Trojan-GameThief	Trojanische Programme zum Diebstahl von Benutzerdaten aus Netzwerkspielen	Sie stehlen Kontodaten von Benutzern, die an Netzwerkspielen für Computer teilnehmen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Banker	Trojanische Programme zum Diebstahl von Daten über Bankkonten	Sie stehlen Daten über Bankkonten oder über Konten bei elektronischen Zahlungssystemen. Die Daten werden per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer weitergeleitet.
Trojan-Mailfinder	Trojanische Programme, die E-Mail-Adressen sammeln	Sie sammeln auf einem Computer E-Mail-Adressen und übermitteln diese per E-Mail, via FTP, durch Zugriff auf eine spezielle Webseite oder auf andere Weise an den Angreifer. An die gesammelten Adressen kann der Angreifer Spam verschicken.

- **Schädliche Tools**

  Subkategorie: schädliche Tools

  Gefahrenstufe: Mittel

  Im Gegensatz zu anderen Arten von Malware führen bösartige Tools ihre Aktionen nicht sofort nach dem Start aus. Sie können auf dem Computer des Benutzers sicher gespeichert und gestartet werden. Angreifer verwenden die Funktionen dieser Programme, um Viren, Würmer und Trojaner zu erstellen, Netzwerkangriffe gegen Remote-Server zu organisieren, Computer zu „hacken" und andere schädliche Aktionen durchzuführen.

  Die folgende Tabelle kategorisiert die unterschiedlichen Funktionen von schädlichen Tools.

  Funktionen von schädlichen Tools

Typ	Name	Beschreibung
Constructor	Konstrukteure	Mit ihrer Hilfe können neue Viren, Würmer und Trojaner erstellt werden. Einige Konstrukteure verfügen über eine standardmäßige Fensteroberfläche, in der über ein Menü der Typ einer zu erstellenden Schadsoftware, die Methode zur Debugger-Abwehr und sonstige Eigenschaften gewählt werden.
Dos	Netzwerkangriffe	Von einem PC wird eine hohe Anzahl von Anfragen an einen Remote-Server gesendet. Die Serverressourcen reichen nicht aus, um die Anfragen zu verarbeiten, und der Server funktioniert nicht mehr (Denial-of-Service (DoS), zu Deutsch etwa: Dienstverweigerung).
Exploit	Exploits	*Exploits* bestehen aus einer Datenkombination oder aus Programmcode, der die Schwachstellen eines Programms, in dem er verarbeitet wird, ausnutzt, um auf dem Computer eine schädliche Aktion auszuführen. Ein Exploit kann beispielsweise Dateien schreiben oder lesen oder auf „infizierte" Webseiten zugreifen. Es gibt verschiedene Arten von Exploits, die Schwachstellen unterschiedlicher Programme oder Netzwerkdienste ausnutzen. Exploits werden als Netzwerkpaket über ein Netzwerk an mehrere Computer übertragen, um Computer mit anfälligen Netzwerkdiensten zu finden. Ein Exploit in einer DOC-Datei nutzt die Schwachstellen eines Textverarbeitungsprogramms. Er kann damit beginnen, die vom Angreifer programmierten Funktionen auszuführen, sobald der Benutzer eine infizierte Datei öffnet. Ein Exploit, der in eine E-Mail-Nachricht eingebettet ist, sucht nach Schwachstellen in einem Mail-Client. Er kann mit der Ausführung einer schädlichen Aktion beginnen, sobald der Benutzer die infizierte E-Mail in diesem Mail-Client öffnet. Mithilfe von Exploits werden Netzwürmer (Net-Worm) verbreitet. Nuker sind Netzwerkpakete, die einen Computer zum Absturz bringen.
FileCryptor	Verschlüsselungsprogramme	Chiffreure verschlüsseln schädliche Programme, um sie vor Antiviren-Programmen zu verstecken.
Flooder	Programme zur „Verunreinigung" von Netzwerken	Sie versenden eine hohe Anzahl von Nachrichten über Netzwerkkanäle. Zu diesem Typ zählen beispielsweise Programme, die der Verunreinigung von Internet Relay Chats dienen. Programme, die der Verunreinigung von Kanälen für E-Mail, IM-Clients und Mobilfunksysteme dienen, zählen nicht zu diesem Typ. Diese Programme werden separaten Typen zugeordnet, die ebenfalls in dieser Tabelle beschrieben sind (Email-Flooder, IM-Flooder und SMS-Flooder).
HackTool	Hacker-Tools	Sie können die Kontrolle über den Computer, auf dem sie installiert sind, übernehmen oder einen anderen Computer angreifen (z. B. ohne Erlaubnis des Benutzers andere Systembenutzer hinzufügen und Systemberichte löschen, um ihre Spuren im System zu verwischen). Zu diesem Typ gehören bestimmte Sniffer, die über schädliche Funktionen wie z. B. das Abfangen von Kennwörtern verfügen. Sniffer (Sniffers) sind Programme, die den Netzwerkverkehr abhören können.
Hoax	Böse Scherze	Diese Programme erschrecken einen Benutzer mit virenähnlichen Meldungen: Sie zeigen fiktive Meldungen über Virenfunde in sauberen Dateien oder über das Formatieren der Festplatte an.
Spoofer	Imitator-Tools	Sie senden E-Mails und Netzwerkanfragen mit gefälschten Absenderadressen. Imitatoren werden beispielsweise von Angreifern verwendet, um einen falschen Absender vorzutäuschen.
VirTool	Tools zur Modifikation schädlicher Programme	Sie erlauben es, andere schädliche Programme so zu modifizieren, dass sie sich vor Antiviren-Programmen verstecken können.

Email-Flooder	Programme zur „Verunreinigung" von E-Mail-Postfächern	Sie versenden eine hohe Anzahl von Nachrichten an E-Mail-Adressen („verstopfen diese mit Müll"). Die große Menge von E-Mails hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
IM-Flooder	Programme zur „Verunreinigung" von IM-Clients	Sie versenden eine hohe Anzahl von Nachrichten an Benutzer von IM-Clients Das hohe Nachrichtenaufkommen hindert den Benutzer daran, erwünschte eingehende Post zu erkennen.
SMS-Flooder	Programme zur „Verunreinigung" von SMS-Systemen	Sie versenden eine große Anzahl von SMS-Nachrichten an Mobiltelefone.

- **Adware**

  Unterkategorie: Werbe-Software (Adware)

  Gefahrenstufe: Mittel

  Adware-Programme dienen dazu, dem Benutzer Werbung zu zeigen. Sie zeigen auf der Oberfläche anderer Programme Werbebanner an oder leiten Suchanfragen auf Webseiten mit Werbung um. Einige von ihnen sammeln auf Werbung bezogene Informationen über den Benutzer und leiten sie an ihren Urheber weiter, z.B. Informationen darüber, welche Webseiten der Benutzer besucht und welche Suchanfragen er vornimmt. Im Gegensatz zu trojanischer Spyware leiten Adware-Programme diese Informationen mit der Erlaubnis des Benutzers weiter.

- **Dialer**

  Unterkategorie: Legitime Programme, mit denen Angreifer Ihren Computer oder Ihre Daten beschädigen können.

  Gefahrenstufe: Mittel

  Die Mehrzahl dieser Programme sind nützliche Programme. Zu diesen Programmen zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für FTP, HTTP und Telnet.

  Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf einem PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

  Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern. Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- **legitimes Programm, mit dem Angreifer den Computer oder die Benutzerdaten beschädigen können**

  Unterkategorie: Legitime Programme, mit denen Angreifer Ihren Computer oder Ihre Daten beschädigen können.

  Gefahrenstufe: Mittel

  Die Mehrzahl dieser Programme sind nützliche Programme. Zu diesen Programmen zählen IRC-Clients, Dialer, Download-Manager für Dateien, Aktivitätsmonitore für Computersysteme, Kennwort-Manager sowie Internetserver für FTP, HTTP und Telnet.

  Wenn allerdings ein Angreifer Zugriff auf diese Programme erhält oder sie auf einem PC installiert, können ihre Funktionen dazu dienen, die Sicherheit zu verletzen.

  Solche Programme haben unterschiedliche Funktionen, deren Typen in der nachstehenden Tabelle beschrieben werden.

Typ	Name	Beschreibung
Client-IRC	Clients für Internet-Chats	Diese Programme werden von Benutzern installiert, um in Internet Relay Chats zu kommunizieren. Angreifer verwenden sie zur Verbreitung von schädlichen Programmen.
Downloader	Download-Programme	Downloader können heimlich Dateien von Webseiten herunterladen.
Monitor	Monitorprogramme	Sie können die Aktivitäten auf einem Computer, auf dem sie installiert sind, beobachten (sie überwachen, welche Programme laufen und wie sie Daten mit Programmen auf anderen Computern austauschen).
PSWTool	Programme zur Wiederherstellung von Kennwörtern	Sie erlauben es, vergessene Kennwörter zu lesen und wiederherzustellen. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert.
RemoteAdmin	Programme zur Remote-Administration	Sie sind bei Systemadministratoren weit verbreitet. Diese Programme bieten Zugriff auf die Oberfläche eines Remote-Computers, der auf diese Weise überwacht und gesteuert werden kann. Zu diesem Zweck werden sie heimlich von Angreifern auf PCs installiert, um Remote-Computer zu beobachten und zu steuern. Legale Programme zur Remote-Administration unterscheiden sich von trojanischen Fernsteuerungsprogrammen des Typs Backdoor. Trojanische Programme besitzen Funktionen, die ihnen erlauben, selbständig in ein System einzudringen und sich zu installieren. Legale Programme verfügen nicht über diese Funktionen.
Server-FTP	FTP-Server	Sie erfüllen die Funktionen eines FTP-Servers. Angreifer installieren sie auf einem PC, um über das FTP-Protokoll Remote-Zugriff zu erhalten.
Server-Proxy	Proxyserver	Sie erfüllen die Funktionen eines Proxyservers. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
Server-Telnet	Telnet-Server	Erfüllt die Funktionen eines Telnet-Servers. Angreifer installieren sie auf einem PC, um Remote-Zugriff über das Telnet-Protokoll zu erhalten.
Server-Web	Webserver	Sie erfüllen die Funktionen eines Webservers. Angreifer installieren sie auf einem PC, um über das HTTP-Protokoll Remote-Zugriff zu erhalten.
RiskTool	Tools für die Arbeit auf einem lokalen Computer	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit am eigenen Rechner. Die Werkzeuge ermöglichen es dem Benutzer, Dateien oder Fenster von aktiven Programmen auszublenden und aktive Prozesse zu beenden.
NetTool	Netzwerk-Tools	Sie bieten dem Benutzer zusätzliche Optionen bei der Arbeit mit anderen Computern im Netzwerk. Diese Tools ermöglichen es, sie neu zu starten, offene Ports zu erkennen und Programme zu starten, die auf den Computern installiert sind.
Client-P2P	Clients für Peering-Netzwerke	Sie erlauben die Arbeit in Peering-Netzwerken (Peer-to-Peer). Angreifer können sie zur Verbreitung schädlicher Programme verwenden.
Client-SMTP	SMTP-Clients	Sie können heimlich E-Mail-Nachrichten senden. Angreifer installieren sie auf einem PC, um von ihm aus Spam zu verschicken.
WebToolbar	Web-Symbolleisten	Sie fügen den Oberflächen anderer Programme Symbolleisten für Suchmaschinen hinzu.
FraudTool	Pseudoprogramme	Sie geben sich als andere Programme aus. Es gibt zum Beispiel Pseudo-Anti-Virus-Programme, die Meldungen über die Erkennung von Malware anzeigen. In Wirklichkeit finden oder desinfizieren sie jedoch nichts.

- **Gepackte Objekte, mit deren Packverfahren bösartiger Code geschützt werden kann**

  Unterkategorie: Gepackte Dateien, die Schaden verursachen können.

  Gefahrenstufe: Mittel.

  Die Datei wurde mit einem speziellen Packer gepackt, der zum Packen von Schadsoftware verwendet wird: Viren, Würmer, Trojaner. Kaspersky Endpoint Security untersucht das SFX-Modul von selbstentpackenden SFX-Archiven (self-extracting archive).

  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.

- **Mehrfach gepackte Objekte**

  Unterkategorie: Gepackte Dateien, die Schaden verursachen können.

  Gefahrenstufe: Mittel.

  Die Datei wurde mit einem speziellen Packer gepackt, der zum Packen von Schadsoftware verwendet wird: Viren, Würmer, Trojaner. Kaspersky Endpoint Security untersucht das SFX-Modul von selbstentpackenden SFX-Archiven (self-extracting archive).

	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.

Ausnahmen	Diese Tabelle enthält Informationen über die Untersuchungsausnahmen.
	
	Empfehlung: Geben Sie relative Pfade an, keine absoluten Pfade. Dadurch können Sie nicht nur Dateisystemobjekte ausschließen, sondern auch dateilose Objekte. Beispiel: `*\Program Files (x86)\Folder\Subfolder`.
	
	Objekte können wie folgt von der Untersuchung ausgeschlossen werden:
	
	• Geben Sie einen Datei- oder Ordnerpfad an.
	
	• Geben Sie den Hash eines Objekts an.
	
	• 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` funktioniert nicht.
	
	  • 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.
	
	  Sie können Masken überall in einem Datei- oder Ordnerpfad verwenden. Wenn Sie beispielsweise möchten, dass der Untersuchungsbereich den Ordner „Downloads“ für alle Benutzerkonten auf dem Computer umfasst, geben Sie folgende Maske ein: `C:\Users\*\Downloads\`.
	
	  Kaspersky Endpoint Security unterstützt Umgebungsvariablen
	
	  Die Umgebungsvariable `%userprofile%` wird von Kaspersky Endpoint Security nicht unterstützt, wenn mit der Kaspersky Security Center-Konsole eine Liste mit Ausnahmen erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen * verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten.
	
	• Um den Namen des Objekttyps einzugeben, verwenden Sie die Klassifikation der Kaspersky-Enzyklopädie (z. B. `Email-Worm`, `Rootkit` oder `RemoteAdmin`). Möglich sind auch Masken mit dem Zeichen `?` (Platzhalter für ein beliebiges Einzelzeichen) und dem Zeichen `*` (Platzhalter für eine beliebige Anzahl von Zeichen). Beispiel: Bei Angabe der Maske `Client*` schließt das Programm die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.
	
	Kaspersky Endpoint Security blendet die Liste der Untersuchungsausnahmen in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration von Untersuchungsausnahmen in der Konsole blockiert (Symbol „geschlossenes Schloss“) und lokale Untersuchungsausnahmen verboten sind (das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben** ist deaktiviert).

Vertrauenswürdige Programme	Tabelle mit vertrauenswürdigen Programmen, deren Aktivität von Kaspersky Endpoint Security nicht untersucht wird. Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske. Die Umgebungsvariable `%userprofile%` wird von Kaspersky Endpoint Security nicht unterstützt, wenn eine Liste mit vertrauenswürdigen Programmen in der Kaspersky Security Center-Konsole erstellt wird. Um den Eintrag auf alle Benutzerkonten anzuwenden, können Sie das Zeichen `*` verwenden (z. B. `C:\Users\*\Documents\File.exe`). Nach jeder Eingabe einer neuen Umgebungsvariablen müssen Sie das Programm neu starten. Die Komponente „Programmkontrolle“ reguliert den Start aller Programme unabhängig davon, ob ein Programm in der Tabelle der vertrauenswürdigen Programme angegeben ist oder nicht. Kaspersky Endpoint Security blendet die konsolidierte Liste für vertrauenswürdige Programme in der App-Benutzeroberfläche aus, wenn der Administrator die Konfiguration vertrauenswürdiger Programme in der Konsole blockiert (Symbol „geschlossenes Schloss“) und lokale vertrauenswürdige Programme verboten sind (das Kontrollkästchen **Verwendung lokaler vertrauenswürdiger Programme erlauben** ist deaktiviert).
Bei Vererbung Werte zusammenführen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Dadurch wird die Liste der Untersuchungsausnahmen und vertrauenswürdigen Programme in den übergeordneten und untergeordneten Richtlinien von Kaspersky Security Center zusammengeführt. Um Listen zusammenzuführen, muss die untergeordnete Richtlinie so konfiguriert werden, dass sie die Einstellungen der übergeordneten Richtlinie von Kaspersky Security Center erbt. Wenn das Kontrollkästchen aktiviert ist, werden Listenelemente aus der übergeordneten Richtlinie von Kaspersky Security Center in untergeordneten Richtlinien angezeigt. Auf diese Weise können Sie z. B. eine konsolidierte Liste der vertrauenswürdigen Programme für die gesamte Organisation erstellen. Vererbte Listenelemente in einer untergeordneten Richtlinie können nicht gelöscht oder bearbeitet werden. Elemente auf der Liste der Untersuchungsausnahmen und der Liste der vertrauenswürdigen Programme, die während der Vererbung zusammengeführt werden, können nur in der übergeordneten Richtlinie gelöscht und bearbeitet werden. Sie können Listenelemente in untergeordneten Richtlinien hinzufügen, bearbeiten oder löschen. Wenn Elemente auf Listen der untergeordneten und übergeordneten Richtlinie übereinstimmen, werden diese Elemente als dasselbe Element der übergeordneten Richtlinie angezeigt. Wenn das Kontrollkästchen deaktiviert ist, werden die Elemente der Listen mit vertrauenswürdigen Geräten bei der Vererbung der Einstellungen der Richtlinien für Kaspersky Security Center nicht zusammengefasst. Mit dieser Funktionalität können Listen auch in Richtlinienprofilen zusammengeführt werden. Um Listen im Profil mit der höchsten Priorität zusammenzuführen, aktivieren Sie die Vererbung der Einstellungen aus einem Profil mit niedrigerer Priorität. Details über die Prioritäten von Richtlinienprofilen finden Sie in der Hilfe zu Kaspersky Security Center.
Verwendung lokaler Ausnahmen erlauben / **Verwendung lokaler vertrauenswürdiger Programme erlauben** *(nur in der Konsole von Kaspersky Security Center verfügbar)*	*Lokale Ausnahmen und lokale vertrauenswürdige Programme (lokale vertrauenswürdige Zone)* – benutzerdefinierte Liste von Objekten und Programmen in Kaspersky Endpoint Security für einen bestimmten Computer. Kaspersky Endpoint Security überwacht keine Objekte und Programme aus der lokalen vertrauenswürdigen Zone. Auf diese Weise können Benutzer zusätzlich zu der allgemeinen vertrauenswürdigen Zone in einer Richtlinie ihre eigenen lokalen Listen mit Ausnahmen und vertrauenswürdigen Programmen erstellen. Wenn das Kontrollkästchen aktiviert ist, kann ein Benutzer eine lokale Liste von Untersuchungsausnahmen und eine lokale Liste von vertrauenswürdigen Programmen erstellen. Ein Administrator kann das Kaspersky Security Center verwenden, um Listenelemente in den Computereigenschaften anzuzeigen, hinzuzufügen, zu bearbeiten oder zu löschen. Wenn das Kontrollkästchen deaktiviert ist, kann der Benutzer nur auf die allgemeine Liste der in der Richtlinie generierten Untersuchungsausnahmen und vertrauenswürdigen Programme zugreifen.
Telemetrie für EDR (KATA)/NDR (KATA) *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Diese Tabelle enthält Informationen über die EDR-Telemetrie-Ausnahmen.

Telemetrie für KUMA *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Liste der Ereignisse, die an Kaspersky Unified Monitoring and Analysis Platform (KUMA) gesendet werden sollen. Kaspersky Endpoint Security funktioniert in den folgenden Modi: • **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.
Vertrauenswürdiger Zertifikatspeicher des Systems	Wenn einer der vertrauenswürdigen Zertifikatspeicher des Systems ausgewählt wird, schließt Kaspersky Endpoint Security die Programme, die mit einer vertrauenswürdigen digitalen Signatur signiert sind, von Untersuchungen aus. Kaspersky Endpoint Security weist solche Programme automatisch der Gruppe **Vertrauenswürdig** zu. Wenn **Nicht verwenden** ausgewählt ist, untersucht Kaspersky Endpoint Security die Programme, unabhängig davon, ob sie eine digitale Signatur haben oder nicht. Welcher Sicherheitsgruppe Kaspersky Endpoint Security ein Programm zuweist, ist von der Gefahrenstufe abhängig, die dieses Programm für den Computer darstellen kann.

Programmeinstellungen

Sie können die folgenden allgemeinen Programmeinstellungen anpassen:

- Funktionsmodus
- Selbstschutz
- Leistung
- Debug-Informationen;
- Computerstatus beim Anwenden der Einstellungen

Programmeinstellungen

Einstellung	Beschreibung
Programm beim Hochfahren des Computers starten (empfohlen)	Ist diese Option ausgewählt, so wird Kaspersky Endpoint Security nach dem Laden des Betriebssystems gestartet und schützt den Computer während der gesamten Sitzung. Ist diese Option deaktiviert, so wird Kaspersky Endpoint Security nach dem Hochfahren des Betriebssystems nicht automatisch gestartet. Das Programm muss vom Benutzer manuell gestartet werden. Der Schutz des Computers ist deaktiviert, was ein Risiko für die Daten des Benutzers darstellt.
Technologie zur aktiven Desinfektion verwenden (beansprucht die Computerressourcen erheblich)	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*. Dann müssen Sie eine Aufgabe *Schadsoftware-Untersuchung* starten.

Einstellung	Beschreibung
Kaspersky Security Center als Proxyserver für die Aktivierung verwenden *(nur in der Konsole von Kaspersky Security Center verfügbar)*	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 Sie einen Aktivierungscode verwenden, um die App in einem isolierten Netzwerksegment ohne Internetzugang zu aktivieren. Wenn Sie die App mit einer Schlüsseldatei aktivieren, ist kein Internetzugang erforderlich.
Selbstschutz aktivieren	Wenn diese Funktionalität aktiviert ist, verhindert Kaspersky Endpoint Security, dass Programmdateien auf der Festplatte, Prozesse im Arbeitsspeicher und Einträge in der Systemregistrierung verändert oder gelöscht werden.
Externe Verwaltung von Programmdiensten blockieren	Wenn diese Funktionalität aktiviert ist, verbietet Kaspersky Endpoint Security die Verwaltung von Programmdiensten mithilfe von Drittanbieter-Anwendungen (z. B. CMD). Wenn versucht wird, die Programmdienste über Drittanbieter-Programme zu verwalten, erscheint eine entsprechende Meldung über dem Programmsymbol im Infobereich der Microsoft Windows-Taskleiste (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde). Sie können die externe Verwaltung von Programmdiensten nur auf Computern erlauben, die die AM-PPL-Technologie nicht unterstützen, oder auf Computern, auf denen diese Technologie deaktiviert ist.
Geplante Aufgaben bei Akkubetrieb aufschieben	Wenn dieses Kontrollkästchen aktiviert ist, wird der Energiesparmodus aktiviert, sobald der Computer in den Akkubetrieb wechselt. Kaspersky Endpoint Security schiebt geplante Aufgaben auf. 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: • *Vollständige Untersuchung*. • *Untersuchung wichtiger Bereiche*. • *Benutzerdefinierte Untersuchung*. • *Prüfung der Anwendungsintegrität*. • *IOC-Untersuchung*. • *Update der Datenbanken und Programm-Module* (nur Patches) Die Anwendung überspringt geplante Datenbanken-Updates nur dann, wenn der Laptop im Akkubetrieb läuft und der Akkuladestand unter 30 % liegt (Standardwert). Sie können durch Bearbeiten der Registrierung den Mindestakkuladestand ändern, ab dem die Anwendung beginnt, geplante Updates der Antiviren-Datenbanken zu überspringen. In allen anderen Fällen aktualisiert Kaspersky Endpoint Security die Datenbanken nach Zeitplan, unabhängig davon, ob sich der Laptop im Netz- oder Akkubetrieb befindet oder ob die Anwendung im Energiesparmodus läuft.
Ressourcen für andere Programme freigeben	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.
CPU-Auslastung für Untersuchungsaufgaben begrenzen	Um die Leistung von Kaspersky Endpoint Security zu optimieren, können Sie die CPU-Auslastung durch die Aufgabe *Schadsoftware-Untersuchung* begrenzen. Ist das Kontrollkästchen aktiviert, wird die durchschnittliche Belastung aller CPU-Kerne durch die Aufgabe *Schadsoftware-Untersuchung* dem angegebenen Wert angeglichen. Das Kontrollkästchen ist standardmäßig deaktiviert.
Dump-Aufzeichnung aktivieren	Ist das Kontrollkästchen aktiviert, so erstellt Kaspersky Endpoint Security Dump-Dateien, wenn das Programm abstürzt. Ist das Kontrollkästchen deaktiviert, so erstellt Kaspersky Endpoint Security keine Dump-Dateien. Das Programm löscht Speicherabbilder, die bereits auf der Festplatte des Computers vorhanden sind.

Einstellung	Beschreibung
Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren	Ist das Kontrollkästchen aktiviert, so besitzen folgende Personen Zugriff auf Dump-Dateien: Systemadministrator und lokaler Administrator, und der Benutzer, der die Aufzeichnung von Dump- und Protokolldateien aktiviert hat. Zugriff auf Protokolldateien besitzen nur der Systemadministrator und der lokale Administrator. Ist dieses Kontrollkästchen deaktiviert, so besitzen beliebige Benutzer Zugriff auf Dump-Dateien und Protokolldateien.
Computerstatus beim Anwenden von Einstellungen *(nur in der Konsole von Kaspersky Security Center verfügbar)*	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*.
Updates ohne Computer-Neustart installieren	Wenn das App-Upgrade ohne Computerneustart erfolgt, ist gewährleistet, dass der Betrieb der Server nicht unterbrochen wird. Ein Programm-Upgrade ohne Neustart ist ab Version 11.10.0 möglich. Beim Upgrade älterer Programmversionen müssen Sie den Computer neu starten. Ab Version 11.11.0 können Sie die folgenden Aktionen ausführen, ohne den Computer neu zu starten: • Patches installieren • Auswahl der App-Komponenten ändern • Kaspersky Endpoint Security über Kaspersky Security für Windows Server installieren 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 *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Sollte bei der Verwendung von Kaspersky Endpoint Security zusammen mit Fernverwaltungs-Tools (RAT) Probleme auftreten, können Sie den Kompatibilitätsmodus aktivieren. Die Probleme können darauf zurückgehen, dass ein Fernverwaltungs-Tool mit der Programmfunktionalität „Secure Desktop“ inkompatibel ist. 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. Wenn diese Option ausgewählt wird, ist der RAT-Kompatibilitätsmodus aktiviert. Die Anwendung zeigt einen Bestätigungsdialog an, ohne diese Funktionalität zu verwenden. Dadurch 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. Wenn diese Option deaktiviert ist, ist der RAT-Kompatibilitätsmodus deaktiviert. Das Kontrollkästchen 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.

Berichte und Speicher

Berichte

In den 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.

Berichte werden im Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\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 Ordner `C:\ProgramData\Kaspersky Lab\KES.14.2\QB` gespeichert.

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.

In Kaspersky Endpoint Security können die Zugriffsrechte für Benutzer auf die Backup-Kopien von Dateien nicht angepasst werden.

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. Unter Quarantäne stehende Dateien werden in verschlüsselter Form gespeichert und gefährden die Sicherheit des Gerätes nicht. Kaspersky Endpoint Security verwendet die Quarantäne nur dann, wenn das Programm in Kaspersky Detection and Response-Lösungen integriert ist. In anderen Fällen legt Kaspersky Endpoint Security die entsprechende Datei im Backup ab. Ausführliche Informationen zur Verwaltung der Quarantäne als Teil dieser Lösungen finden Sie in der Hilfe zu Kaspersky Sandbox, Hilfe zu Kaspersky Endpoint Detection and Response Optimum, Hilfe zu Kaspersky Endpoint Detection and Response Expert, Hilfe zu Kaspersky Anti Targeted Attack Platform, und Hilfe zu Kaspersky Endpoint Detection and Response Expert (on-premises).

Die Quarantäne kann nur über die „Web Console“ konfiguriert werden. Mit der „Web Console“ können Sie unter Quarantäne stehende Objekte auch verwalten (z. B. wiederherstellen, löschen oder hinzufügen). Sie können Objekte über die Befehlszeile lokal auf dem Computer wiederherstellen.

Kaspersky Endpoint Security verwendet das Systemkonto (SYSTEM), um Dateien unter Quarantäne zu stellen.

Einstellungen für Berichte und Speicher

Einstellung	Beschreibung
Berichte löschen nach (Tagen)	Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Berichte durch das festgelegte Zeitintervall beschränkt. Die maximale Speicherdauer für Berichte beträgt standardmäßig 30 Tage. Nach Ablauf dieses Zeitraums löscht Kaspersky Endpoint Security automatisch die ältesten Einträge aus der Berichtsdatei.
Maximale Größe der Berichtsdatei (MB)	Ist das Kontrollkästchen aktiviert, so ist die maximale Größe der Berichtsdatei durch den festgelegten Wert beschränkt. Die maximale Dateigröße beträgt standardmäßig 1024 MB. 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.
Objekte löschen nach (Tagen)	Ist das Kontrollkästchen aktiviert, so ist die maximale Speicherdauer für Dateien durch das festgelegte Zeitintervall beschränkt. Die maximale Speicherdauer für Dateien beträgt standardmäßig 30 Tage. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Endpoint Security die ältesten Dateien aus dem Backup.
Maximale Größe des Backup-Speichers (MB)	Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 1024 MB. 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.

Einstellung	Beschreibung
Maximale Größe der Quarantäne	Wenn das Kontrollkästchen aktiviert ist, ist die Quarantäne-Größe auf den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 1024 MB. Wenn die maximale Quarantäne-Größe erreicht wird, sendet Kaspersky Endpoint Security das Ereignis *Zu wenig Platz im Quarantäne-Speicher* an Kaspersky Security Center und veröffentlicht das Ereignis im Windows-Ereignisprotokoll. 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 Kaspersky Endpoint Security ein entsprechendes Ereignis an Kaspersky Security Center und veröffentlicht das Ereignis im Windows-Ereignisprotokoll. Die Anwendung stellt weiterhin neue Objekte unter Quarantäne.
Datenübertragung an den Administrationsserver *(nur in Kaspersky Security Center verfügbar)*	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: • **Über Quarantäne-Dateien**. Eine Liste der Quarantäne-Dateien können Sie in der Kaspersky Security Center-Konsole im Ordner **Erweitert** → **Datenverwaltung** → **Quarantäne** einsehen. Kaspersky Endpoint Security verwendet die Quarantäne nur dann, wenn das Programm in Kaspersky Detection and Response-Lösungen integriert ist. • **Über Backup-Dateien**. Eine Liste der Backup-Dateien können Sie in der Kaspersky Security Center-Konsole im Ordner **Erweitert** → **Datenverwaltung** → **Backup** einsehen. • **Über nicht verarbeitete Dateien**. Eine Liste der unverarbeiteten Dateien können Sie in der Kaspersky Security Center-Konsole im Ordner **Erweitert** → **Datenverwaltung** → **Aktive Bedrohungen** einsehen. • **Über installierte Geräte**. Eine Liste der verbundenen Geräte können Sie in Kaspersky Security Center im Ordner **Erweitert** → **Datenverwaltung** → **Hardware** einsehen. Die Liste der Geräte ist auch in den Computereigenschaften und in der Richtlinie für Kaspersky Endpoint Security für Windows (Abschnitt **Gerätekontrolle**) verfügbar. • **Über gestartete Programme**. Eine Liste der ausführbaren Dateien können Sie in der Kaspersky Security Center-Konsole im Ordner **Erweitert** → **Programmverwaltung** → **Ausführbare Dateien** einsehen. Die Liste der ausführbaren Dateien ist auch in den Computereigenschaften verfügbar. • **Über Fehler bei der Dateiverschlüsselung**. Eine Liste der Fehler bei der Dateiverschlüsselung können Sie in der Kaspersky Security Center-Konsole im Ordner **Erweitert** → **Verschlüsselung und Datenschutz** → **Verschlüsselungsereignisse** einsehen. Die Fehlerliste ist auch in den Computereigenschaften verfügbar. • **Statusbericht für Regeln der „Adaptiven Kontrolle von Anomalien“**. Diesen Bericht können Sie in der Kaspersky Security Center-Konsole im Knoten **Administrationsserver** auf der Registerkarte **Berichte** einsehen. Dieser Bericht ist auch in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows verfügbar (Abschnitt **Adaptive Kontrolle von Anomalien**). • **Bericht über ausgelöste Regeln der „Adaptiven Kontrolle von Anomalien“**. Diesen Bericht können Sie in der Kaspersky Security Center-Konsole im Knoten **Administrationsserver** auf der Registerkarte **Berichte** einsehen. Dieser Bericht ist auch in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows verfügbar (Abschnitt **Adaptive Kontrolle von Anomalien**). • **Über eine Bedrohungsentwicklungskette**. Details über solche Funde können Sie in Kaspersky Security Center Web Console im Abschnitt **Überwachung** → **Alarme** einsehen. Die Informationen über die Entwicklungskette einer Bedrohung werden von Kaspersky Endpoint Detection and Response-Lösungen verwendet.

Netzwerkeinstellungen

Sie können die Proxyserver-Einstellungen für die Internetverbindung und das Update der Antiviren-Datenbanken konfigurieren, einen Modus für die Überwachung von Netzwerkports auswählen und die Untersuchung verschlüsselter Verbindungen einrichten.

Einstellung	Beschreibung
Datenverkehr bei getakteter Verbindung beschränken	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	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. Ohne dieses Skript können Sie die Überwachung der Internet-Aktivitäten der Benutzer nicht aktivieren. Kaspersky-Experten empfehlen, dieses Webseiten-Interaktionsskript in den Datenverkehr einzuspeisen, um den korrekten Betrieb der Web-Kontrolle zu gewährleisten.
Proxyserver-Einstellungen	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. Um einen Proxyserver automatisch anzupassen, verwendet Kaspersky Endpoint Security das WPAD-Protokoll (Web Proxy Auto-Discovery Protocol). Wenn die IP-Adresse des Proxyservers mit diesem Protokoll nicht ermittelt werden kann, verwendet das Programm die Proxyserver-Adresse, die in den Einstellungen des Browsers Microsoft Internet Explorer angegeben ist.
Einen Proxyserver für lokale Adressen umgehen	Ist dieses Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security keinen Proxyserver, wenn ein Update aus einem gemeinsamen Ordner erfolgt.
Einstellungen für die Proxyserver-Authentifizierung	Um das Programm auf dem Proxyserver für den Internetzugang zu authentifizieren, müssen Sie die Anmeldedaten des Benutzers eingeben. Kaspersky Endpoint Security unterstützt die automatische Authentifizierung am Proxyserver. Wenn die automatische Authentifizierung fehlschlägt, fordert das Programm Sie zur Eingabe der Anmeldedaten auf. **Keine Authentifizierung verwenden**. **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. Um sicherzustellen, dass die Kerberos-Authentifizierung korrekt funktioniert, wenn CNAME-Einträge für die Proxyserver-Adresse verwendet werden, müssen Sie für jeden CNAME-Eintrag einen Dienstprinzipalnamen (SPN) registrieren. **Kerberos-Authentifizierung mit Benutzername und Kennwort**. Kerberos-Authentifizierung mit manuell angegebenen Anmeldedaten. Wenn die Kerberos-Authentifizierung ausgewählt ist, kann Kaspersky Endpoint Security abhängig von den Proxyserver-Einstellungen die Authentifizierung anhand des Kerberos- oder NTLM-Protokolls durchführen.
Überwachte Ports	**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. **Alle Ports für Programme überwachen, die auf der von Kaspersky empfohlenen Liste stehen**. Es wird eine vordefinierte Liste mit Programmen verwendet, deren Netzwerkports von Kaspersky Endpoint Security überwacht werden. Diese Liste enthält z. B. Google Chrome, Adobe Reader, Java und andere Programme. **Alle Ports für die angegebenen Programme überwachen**. Es wird eine Liste mit Programmen verwendet, deren Netzwerkports von Kaspersky Endpoint Security überwacht werden.

Einstellung	Beschreibung
Untersuchung verschlüsselter Verbindungen	Kaspersky Endpoint Security untersucht den verschlüsselten Netzwerkverkehr, der über die folgenden Protokolle übertragen wird: • SSL 3.0; • TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3. Kaspersky Endpoint Security unterstützt die folgenden Untersuchungsmodi für verschlüsselte Verbindungen: • **Verschlüsselte Verbindungen nicht untersuchen**. Kaspersky Endpoint Security kann nicht auf Inhalte von Websites zugreifen, deren Adressen mit `https://` beginnen. • **Verschlüsselte Verbindungen auf Anfrage von Schutzkomponenten untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr nur, wenn die Untersuchung von den Komponenten „Schutz vor Web-Bedrohungen", „Schutz vor E-Mail-Bedrohungen" und „Web-Kontrolle" angefordert wird. • **Verschlüsselte Verbindungen immer untersuchen**. Kaspersky Endpoint Security untersucht den verschlüsselten Datenverkehr auch dann, wenn die Schutzkomponenten deaktiviert sind. Kaspersky Endpoint Security überprüft keine geschützten Verbindungen, die von vertrauenswürdigen Programmen hergestellt wurden, für die die Überprüfung des Datenverkehrs deaktiviert ist. Kaspersky Endpoint Security untersucht keine geschützten Verbindungen aus der vordefinierten Liste der vertrauenswürdigen Websites. Die vordefinierte Liste der vertrauenswürdigen Websites wird von Kaspersky-Experten erstellt. Diese Liste wird mit den Antiviren-Datenbanken des Programms aktualisiert. Sie können die vordefinierte Liste der vertrauenswürdigen Websites nur in der Oberfläche von Kaspersky Endpoint Security anzeigen. Sie können die Liste in der Konsole von Kaspersky Security Center nicht anzeigen.
Vertrauenswürdige Stammzertifikate	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.
Besuch einer Domäne mit nicht vertrauenswürdigem Zertifikat	• **Erlauben**. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat erfolgt, erlaubt Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite enthält eine Warnung und Informationen über den Grund, aus welchem ein Besuch dieser Domäne als riskant gilt. Die HTML-Seite mit der Warnmeldung enthält einen Link, mit dessen Hilfe der Benutzer auf die angeforderte Webressource zugreifen kann. Wenn eine Drittanbieter-Anwendung oder ein Drittanbieter-Dienst eine Verbindung zu einer Domäne mit einem nicht vertrauenswürdigen Zertifikat herstellt, erstellt Kaspersky Endpoint Security ein eigenes Zertifikat für die Untersuchung des Datenverkehrs. Das neue Zertifikat hat den Status *Nicht vertrauenswürdig*. Dies ist notwendig, um die Drittanbieter-Anwendung vor der nicht vertrauenswürdigen Verbindung zu warnen, da die HTML-Seite in diesem Fall nicht angezeigt und die Verbindung im Hintergrundmodus hergestellt werden kann. • **Blockieren**. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat erfolgt, blockiert Kaspersky Endpoint Security den Aufbau einer Netzwerkverbindung. Wenn ein Wechsel zu einer Domäne mit nicht vertrauenswürdigem Zertifikat in einem Browser erfolgt, so zeigt Kaspersky Endpoint Security eine HTML-Seite an. Diese Seite informiert über den Grund, aus dem der Wechsel zu dieser Domäne blockiert wurde.
Beim Besuch einer Domäne mit Untersuchungsfehler wegen verschlüsselten Verbindungen	• **Blockieren**. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, blockiert Kaspersky Endpoint Security die Netzwerkverbindung. • **Erlauben und Domäne zu Ausnahmen hinzufügen**. Wenn bei der Untersuchung einer verschlüsselten Verbindung ein Fehler auftritt, fügt Kaspersky Endpoint Security die Domäne zur Liste der Domänen mit Untersuchungsfehlern hinzu und überwacht den verschlüsselten Netzwerkverkehr beim Besuch dieser Domäne nicht. Die Anzeige einer Liste der Domänen mit Untersuchungsfehlern bei geschützten Verbindungen ist nur auf der lokalen Programmoberfläche möglich. Um den Inhalt der Liste zurückzusetzen, wählen Sie das Element **Blockieren** aus. Kaspersky Endpoint Security generiert auch ein Ereignis für den Fehler bei der Untersuchung der verschlüsselten Verbindung.
SSL 2.0-Verbindungen blockieren	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.
SSL 3.0-Verbindungen blockieren	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.

Einstellung	Beschreibung
TLS 1.0-Verbindungen blockieren	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.
Verschlüsselte Verbindung mit einer Website, die ein EV-Zertifikat verwendet, entschlüsseln	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. Ist das Kontrollkästchen aktiviert, werden geschützte Verbindungen, die ein EV-Zertifikat verwenden, vom Programm entschlüsselt und überwacht. Ist das Kontrollkästchen deaktiviert, hat Kaspersky Endpoint Security keinen Zugriff auf den Inhalt des HTTPS-Datenverkehrs. Deshalb kontrolliert das Programm den HTTPS-Datenverkehr nur nach 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.
Vertrauenswürdige Adressen konfigurieren	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. Kaspersky Endpoint Security unterstützt das Symbol `*` bei IP-Adressen nicht. Sie können eine breite Auswahl an IP-Adressen mithilfe einer Subnetz-Maske auswählen (zum Beispiel 198.51.100.0/24). Beispiele: • `domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Der Eintrag umfasst keine Unterdomänen (z. B. `subdomain.domain.com`). • `subdomain.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`. • `*.domain.com` – Der Eintrag umfasst die folgenden Adressen: `https://movies.domain.com`, `https://images.domain.com/page123`. Der Eintrag umfasst ausschließlich die Domäne `domain.com`.
Vertrauenswürdige Programme konfigurieren	Liste mit Programmen, deren Aktivität von Kaspersky Endpoint Security nicht untersucht wird. Sie können die Typen der Programmaktivität auswählen, die Kaspersky Endpoint Security nicht überwachen soll (z. B. Datenverkehr nicht untersuchen). Kaspersky Endpoint Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske.
Folgenden Speicher verwenden, um verschlüsselte Verbindungen in Anwendungen mit eigenem Zertifikatspeicher zu untersuchen *(nur in der Kaspersky Endpoint Security-Oberfläche verfügbar)*	Ist dieses Kontrollkästchen aktiviert, untersucht das Programm den verschlüsselten Datenverkehr im Browser Mozilla Firefox und im Mail-Client Thunderbird. Der Zugriff auf einige Websites über das HTTPS-Protokoll ist möglicherweise gesperrt. Um den Datenverkehr im Browser Mozilla Firefox und im E-Mail-Client Thunderbird zu untersuchen, müssen Sie die Untersuchung verschlüsselter Verbindungen aktivieren. Wenn die Untersuchung verschlüsselter Verbindungen deaktiviert ist, untersucht das Programm den Datenverkehr im Browser Mozilla Firefox und im E-Mail-Client Thunderbird nicht. Das Programm verwendet das Kaspersky-Stammzertifikat, um den verschlüsselten Datenverkehr zu entschlüsseln und zu analysieren. Sie können den Zertifikatspeicher auswählen, in dem das Kaspersky-Stammzertifikat abgelegt werden soll. • **Windows-Zertifikatspeicher (empfohlen)**. Das Kaspersky-Stammzertifikat wird zu diesem Speicher hinzugefügt, während Kaspersky Endpoint Security installiert wird. • **Eigener Zertifikatspeicher**. Mozilla Firefox und Thunderbird verwenden ihre eigenen Zertifikatspeicher. Wenn der Mozilla-Zertifikatspeicher ausgewählt ist, müssen Sie das Kaspersky-Stammzertifikat in den Browser-Eigenschaften manuell zu diesem Speicher hinzufügen.

Benutzeroberfläche

Sie können die Einstellungen der Programmoberfläche anpassen.

Einstellungen der Benutzeroberfläche

Einstellung	Beschreibung
Interaktion mit dem Benutzer *(nur in der Konsole von Kaspersky Security Center verfügbar)*	**Vereinfachte Programmoberfläche anzeigen**. Das Programmhauptfenster ist auf dem Client-Computer nicht verfügbar. Nur das Symbol im Infobereich der Windows-Taskleiste ist verfügbar. Der Benutzer kann im Kontextmenü des Symbols eine beschränkte Auswahl von Vorgängen mit Kaspersky Endpoint Security ausführen. Außerdem zeigt Kaspersky Endpoint Security über dem Anwendungssymbol nur Benachrichtigungen an, die das Eingreifen des Benutzers erfordern. **Benutzeroberfläche anzeigen**. Auf dem Client-Computer sind das Hauptfenster von Kaspersky Endpoint Security und das Symbol im Infobereich der Windows-Taskleiste verfügbar. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Endpoint Security ausführen. Kaspersky Endpoint Security zeigt Benachrichtigungen über dem Programmsymbol an. **Abschnitt „Aktivitätsmonitor für Programme“ ausblenden**. Die Schaltfläche **Aktivitätsmonitor für Programme** ist auf dem Client-Computer im Hauptfenster von Kaspersky Endpoint Security nicht verfügbar. Der *Aktivitätsmonitor für Programme* dient dazu, in Echtzeit Informationen über die Aktivität von Programmen auf einem Benutzercomputer anzuzeigen. **Benutzeroberfläche nicht anzeigen**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Endpoint Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar.
Auf lokale Aufgaben zugreifen	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. Wenn dieses Kontrollkästchen deaktiviert ist, werden lokale Aufgaben in der Programmoberfläche ausgeblendet. 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	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	Wenn das Kontrollkästchen aktiviert ist, können Benutzer die in der Kaspersky Security Center-Konsole angegebenen 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: Entweder startet Kaspersky Endpoint Security die geplanten Aufgaben automatisch oder der Administrator startet die Aufgaben manuell über die Kaspersky Security Center-Konsole.
Benachrichtigungen konfigurieren	Tabelle mit Einstellungen für die Benachrichtigungen über unterschiedliche Ereigniskategorien. Diese Ereignisse können den Betrieb einer Komponente oder des gesamten Programms sowie die Ausführung einer Aufgabe betreffen. Die Benachrichtigungen über diese Ereignisse werden von Kaspersky Endpoint Security auf dem Bildschirm angezeigt, per E-Mail gesendet oder in Protokollen gespeichert.

Einstellung	Beschreibung
E-Mail-Benachrichtigungen konfigurieren	Einstellungen des SMTP-Servers für den Versand von Benachrichtigungen über Ereignisse, die im Programm registriert werden. Kaspersky Endpoint Security verwendet standardmäßig die E-Mail-Benachrichtigungseinstellungen von Kaspersky Security Center. Weitere Informationen über die E-Mail-Benachrichtigungseinstellungen finden Sie in der Hilfe zu Kaspersky Security Center. Um eine individuelle E-Mail-Benachrichtigung anzupassen, können Sie die folgenden Einstellungen bearbeiten: • **Absenderadresse**. E-Mail-Adresse des Absenders. Es wird davon abgeraten, eine nicht vorhandene Adresse zu verwenden. • **SMTP-Server**. Eine oder mehrere Adressen von E-Mail-Servern Ihres Unternehmens (z. B. `mail.company.com`). Sie können eine IP-Adresse eingeben (IPv4 oder IPv6). Um den Benutzer auf dem SMTP-Server zu authentifizieren, tragen Sie die Anmeldedaten des Absenders in die entsprechenden Felder ein. Um die E-Mail-Benachrichtigungen zu testen, können Sie eine Testnachricht senden. • **Empfängeradresse**. E-Mail-Adressen der Empfänger, an die die Anwendung Benachrichtigungen sendet. • **Versandmodus**. Versandmodus für E-Mail-Benachrichtigungen. Kaspersky Endpoint Security kann Nachrichten entweder sofort senden, wenn ein Ereignis eintritt, oder einen vorkonfigurierter Zeitplan verwenden.
Programmstatus im Infobereich der Taskleiste anzeigen	Kategorien der Programmereignisse, bei deren Eintreten sich das Symbol von Kaspersky Endpoint Security im Infobereich der Microsoft-Windows-Taskleiste ändert (oder).
Statusmeldungen der lokalen Anti-Malware-Datenbanken	Einstellungen für die Benachrichtigungen über veraltete Antiviren-Datenbanken, die vom Programm verwendet werden.
Kennwortschutz	Ist der Schalter aktiviert, so fragt Kaspersky Endpoint Security nach dem Kennwort, wenn der Benutzer versucht, einen Vorgang auszuführen, der zum Gültigkeitsbereich des „Kennwortschutzes“ gehört. Der Gültigkeitsbereich des „Kennwortschutzes“ umfasst verbotene Vorgänge (z. B. Deaktivierung von Schutzkomponenten) und Benutzerkonten, die zum Gültigkeitsbereich des „Kennwortschutzes“ gehören. Nachdem der Kennwortschutz aktiviert wurde, fordert Kaspersky Endpoint Security dazu auf, ein Kennwort für das KLAdmin-Benutzerkonto festzulegen.
Support für Benutzer / Links zu Websites *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Liste mit Links für Websites mit Informationen über den Technischen Support für das Programm Kaspersky Endpoint Security. Die hinzugefügten Links werden im Fenster **Support** der lokalen Benutzeroberfläche von Kaspersky Endpoint Security anstelle der Standardlinks angezeigt.
Support für Benutzer / Beschreibung *(nur in der Konsole von Kaspersky Security Center verfügbar)*	Nachricht, die im Fenster **Support** der lokalen Oberfläche von Kaspersky Endpoint Security erscheint.

Einstellungen verwalten

Sie können die aktuellen Einstellungen von Kaspersky Endpoint Security in einer Datei speichern und diese zur schnellen Konfiguration des Programms auf einem anderen Computer verwenden. Sie können auch eine Konfigurationsdatei verwenden, wenn Sie das Programm über Kaspersky Security Center mit einem Installationspaket bereitstellen. Sie können die Standardeinstellungen jederzeit wiederherstellen.

Die Einstellungen für die Verwaltung der Programmkonfiguration sind nur in der Benutzeroberfläche von Kaspersky Endpoint Security verfügbar.

Einstellungen zur Verwaltung der Programmkonfiguration

Einstellungen	Beschreibung
Import	Laden der Einstellungen für die Ausführung des Programms aus Dateien im cfg-Format und ihre Anwendung.
Export	Aktuelle Einstellungen für die Ausführung des Programms in einer Datei im cfg-Format speichern.
Wiederherstellen	Sie können jederzeit die von Kaspersky- empfohlenen Programmeinstellungen wiederherstellen. Wenn die Einstellungen wiederhergestellt werden, wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** festgelegt.

Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Endpoint Security gewährleistet die Aktualität des Computerschutzes. Jeden Tag tauchen neue Viren und andere Schadprogramme auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Endpoint Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) ist in der Software in den USA möglicherweise nicht verfügbar.

Für ein regelmäßiges Update ist eine aktuelle Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Der Computer muss mit dem Internet verbunden sein, um das Update-Paket erfolgreich von den Kaspersky-Update-Servern herunterzuladen. Standardmäßig wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, müssen Sie die Proxyserver-Einstellungen konfigurieren.

Updates werden mit dem HTTPS-Protokoll heruntergeladen. Falls ein Download mit dem HTTPS-Protokoll nicht möglich ist, erfolgt der Download mit dem HTTP-Protokoll.

Bei einer Aktualisierung werden folgende Objekte auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Endpoint Security. Der Computerschutz basiert auf Datenbanken, die Signaturen für Viren und andere bedrohliche Programme, sowie Informationen über entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese Informationen bei der Suche nach und der Desinfektion von infizierten Dateien auf dem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Endpoint Security werden auch die Netzwerktreiber aktualisiert, die gewährleisten, dass die Schutzkomponenten den Netzwerkverkehr abfangen können.

- Programm-Module. Neben den Datenbanken von Kaspersky Endpoint Security können auch die Programm-Module aktualisiert werden. Updates für Programm-Module beheben Schwachstellen von Kaspersky Endpoint Security, fügen neue Funktionen hinzu und optimieren vorhandene Funktionen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version verglichen, die in der Update-Quelle vorliegt. Sind die Datenbanken und Programm-Module nicht aktuell, werden fehlende Teile der Updates auf dem Computer installiert.

Sind die Datenbanken stark veraltet, kann das Update-Paket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Informationen über den aktuellen Status der Datenbanken von Kaspersky Endpoint Security werden im Programmhauptfenster oder in einem Tooltip angezeigt. Den Tooltip sehen Sie, wenn Sie den Mauszeiger über das Programmsymbol im Infobereich bewegen.

Informationen über die Aktualisierungsergebnisse und über alle Ereignisse, die bei der Ausführung einer Update-Aufgabe auftreten, werden im Bericht von Kaspersky Endpoint Security protokolliert.

Wenn das Programm im Light Agent-Modus ausgeführt wird, müssen beim Update der Programm-Datenbanken und Module einige Besonderheiten berücksichtigt werden.

Einstellungen für Programmmodul und Datenbanken-Update

Einstellung	Beschreibung
Zeitplan für das Datenbanken-Update	**Automatisch**. In diesem Startmodus für die Update-Aufgabe prüft das Programm regelmäßig, ob an der Update-Quelle ein neue Update-Pakete vorliegen. Die Häufigkeit, mit der nach einem neuen Update-Paket gesucht wird, kann während Viren-Epidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neues Update-Paket gefunden wird, lädt Kaspersky Endpoint Security es herunter und installiert die Updates auf dem Computer. **Manuell**. In diesem Startmodus für die Update-Aufgabe können Sie die Update-Aufgabe manuell starten. **Nach Zeitplan**. In diesem Startmodus für die Update-Aufgabe führt Kaspersky Endpoint Security das Update nach einem von Ihnen erstellten Zeitplan aus. Bei Auswahl dieses Startmodus für die Update-Aufgabe können Sie das Update von Kaspersky Endpoint Security auch manuell starten.
Übersprungene Aufgaben starten	Ist das Kontrollkästchen aktiviert, startet Kaspersky Endpoint Security die übersprungene Aufgabe, sobald dies möglich ist. Die Aufgabe kann z. B. übersprungen werden, wenn der Computer zur geplanten Startzeit der Aufgabe ausgeschaltet war. Wenn die App die Möglichkeit erhält, versäumte Aufgaben auszuführen, werden die Aufgaben innerhalb eines bestimmten Zeitraums nach dem Zufallsprinzip ausgeführt, um die Auslastung des Computers gleichmäßig zu verteilen. Wenn dieses Kontrollkästchen deaktiviert ist, führt Kaspersky Endpoint Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Update-Quellen	Eine *Update-Quelle* ist eine Ressource, die Updates der Datenbanken und der Programm-Module für Kaspersky Endpoint Security enthält. Zu den Update-Quellen gehören der Kaspersky-Security-Center-Server, die Kaspersky-Update-Server sowie Netzwerkordner und lokale Ordner. Wenn die Kaspersky-Update-Server nicht verfügbar sind, kann Kaspersky Endpoint Security alternative Domänen verwenden, um die Datenbanken und Programm-Module zu aktualisieren. Ausführliche Informationen finden Sie in der Wissensdatenbank der Technischen Supports. Standardmäßig enthält die Liste für Update-Quellen den Server von Kaspersky Security Center und die Kaspersky-Update-Server. Sie können der Liste weitere Update-Quellen hinzufügen. Als Update-Quellen können HTTP- oder FTP-Server oder gemeinsame Ordner angegeben werden. Kaspersky Endpoint Security unterstützt keine Updates von HTTPS-Servern, außer es sind Kaspersky-Update-Server. Wurden mehrere Ressourcen als Update-Quellen gewählt, greift Kaspersky Endpoint Security bei einer Aktualisierung streng der Reihe nach darauf zu. Bei der Update-Aufgabe wird das Update-Paket aus der ersten verfügbaren Update-Quelle verwendet. Standardmäßig verwendet Kaspersky Endpoint Security den Kaspersky Security Center-Server als primäre Update-Quelle. Dadurch wird beim Update Datenverkehr eingespart. Wenn keine Richtlinie auf den Computer angewendet wird, werden in den Einstellungen der lokalen *Update der Datenbanken und Programm-Module*-Aufgabe die Kaspersky-Server als primäre Update-Quelle ausgewählt, da die Anwendung möglicherweise keinen Zugriff auf den Kaspersky Security Center-Server hat. Wenn das Programm im Light Agent-Modus ausgeführt wird, wird ein Ordner auf der SVM als Update-Quelle ausgewählt.
Datenbanken-Updates starten als	Die Update-Aufgabe für Kaspersky Endpoint Security wird standardmäßig im Namen des Benutzers gestartet, mit dessen Rechten Sie sich im Betriebssystem angemeldet haben. Das Update für Kaspersky Endpoint Security kann aber auch aus einer Update-Quelle erfolgen, für welche der Benutzer keine Zugriffsrechte besitzt (z. B. aus einem gemeinsamen Ordner, welcher das Update-Paket enthält) oder für welche die Verwendung der Authentifizierung auf dem Proxyserver nicht angepasst ist. Sie können in den Programmeinstellungen einen Benutzer angeben, der über die entsprechenden Rechte verfügt, und die Update-Aufgabe für Kaspersky Endpoint Security im Namen dieses Benutzers starten.

Einstellung	Beschreibung
Updates für Programm-Module herunterladen	Updates für die Programm-Module gemeinsam mit den Programm-Datenbanken herunterladen. Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Endpoint Security den Benutzer über verfügbare Updates für Programm-Module und aktualisiert im Verlauf von Update-Vorgängen die Programm-Module. Updates für die Programm-Module werden dabei nach folgenden Einstellungen angewendet: • **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security zum Einen kritische Updates der Programm-Module automatisch und zum Andern alle übrigen Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. • **Nur bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Endpoint Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard. Wenn dieses Kontrollkästchen nicht aktiviert ist, benachrichtigt Kaspersky Endpoint Security den Benutzer nicht über verfügbare Updates für Programm-Module und aktualisiert die Programm-Module im Verlauf von Update-Vorgängen nicht. Falls für ein Programm-Modul-Update zuerst ein Lizenzvertrag gelesen und bestätigt werden muss, dann installiert das Programm das Update erst nach der Zustimmung zum Lizenzvertrag. Das Kontrollkästchen ist standardmäßig aktiviert.
Updates in folgenden Ordner kopieren	Ist das Kontrollkästchen aktiviert, so kopiert Kaspersky Endpoint Security das Update-Paket in den gemeinsamen Ordner, der unter dem Kontrollkästchen angegeben ist. Anschließend können die übrigen Computer des lokalen Netzwerks das Update-Paket aus dem gemeinsamen Ordner herunterladen. Dadurch lässt sich Internet-Datenverkehr einsparen, da das Update-Paket nur einmal heruntergeladen werden muss. Standardmäßig ist folgender Ordner angegeben: `C:\ProgramData\Kaspersky Lab\KES.14.2\Update distribution\`.
Proxyserver für Updates *(nur in der Kaspersky Endpoint Security-Oberfläche verfügbar)*	Proxyserver-Einstellungen für den Internetzugang der Benutzer von Client-Computern zum Update von Programmmodulen und Datenbanken. Um einen Proxyserver automatisch anzupassen, verwendet Kaspersky Endpoint Security das WPAD-Protokoll (Web Proxy Auto-Discovery Protocol). Wenn die IP-Adresse des Proxyservers nicht mithilfe dieses Protokolls ermittelt werden kann, verwendet Kaspersky Endpoint Security die Proxyserver-Adresse, die in den Einstellungen des Browsers Microsoft Internet Explorer angegeben ist.
Einen Proxyserver für lokale Adressen umgehen *(nur in der Kaspersky Endpoint Security-Oberfläche verfügbar)*	Ist dieses Kontrollkästchen aktiviert, so verwendet Kaspersky Endpoint Security keinen Proxyserver, wenn ein Update aus einem gemeinsamen Ordner erfolgt.

Anhang 2. Sicherheitsgruppen für Programme

Alle Programme, die auf dem Computer gestartet werden, werden von Kaspersky Endpoint Security in Sicherheitsgruppen eingeteilt. Die Programme werden in Sicherheitsgruppen eingeteilt. Die Einteilung erfolgt nach dem Grad der Bedrohung, die von den jeweiligen Programmen für das Betriebssystem ausgeht.

Es existieren folgende Sicherheitsgruppen:

- **Vertrauenswürdig**. Die Programme, die zu dieser Gruppe gehören, erfüllen eine oder mehrere der folgenden Bedingungen:
  - Die Programme haben die digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält Einträge über die Programme.
  - Der Benutzer hat das Programm in die Gruppe *Vertrauenswürdig* verschoben.

Für diese Programme gibt es keine verbotenen Vorgänge.

- **Schwach beschränkt**. Die Programme, die zu dieser Gruppe gehören, erfüllen folgende Bedingungen:
  - Die Programme haben keine digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält keine Einträge über die Programme.
  - Der Benutzer hat das Programm in die Gruppe *Schwach beschränkt* verschoben.

  Für diese Programme gelten minimale Einschränkungen im Hinblick auf Betriebssystemressourcen.
- **Stark beschränkt**. Die Programme, die zu dieser Gruppe gehören, erfüllen folgende Bedingungen:
  - Die Programme haben keine digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält keine Einträge über die Programme.
  - Der Benutzer hat das Programm in die Gruppe *Stark beschränkt* verschoben.

  Für diese Programme gelten erhebliche Einschränkungen im Hinblick auf Betriebssystemressourcen.
- **Nicht vertrauenswürdig**. Die Programme, die zu dieser Gruppe gehören, erfüllen folgende Bedingungen:
  - Die Programme haben keine digitale Signatur eines vertrauenswürdigen Herstellers.
  - Die Datenbank für vertrauenswürdige Programme von Kaspersky Security Network enthält keine Einträge über die Programme.
  - Der Benutzer hat das Programm in die Gruppe *Nicht vertrauenswürdig* verschoben.

  Für solche Anwendungen sind alle Vorgänge verboten.

Anhang 3. Dateierweiterungen für die schnelle Untersuchung von Wechseldatenträgern

com – ausführbare Programmdatei mit einer Größe von maximal 64 KB

exe – ausführbare Datei, selbstextrahierendes Archiv;

sys – Systemdatei von Microsoft Windows;

prg – Text des Programms dBase™, Clipper oder Microsoft Visual FoxPro®, Programm des Pakets WAVmaker

bin – Binärdatei

bat – Batchdatei

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2

dpl – komprimierte Bibliothek für Borland Delphi

dll – Dynamic Link Library

scr – Bildschirmschonerdatei für Microsoft Windows

cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows

ocx – Microsoft OLE-Objekt (Object Linking and Embedding)

tsp – Programm, das im Timesharing-Modus arbeitet

drv – Gerätetreiber

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät

pif – Datei mit Programminformationen

lnk – Linkdatei für Microsoft Windows

reg – Registrierungsschlüsseldatei für Systemregistrierung von Microsoft Windows

ini – Konfigurationsdatei, die Einstellungsdaten für Microsoft Windows, Windows NT und andere Programme enthält

cla – Java-Klasse

vbs – Visual Basic®-Skript

vbe – BIOS-Video-Erweiterung

js, jse – JavaScript-Quelltext

htm – Hypertext-Dokument

htt – Hypertext-Dokumentvorlage für Microsoft Windows

hta – Hypertext-Programm für Microsoft Internet Explorer®;

asp – Active Server Pages-Skript;

chm – kompilierte HTML-Datei

pht – HTML-Datei mit eingebetteten PHP-Skripten

php – Skript, das in eine HTML-Datei eingebettet wird

wsh – Datei für Microsoft Windows Script Host

wsf – Skript von Microsoft Windows

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei im Format Win Help

msg – E-Mail-Nachricht für Microsoft Mail

plg – E-Mail-Nachricht

mbx – gespeicherte E-Mail-Nachricht für Microsoft Office Outlook

doc* – Dokumente für Microsoft Office Word, z.B.: doc – Dokumente für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung

dot* – Dokumentvorlagen in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro

rtf – Rich Text Format-Dokument

shs – Datenauszug für Windows Shell Scrap Object Handler

dwg – Datenbank für AutoCAD®-Skizzen

msi – Microsoft Windows Installer-Paket

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Dokument für Adobe Acrobat

swf – Objekt für Shockwave® Flash

jpg, jpeg – komprimierte Bilddatei

emf – Enhanced Metafile

ico – Symboldatei für ein Objekt

ov? – ausführbare Dateien für Microsoft Office Word

xl* – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung.

pp* – Dokumente und Dateien für Microsoft Office PowerPoint®, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

md* – Dokumente und Dateien für Microsoft Office Access®, z.B.: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank.

sldx – Folie in Microsoft Office PowerPoint 2007

sldm – Folie in Microsoft Office PowerPoint 2007 mit Makrounterstützung

thmx – Thema in Microsoft Office 2007

Anhang 4. Dateitypen für die Anlagenfilterung im „Schutz vor E-Mail-Bedrohungen"

Beachten Sie, dass das tatsächliche Format einer Datei von dem Format abweichen kann, das die Dateierweiterung angibt.

Wenn Sie die Anlagenfilterung für E-Mail-Nachrichten aktiviert haben, kann die Komponente „Schutz vor E-Mail-Bedrohungen" bei der Filterung Dateien mit folgenden Erweiterungen umbenennen oder löschen:

com – ausführbare Programmdatei mit einer Größe von maximal 64 KB

exe – ausführbare Datei, selbstextrahierendes Archiv;

sys – Systemdatei von Microsoft Windows;

prg – Text des Programms dBase™, Clipper oder Microsoft Visual FoxPro®, Programm des Pakets WAVmaker

bin – Binärdatei

bat – Batchdatei

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2

dpl – komprimierte Bibliothek für Borland Delphi

dll – Dynamic Link Library

scr – Bildschirmschonerdatei für Microsoft Windows

cpl – Systemsteuerungsmodul (control panel) für Microsoft Windows

ocx – Microsoft OLE-Objekt (Object Linking and Embedding)

tsp – Programm, das im Timesharing-Modus arbeitet

drv – Gerätetreiber

vxd – Treiber für ein virtuelles Microsoft Windows-Gerät

pif – Datei mit Programminformationen

lnk – Linkdatei für Microsoft Windows

reg – Registrierungsschlüsseldatei für Systemregistrierung von Microsoft Windows

ini – Konfigurationsdatei, die Einstellungsdaten für Microsoft Windows, Windows NT und andere Programme enthält

cla – Java-Klasse

vbs – Visual Basic®-Skript

vbe – BIOS-Video-Erweiterung

js, jse – JavaScript-Quelltext

htm – Hypertext-Dokument

htt – Hypertext-Dokumentvorlage für Microsoft Windows

hta – Hypertext-Programm für Microsoft Internet Explorer®;

asp – Active Server Pages-Skript;

chm – kompilierte HTML-Datei

pht – HTML-Datei mit eingebetteten PHP-Skripten

php – Skript, das in eine HTML-Datei eingebettet wird

wsh – Datei für Microsoft Windows Script Host

wsf – Skript von Microsoft Windows

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei im Format Win Help

msg – E-Mail-Nachricht für Microsoft Mail

plg – E-Mail-Nachricht

mbx – gespeicherte E-Mail-Nachricht für Microsoft Office Outlook

doc* – Dokumente für Microsoft Office Word, z.B.: doc – Dokumente für Microsoft Office Word, docx – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, docm – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung

dot* – Dokumentvorlagen in Microsoft Office Word, z.B. dot – Dokumentvorlage in Microsoft Office Word, dotx – Dokumentvorlage in Microsoft Office Word 2007, dotm – Dokumentvorlage in Microsoft Office Word 2007 mit Makrounterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro

rtf – Rich Text Format-Dokument

shs – Datenauszug für Windows Shell Scrap Object Handler

dwg – Datenbank für AutoCAD®-Skizzen

msi – Microsoft Windows Installer-Paket

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Dokument für Adobe Acrobat

swf – Objekt für Shockwave® Flash

jpg, jpeg – komprimierte Bilddatei

emf – Enhanced Metafile

ico – Symboldatei für ein Objekt

ov? – ausführbare Dateien für Microsoft Office Word

xl* – Dokumente und Dateien für Microsoft Office Excel, z.B.: xla – Erweiterung für Microsoft Office Excel, xlc – Diagramm, xlt – Dokumentvorlage, xlsx – Arbeitsblatt für Microsoft Office Excel 2007, xltm – Arbeitsblatt für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlsb – Arbeitsblatt für Microsoft Office Excel 2007 im Binärformat (nicht XML), xltx – Vorlage für Microsoft Office Excel 2007, xlsm – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, xlam – Konfigurationsdatei für Microsoft Office Excel 2007 mit Makro-Unterstützung.

pp* – Dokumente und Dateien für Microsoft Office PowerPoint®, z.B.: pps – Folie für Microsoft Office PowerPoint, ppt – Präsentation, pptx – Präsentation für Microsoft Office PowerPoint 2007, pptm – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, potx – Präsentationsvorlage für Microsoft Office PowerPoint 2007, potm – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppsx – Folienpräsentation für Microsoft Office PowerPoint 2007, ppsm – Folienpräsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, ppam – Konfigurationsdatei für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

md* – Dokumente und Dateien für Microsoft Office Access®, z.B.: mda – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank.

sldx – Folie in Microsoft Office PowerPoint 2007

sldm – Folie in Microsoft Office PowerPoint 2007 mit Makrounterstützung

thmx – Thema in Microsoft Office 2007

Anhang 5. Netzwerkeinstellungen für die Interaktion mit externen Diensten

Kaspersky Endpoint Security und Kaspersky Security Center verwenden einen verschlüsselten Kommunikationskanal mit TLS (Transport Layer Security), um mit externen Diensten von Kaspersky zusammenzuarbeiten.

Kaspersky Endpoint Security verwendet die folgenden Netzwerkeinstellungen für die Interaktion mit externen Diensten.

Netzwerkeinstellungen

Adresse	Beschreibung
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protokoll: `HTTPS` Port: `443`	Programm aktivieren.

Adresse	Beschreibung

`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`
`cm.k.kaspersky-labs.com`
Protokoll: `HTTPS`
Port: `443`
	Update der Datenbanken und Programm-Module.

`downloads.upd.kaspersky.com` Protokoll: `HTTPS` Port: `443`	• Update der Datenbanken und Programm-Module. • Überprüfung des Zugriffs auf Kaspersky-Server. Wenn die Server nicht über System-DNS erreichbar sind, verwendet das Programm öffentliches DNS. Dadurch wird sichergestellt, dass die Antiviren-Datenbanken aktualisiert werden und das Sicherheitsniveau des Computer aufrechterhalten bleibt. Kaspersky Endpoint Security verwendet die DNS-Server aus der unten angegeben Liste in der folgenden Reihenfolge: 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, die vom Programm gesendet werden, können Adressen von Domänen und die öffentliche IP-Adresse des Benutzers enthalten, da das Programm eine TCP/UDP-Verbindung mit dem DNS-Server herstellt. Diese Informationen sind beispielsweise erforderlich, um bei Verwendung von HTTPS das Zertifikat der Webressource zu validieren. Wenn Kaspersky Endpoint Security einen öffentlichen DNS-Server verwendet, richtet sich die Datenverarbeitung nach der Datenschutzrichtlinie des entsprechenden Dienstes. Wenn Sie verhindern möchten, dass Kaspersky Endpoint Security einen öffentlichen DNS-Server verwendet, fordern Sie beim Technischen Support einen privaten Patch an.

Adresse	Beschreibung
`touch.kaspersky.com` Protokoll: `HTTP`	• Abrufen der vertrauenswürdigen Zeit, um die Gültigkeitsdauer des Zertifikats zu überprüfen (TLS-Verbindung). • Ist der „Schutz vor Web-Bedrohungen" aktiviert, so erfolgt eine Warnung, wenn im Browser der Zugriff auf eine Webressource verweigert wurde.

`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`
`cm.k.kaspersky-labs.com`
Protokoll: `HTTP`
Port: `80`
	Update der Datenbanken und Programm-Module.

`ds.kaspersky.com`
`dc1.ksn.kaspersky-labs.com`
`dc1-file.ksn.kaspersky-labs.com`
`dc1-pp.ksn.kaspersky-labs.com`
`dc1-st.ksn.kaspersky-labs.com`
Protokoll: `HTTPS`
Port: `443`
	Verwendung von Kaspersky Security Network

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-info-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protokoll: `KSN`
Port: `443`, `1443`
	Verwendung von Kaspersky Security Network

`click.kaspersky.com`
 	
`redirect.kaspersky.com`
Protokoll: `HTTPS`
Port: `443`
	Folgen Sie den Links auf der Benutzeroberfläche.

Einstellungen, die für die Verschlüsselung verwendet werden

Adresse	Beschreibung

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protokoll: `HTTP`
Port: `80`
	Public Key Infrastructure (PKI).

Anhang 6. Programmereignisse

Im Kaspersky Security Center-Ereignisprotokoll und im Windows-Ereignisprotokoll werden protokolliert: Informationen über die Ausführung der einzelnen Komponenten von Kaspersky Endpoint Security, über Ereignisse bei der Datenverschlüsselung, über den Abschluss der einzelnen Aufgaben zur Virensuche, der Update-Aufgabe und der Aufgabe zur Integritätsprüfung, sowie über die allgemeine Programmausführung.

Kaspersky Endpoint Security generiert Ereignisse der folgenden Typen: allgemeine Ereignisse und spezifische Ereignisse. Spezifische Ereignisse werden nur von Kaspersky Endpoint Security für Windows erstellt. Spezifische Ereignisse haben eine einfache ID, z. B. `000000cb`. Spezifische Ereignisse enthalten die folgenden obligatorischen Parameter:

- `GNRL_EA_DESCRIPTION` ist der Inhalt des Ereignisses.
- `GNRL_EA_ID` ist die Dienst-ID des Ereignisses.
- `GNRL_EA_SEVERITY` ist der Status des Ereignisses. `1` – *Information* ⓘ, `2` – *Warnung* ⚠, `3` – *Funktionsfehler* ⓘ, `4` – *Kritisch* ⓘ.
- `EVENT_TYPE_DISPLAY_NAME` ist der Titel des Ereignisses.
- `TASK_DISPLAY_NAME` ist der Name der Programmkomponente, die das Ereignis initiiert hat.

Allgemeine Ereignisse können sowohl von Kaspersky Endpoint Security für Windows erstellt werden als auch von anderen Kaspersky-Programmen (z. B. Kaspersky Security für Windows Server). Allgemeine Ereignisse haben eine komplexere ID, z. B. `GNRL_EV_VIRUS_FOUND`. Allgemeine Ereignisse enthalten neben den obligatorischen Einstellungen auch erweiterte Einstellungen.

Speicherdauer von Ereignissen auf dem Server

Kritisch

Die Lizenz ist abgelaufen

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	`201`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_LICENSE_EXPIRATION`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Lizenz ist fast abgelaufen

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	203
Ereignis-ID in Kaspersky Security Center	000000cb
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Datenbanken fehlen oder sind beschädigt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	206
Ereignis-ID in Kaspersky Security Center	000000ce
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Datenbanken sind stark veraltet

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	207
Ereignis-ID in Kaspersky Security Center	000000cf
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Autostart des Programms wurde deaktiviert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	209
Ereignis-ID in Kaspersky Security Center	000000d1
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aktivierungsfehler

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	229
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine aktive Bedrohung wurde gefunden. Die aktive Desinfektion muss gestartet werden

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	231
Ereignis-ID in Kaspersky Security Center	000000e7
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

KSN-Server sind nicht verfügbar

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	2023
Ereignis-ID in Kaspersky Security Center	000007e7
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zu wenig Platz im Quarantäne-Speicher

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	343
Ereignis-ID in Kaspersky Security Center	00000157
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Objekt wurde nicht aus der Quarantäne wiederhergestellt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	346
Ereignis-ID in Kaspersky Security Center	0000015a
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Objekt wurde nicht aus der Quarantäne gelöscht

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	348
Ereignis-ID in Kaspersky Security Center	0000015c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Programm hat eine Verbindung zu einer Website mit einem nicht vertrauenswürdigen Zertifikat hergestellt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	57
Ereignis-ID in Kaspersky Security Center	00000039
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine verschlüsselte Verbindung konnte nicht überprüft werden. Die Domäne wurde zur Ausnahmeliste hinzugefügt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	60
Ereignis-ID in Kaspersky Security Center	0000003c
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein schädliches Objekt wurde gefunden (lokale Datenbanken)

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Programm-Überwachung Verhaltensanalyse Schutz vor Verschlüsselung Exploit-Prävention Schadsoftware-Untersuchung
Windows-Ereignis-ID	302
Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Hash des Objekts (SHA256). • GNRL_EA_PARAM_2 ist der Name des Objekts. Wenn die externe Verschlüsselung von gemeinsamen Ordnern erkannt wird, zeigt die Anwendung den Pfad der Zieldatei an. • GNRL_EA_PARAM_5 ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. EICAR-Test-File. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (Typ). • GNRL_EA_PARAM_9 sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (engine). Technologien zum Erkennen von Bedrohungen (method). Bedrohung wurde von Kaspersky Private Security Network erkannt (Blacklist): true oder false. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein schädliches Objekt wurde gefunden (KSN)

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Programm-Überwachung Verhaltensanalyse Schutz vor Verschlüsselung Exploit-Prävention Schadsoftware-Untersuchung
Windows-Ereignis-ID	`302`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_VIRUS_FOUND_BY_KSN`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_2` ist der Name des Objekts. • `GNRL_EA_PARAM_5` ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_8` ist der Typ der Bedrohung (`Typ`). • `GNRL_EA_PARAM_9` sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (`engine`). Technologien zum Erkennen von Bedrohungen (`method`). Bedrohung wurde von Kaspersky Private Security Network erkannt (`Blacklist`): `true` oder `false`. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Desinfektion nicht möglich

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen Programm-Überwachung Verhaltensanalyse Schutz vor Verschlüsselung Schadsoftware-Untersuchung
Windows-Ereignis-ID	`312`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_OBJECT_NOTCURED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_2` ist der Name des Objekts. • `GNRL_EA_PARAM_5` ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_8` ist der Typ der Bedrohung (`Typ`). • `GNRL_EA_PARAM_9` sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (`engine`). Technologien zum Erkennen von Bedrohungen (`method`). Bedrohung wurde von Kaspersky Private Security Network erkannt (`Blacklist`): `true` oder `false`. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Löschen nicht möglich

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Programm-Überwachung Verhaltensanalyse Schutz vor Verschlüsselung Schadsoftware-Untersuchung
Windows-Ereignis-ID	313
Ereignis-ID in Kaspersky Security Center	00000139
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Bearbeitungsfehler

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen Programm-Überwachung AMSI-Schutz Schadsoftware-Untersuchung
Windows-Ereignis-ID	317
Ereignis-ID in Kaspersky Security Center	0000013d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Prozess beendet

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Programm-Überwachung Verhaltensanalyse Schadsoftware-Untersuchung
Windows-Ereignis-ID	452
Ereignis-ID in Kaspersky Security Center	000001c4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Prozess kann nicht beendet werden

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Programm-Überwachung Verhaltensanalyse Schadsoftware-Untersuchung
Windows-Ereignis-ID	453
Ereignis-ID in Kaspersky Security Center	000001c5

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Ein gefährlicher Link wurde blockiert

Zustand	ⓘ
Komponente	Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	362
Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
Ereignisparameter	• GNRL_EA_PARAM_2 ist der Pfad des Objekts. • GNRL_EA_PARAM_5 ist der Name des Objekts gemäß der Kaspersky-Klassifizierung. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (Typ). • GNRL_EA_PARAM_9 sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (engine). Technologien zum Erkennen von Bedrohungen (method). Bedrohung wurde von Private KSN erkannt (Blacklist): true oder false.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein gefährlicher Link wurde geöffnet

Zustand	ⓘ
Komponente	Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	363
Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
Ereignisparameter	• GNRL_EA_PARAM_2 ist der Pfad des Objekts. • GNRL_EA_PARAM_5 ist der Name des Objekts gemäß der Kaspersky-Klassifizierung. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (Typ). • GNRL_EA_PARAM_9 sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (engine). Technologien zum Erkennen von Bedrohungen (method). Bedrohung wurde von Private KSN erkannt (Blacklist): true oder false.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zuvor geöffneten gefährlichen Link gefunden

Zustand	ⓘ
Komponente	Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	1201

Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
Ereignisparameter	• GNRL_EA_PARAM_2 ist der Pfad des Objekts. • GNRL_EA_PARAM_5 ist der Name des Objekts gemäß der Kaspersky-Klassifizierung. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (Typ). • GNRL_EA_PARAM_9 sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (engine). Technologien zum Erkennen von Bedrohungen (method). Bedrohung wurde von Private KSN erkannt (Blacklist): true oder false.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aktion eines Prozesses blockiert

Zustand	ⓘ
Komponente	Adaptive Kontrolle von Anomalien
Windows-Ereignis-ID	2200
Ereignis-ID in Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Name der Regel der „Adaptiven Kontrolle von Anomalien“. • GNRL_EA_PARAM_2 ist die ID der heuristischen Regel. • GNRL_EA_PARAM_3 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_4 ist der Quellprozess. • GNRL_EA_PARAM_5 ist das Quellobjekt. • GNRL_EA_PARAM_6 ist der Zielprozess. • GNRL_EA_PARAM_7 ist das Zielobjekt. • GNRL_EA_PARAM_8 sind zusätzliche Informationen über das erkannte Objekt: Prüfsummen des Quellprozesses/-objekts und des Zielprozesses/-objekts. Prozess wurde blockiert (verdict_type): true oder false. Benutzer-Sicherheits-ID (SID).
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Tastatur nicht autorisiert

Zustand	ⓘ
Komponente	Schutz vor modifizierten USB-Geräten
Windows-Ereignis-ID	2051
Ereignis-ID in Kaspersky Security Center	00000803
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

AMSI-Anfrage wurde blockiert

Zustand	ⓘ
Komponente	AMSI-Schutz
Windows-Ereignis-ID	2200
Ereignis-ID in Kaspersky Security Center	00000898
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkaktivität verboten

Zustand	⚠
Komponente	Firewall
Windows-Ereignis-ID	`602`
Ereignis-ID in Kaspersky Security Center	`00000329`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkangriff erkannt

Zustand	⚠
Komponente	Schutz vor Netzwerkbedrohungen
Windows-Ereignis-ID	`651`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_ATTACK_DETECTED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Name des Angriffs. • `GNRL_EA_PARAM_2` ist das Protokoll. • `GNRL_EA_PARAM_3` ist die IP-Adresse des Computers, der als Quelle des Netzwerkangriffs fungiert. Die IP-Adresse wird in der Byte-Reihenfolge des Hosts angegeben. Zum Beispiel `2886729929` für `172.16.0.201`. • `GNRL_EA_PARAM_4` ist die Portnummer. • `GNRL_EA_PARAM_5` ist eine IPv6-Adresse, z. B. `12B012B012B012B012B012B012B012B0`. • `GNRL_EA_PARAM_6` ist die IP-Adresse des Computers, der das Ziel des Netzwerkangriffs bildet. Die IP-Adresse wird in der Byte-Reihenfolge des Hosts angegeben. Zum Beispiel `2886729929` für `172.16.0.201`.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Programmstart verboten

Zustand	⚠
Komponente	Programmkontrolle
Windows-Ereignis-ID	`702`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_APPLICATION_LAUNCH_DENIED`
Ereignisparameter	• `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_3` ist die ID der manuell erstellten Kategorie. • `GNRL_EA_PARAM_4` ist die ID der Anwendungskategorie. • `GNRL_EA_PARAM_5` sind Informationen über die digitale Signatur der Anwendung. • `GNRL_EA_PARAM_6` ist der Name der ausführbaren Datei der Anwendung (z. B. chrome.exe). • `GNRL_EA_PARAM_7` ist der Pfad der ausführbaren Datei. • `GNRL_EA_PARAM_8` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_9` ist die Version der Anwendung, die der Benutzer auszuführen versucht.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Vor dem Start von Kaspersky Endpoint Security wurde ein verbotener Prozess gestartet

Zustand	ⓘ
Komponente	Programmkontrolle
Windows-Ereignis-ID	`710`
Ereignis-ID in Kaspersky Security Center	`000002c6`
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zugriff verweigert (lokale Datenbanken)

Zustand	ⓘ
Komponente	Web-Kontrolle
Windows-Ereignis-ID	`752`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_WEB_URL_BLOCKED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist die URL. • `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_3` ist der Name der Regel der „Web-Kontrolle“.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zugriff verweigert (KSN)

Zustand	ⓘ
Komponente	Web-Kontrolle
Windows-Ereignis-ID	`752`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_WEB_URL_BLOCKED_BY_KSN`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist die URL. • `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_3` ist der Name der Regel der „Web-Kontrolle“.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Vorgang mit dem Gerät verboten

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	`802`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUG_DENIED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist die Hardware-ID (HWID). • `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkverbindung blockiert

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	809
Ereignis-ID in Kaspersky Security Center	00000329
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Verwendung des Geräts ist untersagt, bis Kaspersky Endpoint Security gestartet wurde

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	816
Ereignis-ID in Kaspersky Security Center	00000330
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Verbindung des Geräts ist untersagt, bis Kaspersky Endpoint Security gestartet wurde

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	817
Ereignis-ID in Kaspersky Security Center	00000331
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Update einer Komponente

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1011
Ereignis-ID in Kaspersky Security Center	000003f3
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Verteilung von Komponenten-Updates

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1012
Ereignis-ID in Kaspersky Security Center	000003f4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Lokaler Update-Fehler

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1014
Ereignis-ID in Kaspersky Security Center	000003f6
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Netzwerkfehler beim Update

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1015
Ereignis-ID in Kaspersky Security Center	000003f7
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Zwei Aufgaben können nicht gleichzeitig gestartet werden

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1017
Ereignis-ID in Kaspersky Security Center	000003f9
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei Überprüfung der Datenbanken und Programm-Module

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1018
Ereignis-ID in Kaspersky Security Center	000003fa
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei Interaktion mit Kaspersky Security Center

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1019
Ereignis-ID in Kaspersky Security Center	000003fb
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Nicht alle Komponenten wurden aktualisiert

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1021
Ereignis-ID in Kaspersky Security Center	000003fd
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Update wurde erfolgreich abgeschlossen, aber die Update-Verteilung ist fehlgeschlagen

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1023
Ereignis-ID in Kaspersky Security Center	000003ff
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Interner Aufgabenfehler

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	101
Ereignis-ID in Kaspersky Security Center	00000065
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Fehler bei der Patch-Installation

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	2153
Ereignis-ID in Kaspersky Security Center	00000869
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Patch-Rollback

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	2156
Ereignis-ID in Kaspersky Security Center	0000086c
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Anwenden von Verschlüsselungs-/Entschlüsselungsregeln für Dateien

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	`904`
Ereignis-ID in Kaspersky Security Center	`00000388`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Verschlüsselung/Entschlüsselung von Dateien

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	`912`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_ENCRYPTION_ERROR`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Pfad der Datei. • `GNRL_EA_PARAM_2` ist die Ursache des Fehlers. • `GNRL_EA_PARAM_3` ist der Typ des Gerätes.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zugriff auf Datei gesperrt

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	`940`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist das Zielobjekt. • `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_3` ist der Name der ausführbaren Datei des Programms (z. B. chrome.exe), die versucht, Zugriff auf die Datei zu erhalten.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Fehler beim Aktivieren des portablen Modus

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	`951`
Ereignis-ID in Kaspersky Security Center	`000003b7`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Deaktivieren des portablen Modus

Zustand	⚠
Komponente	Datenverschlüsselung

Windows-Ereignis-ID	953
Ereignis-ID in Kaspersky Security Center	000003b9
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Erstellen eines verschlüsselten Archivs

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	931
Ereignis-ID in Kaspersky Security Center	000003a3
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Verschlüsselung/Entschlüsselung eines Gerätes

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1305
Ereignis-ID in Kaspersky Security Center	00000519
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Verschlüsselungsmodul konnte nicht geladen werden

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1311
Ereignis-ID in Kaspersky Security Center	0000051f
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Aufgabe zur Verwaltung von Authentifizierungsagenten-Konten ist fehlgeschlagen

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1340
Ereignis-ID in Kaspersky Security Center	0000053c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Richtlinie kann nicht übernommen werden

Zustand	ⓘ
Komponente	Systemaudit

Windows-Ereignis-ID	1312
Ereignis-ID in Kaspersky Security Center	00000520
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das FDE-Upgrade ist fehlgeschlagen

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1342
Ereignis-ID in Kaspersky Security Center	0000053e
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

FDE-Upgrade konnte nicht zurückgesetzt werden (weitere Informationen finden Sie in der Online-Hilfe zu Kaspersky Endpoint Security für Windows)

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1344
Ereignis-ID in Kaspersky Security Center	00000540
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Server für Kaspersky Anti Targeted Attack Platform nicht verfügbar

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2100
Ereignis-ID in Kaspersky Security Center	00000834
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Löschen des Objekts

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2252
Ereignis-ID in Kaspersky Security Center	000008cc
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde nicht in die Quarantäne verschoben (Sandbox)

Zustand	⚠
Komponente	Sandbox

Windows-Ereignis-ID	2603
Ereignis-ID in Kaspersky Security Center	00000a2b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein interner Fehler ist aufgetreten

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2607
Ereignis-ID in Kaspersky Security Center	00000a2f
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Sandbox-Servers

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2613
Ereignis-ID in Kaspersky Security Center	00000a35
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Sandbox-Knoten ist nicht verfügbar

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2614
Ereignis-ID in Kaspersky Security Center	00000a36
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt konnte nicht in Sandbox verarbeitet werden

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2617
Ereignis-ID in Kaspersky Security Center	00000a39
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Maximale Auslastung von Sandbox wurde überschritten

Zustand	⚠
Komponente	Sandbox

Windows-Ereignis-ID	2618
Ereignis-ID in Kaspersky Security Center	00000a3a
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

IOC gefunden

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2651
Ereignis-ID in Kaspersky Security Center	00000a5b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Überprüfung der "Sandbox"-Lizenz fehlgeschlagen

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2620
Ereignis-ID in Kaspersky Security Center	00000a3c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Untersuchungsaufgabe konnte vom Benutzer nicht an Sandbox übermittelt werden

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2623
Ereignis-ID in Kaspersky Security Center	00000a3e
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Erstellen der Sandbox-Aufgabe

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2621
Ereignis-ID in Kaspersky Security Center	00000a3d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objektstart blockiert

Zustand	⚠
Komponente	Endpoint Detection and Response

Windows-Ereignis-ID	2553
Ereignis-ID in Kaspersky Security Center	000009f9
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Prozess-Start blockiert

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2551
Ereignis-ID in Kaspersky Security Center	000009f7
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Skriptausführung blockiert

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2559
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde nicht in die Quarantäne verschoben (Endpoint Detection and Response)

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2556
Ereignis-ID in Kaspersky Security Center	000009fc
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Prozess-Start wurde nicht blockiert

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2561
Ereignis-ID in Kaspersky Security Center	00000a01
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde nicht blockiert

Zustand	⚠
Komponente	Endpoint Detection and Response

Windows-Ereignis-ID	2562
Ereignis-ID in Kaspersky Security Center	00000a02
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Skriptausführung wurde nicht blockiert

Zustand	ⓘ
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2563
Ereignis-ID in Kaspersky Security Center	00000a03
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Ändern der Auswahl der Programmkomponenten

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	1401
Ereignis-ID in Kaspersky Security Center	00000579
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Anzeichen eines Brute-Force-Angriffs wurden im System gefunden

Zustand	ⓘ
Komponente	Protokollanalyse
Windows-Ereignis-ID	2800
Ereignis-ID in Kaspersky Security Center	00000af0
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Anzeichen für eine Gefährdung der Windows-Ereignisprotokolle wurden gefunden

Zustand	ⓘ
Komponente	Protokollanalyse
Windows-Ereignis-ID	2801
Ereignis-ID in Kaspersky Security Center	00000af1
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungewöhnliche Aktionen im Auftrag eines neu installierten Dienstes wurden erkannt

Zustand	ⓘ
Komponente	Protokollanalyse

Windows-Ereignis-ID	2802
Ereignis-ID in Kaspersky Security Center	00000af2
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine ungewöhnliche Anmeldung mit expliziten Anmeldedaten wurde erkannt

Zustand	⚠
Komponente	Protokollanalyse
Windows-Ereignis-ID	2803
Ereignis-ID in Kaspersky Security Center	00000af3
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Anzeichen eines Angriffs mit gefälschtem Kerberos-PAC (MS14-068) wurden im System gefunden

Zustand	⚠
Komponente	Protokollanalyse
Windows-Ereignis-ID	2804
Ereignis-ID in Kaspersky Security Center	00000af4
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Verdächtige Änderungen in der privilegierten integrierten Administratorgruppe wurden erkannt

Zustand	⚠
Komponente	Protokollanalyse
Windows-Ereignis-ID	2805
Ereignis-ID in Kaspersky Security Center	00000af5
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Es wurde eine ungewöhnliche Aktivität während einer Netzwerkanmeldesitzung erkannt

Zustand	⚠
Komponente	Protokollanalyse
Windows-Ereignis-ID	2806
Ereignis-ID in Kaspersky Security Center	00000af6
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine Protokollanalyse-Regel wurde ausgelöst

Zustand	⚠
Komponente	Protokollanalyse

Windows-Ereignis-ID	2807
Ereignis-ID in Kaspersky Security Center	00000af7
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungewöhnliches Ereignis tritt zu oft auf. Ereignisaggregation gestartet

Zustand	ⓘ
Komponente	Protokollanalyse
Windows-Ereignis-ID	2808
Ereignis-ID in Kaspersky Security Center	00000af8
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Bericht über ein ungewöhnliches Ereignis für den Aggregationszeitraum

Zustand	ⓘ
Komponente	Protokollanalyse
Windows-Ereignis-ID	2809
Ereignis-ID in Kaspersky Security Center	00000af9
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Verbindung mit dem EDR Expert-Server

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises)
Windows-Ereignis-ID	2850
Ereignis-ID in Kaspersky Security Center	00000b22
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des EDR Expert-Servers

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises)
Windows-Ereignis-ID	2851
Ereignis-ID in Kaspersky Security Center	00000b23
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Agenten auf dem EDR Expert-Server

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises)

Windows-Ereignis-ID	2852
Ereignis-ID in Kaspersky Security Center	00000b24
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Verbindung mit dem Reaktionsserver von EDR Expert

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2858
Ereignis-ID in Kaspersky Security Center	00000b22
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Reaktionsservers von EDR Expert

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2859
Ereignis-ID in Kaspersky Security Center	00000b23
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Agenten auf dem Reaktionsserver von EDR Expert

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2860
Ereignis-ID in Kaspersky Security Center	00000b24
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Verbindung zum Telemetrie-Erfassungsserver von EDR Expert

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2854
Ereignis-ID in Kaspersky Security Center	00000b22
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des EDR Expert-Telemetrie-Erfassungsservers

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2855
Ereignis-ID in Kaspersky Security Center	00000b23
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Agenten auf dem EDR Expert-Telemetrie-Erfassungsserver

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2856
Ereignis-ID in Kaspersky Security Center	00000b24
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Verbinden mit dem NDR-Server

Zustand	ⓘ
Komponente	Network Detection and Response (KATA)
Windows-Ereignis-ID	3080
Ereignis-ID in Kaspersky Security Center	00000c08
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des NDR-Servers

Zustand	ⓘ
Komponente	Network Detection and Response (KATA)
Windows-Ereignis-ID	3081
Ereignis-ID in Kaspersky Security Center	00000c09
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Agenten auf dem NDR-Server

Zustand	ⓘ
Komponente	Network Detection and Response (KATA)
Windows-Ereignis-ID	3082
Ereignis-ID in Kaspersky Security Center	00000c0a
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ihr Gerät ist mit einem nicht vertrauenswürdigen Administrationsserver verbunden. Wenden Sie sich an Ihren Administrator

Zustand	⊗
Komponente	Schutz der Verbindung zum Administrationsserver
Windows-Ereignis-ID	3301
Ereignis-ID in Kaspersky Security Center	00000ce5
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Änderung einer Datei oder eines Ordners wurde erkannt

Zustand	ⓘ / ⚠ / ⊗
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2950
Ereignis-ID in Kaspersky Security Center	00000b86
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Das Objekt ändert sich zu oft. Die Ereignisaggregation wurde gestartet

Zustand	ⓘ / ⚠ / ⊗
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2955
Ereignis-ID in Kaspersky Security Center	00000b8b
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Bericht über eine Objektänderung für den Aggregationszeitraum

Zustand	⊗
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2953
Ereignis-ID in Kaspersky Security Center	00000b89
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zustand	ⓘ / ⚠ / ⊗
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2956
Ereignis-ID in Kaspersky Security Center	00000b8c

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Änderung der Registrierung wurde erkannt

Zustand	ⓘ / ⚠ / !
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2951
Ereignis-ID in Kaspersky Security Center	00000b87
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Verbindung bzw. Trennung der Verbindung zu einem Gerät wurde erkannt

Zustand	ⓘ / ⚠ / !
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2952
Ereignis-ID in Kaspersky Security Center	00000b88
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Der Überwachungsbereich enthält ungültige Objekte

Zustand	ⓘ / ⚠ / !
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2903
Ereignis-ID in Kaspersky Security Center	00000b89
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Zu viele Versuche, beschränkte Vorgänge mit dem Objekt auszuführen. Ereignisaggregation gestartet

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2963
Ereignis-ID in Kaspersky Security Center	00000b93
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein Vorgang mit den Dateien des Überwachungsbereichs wurde gesperrt

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2959
Ereignis-ID in Kaspersky Security Center	00000b8f
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Änderung der Registrierung blockiert

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2960
Ereignis-ID in Kaspersky Security Center	00000b90
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Bearbeitungsfehler

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2954
Ereignis-ID in Kaspersky Security Center	00000b8a
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Überwachung der Systemintegrität: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2964
Ereignis-ID in Kaspersky Security Center	00000b94
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Programmkontrolle: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)

Zustand	ⓘ
Komponente	Programmkontrolle
Windows-Ereignis-ID	711
Ereignis-ID in Kaspersky Security Center	000002c7
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Gerätekontrolle: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	810
Ereignis-ID in Kaspersky Security Center	0000032a
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Web-Kontrolle: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)

Zustand	ⓘ
Komponente	Web-Kontrolle
Windows-Ereignis-ID	757
Ereignis-ID in Kaspersky Security Center	000002f5
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Adaptive Kontrolle von Anomalien: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)

Zustand	ⓘ
Komponente	Adaptive Kontrolle von Anomalien
Windows-Ereignis-ID	504
Ereignis-ID in Kaspersky Security Center	000001f8
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Protokollanalyse: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)

Zustand	ⓘ
Komponente	Protokollanalyse
Windows-Ereignis-ID	2810
Ereignis-ID in Kaspersky Security Center	00000afa
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

SVM ist nicht verfügbar

Zustand	ⓘ
Komponente	Light Agent
Windows-Ereignis-ID	3151
Ereignis-ID in Kaspersky Security Center	00000c4f
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Schädliches Objekt gefunden. Die aktive Desinfektion muss auf einer Vorlage für virtuelle Maschinen gestartet werden

Zustand	ⓘ
Komponente	Light Agent
Windows-Ereignis-ID	3182
Ereignis-ID in Kaspersky Security Center	00000c6e
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Netzwerkverbindung wurde über ein veraltetes Protokoll hergestellt und deshalb blockiert

Zustand	ⓘ
Komponente	Schutz
Windows-Ereignis-ID	75
Ereignis-ID in Kaspersky Security Center	0000004b
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei Verbindung zum KUMA-Server

Zustand	ⓘ
Komponente	KUMA-Integration
Windows-Ereignis-ID	2854
Ereignis-ID in Kaspersky Security Center	00000b26
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des KUMA-Servers

Zustand	⚠
Komponente	KUMA-Integration
Windows-Ereignis-ID	2855
Ereignis-ID in Kaspersky Security Center	00000b27
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Agenten auf dem KUMA-Server

Zustand	⚠
Komponente	KUMA-Integration
Windows-Ereignis-ID	2856
Ereignis-ID in Kaspersky Security Center	00000b28
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei Verbindung zum SIEM-Server

Zustand	⚠
Komponente	KUMA-Integration
Windows-Ereignis-ID	3250
Ereignis-ID in Kaspersky Security Center	00000cb2
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des SIEM-Servers

Zustand	⚠
Komponente	KUMA-Integration
Windows-Ereignis-ID	3251
Ereignis-ID in Kaspersky Security Center	00000cb3
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiges Zertifikat des Agenten auf dem SIEM-Server

Zustand	⚠
Komponente	KUMA-Integration
Windows-Ereignis-ID	3252
Ereignis-ID in Kaspersky Security Center	00000cb4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Funktionsstörung

Aufgabe kann nicht ausgeführt werden

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	212
Ereignis-ID in Kaspersky Security Center	000000d4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültige Aufgabeneinstellungen. Einstellungen nicht übernommen

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	707
Ereignis-ID in Kaspersky Security Center	000002c3
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Warnung

Die vorherige Programmsitzung wurde nicht ordnungsgemäß beendet

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	237
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Lizenz läuft bald ab

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	204
Ereignis-ID in Kaspersky Security Center	000000cc
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Datenbanken sind veraltet

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	208
Ereignis-ID in Kaspersky Security Center	000000d0
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das automatische Update wurde deaktiviert

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	210
Ereignis-ID in Kaspersky Security Center	000000d2
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Selbstschutz ist deaktiviert

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	211
Ereignis-ID in Kaspersky Security Center	000000d3
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Schutzkomponenten wurden deaktiviert

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	214
Ereignis-ID in Kaspersky Security Center	000000d6
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Computer läuft im abgesicherten Modus

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	215
Ereignis-ID in Kaspersky Security Center	000000d7
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Es gibt unverarbeitete Dateien

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	216
Ereignis-ID in Kaspersky Security Center	000000d8
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Gruppenrichtlinie wurde übernommen

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	219
Ereignis-ID in Kaspersky Security Center	000000db
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aufgabe abgebrochen

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	222
Ereignis-ID in Kaspersky Security Center	000000de
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Programm muss neu gestartet werden, um das Update abzuschließen

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	224
Ereignis-ID in Kaspersky Security Center	0000057b
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Neustart des Computers ist erforderlich

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	225
Ereignis-ID in Kaspersky Security Center	000000e1
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Lizenz erlaubt die Nutzung weiterer Programmkomponenten, die nicht installiert sind

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	226
Ereignis-ID in Kaspersky Security Center	000000e2
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aktive Desinfektion" wurde gestartet

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	232
Ereignis-ID in Kaspersky Security Center	000000e8
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aktive Desinfektion" wurde abgeschlossen

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	233
Ereignis-ID in Kaspersky Security Center	000000e9
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ungültiger Reserveschlüssel

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	230
Ereignis-ID in Kaspersky Security Center	000000e6
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Abonnement läuft bald ab

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	240
Ereignis-ID in Kaspersky Security Center	000000f0
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Gesperrt

Zustand	⚠
Komponente	Verhaltensanalyse Schutz vor Verschlüsselung Exploit-Prävention Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	`331`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_2` ist der Name des Objekts. Wenn die externe Verschlüsselung von gemeinsamen Ordnern erkannt wird, zeigt die Anwendung den Pfad der Zieldatei an. • `GNRL_EA_PARAM_5` ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_8` ist der Typ der Bedrohung (`type`). • `GNRL_EA_PARAM_9` sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (`engine`). Technologien zum Erkennen von Bedrohungen (`method`). Bedrohung wurde erkannt von Kaspersky Private Security Network (`blacklist`): `true` oder `false`. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Betriebssystemeinstellungen erlauben es nicht, den Zugriff auf WLAN-Netzwerke zu kontrollieren

Zustand	⚠
Komponente	Gerätekontrolle
Windows-Ereignis-ID	`249`
Ereignis-ID in Kaspersky Security Center	`000000f9`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Objekt wurde nicht aus dem Backup wiederhergestellt

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	`336`
Ereignis-ID in Kaspersky Security Center	`00000150`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Eine verdächtige Netzwerkaktivität wurde erkannt

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	2001
Ereignis-ID in Kaspersky Security Center	000007d1
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine verschlüsselte Verbindung wurde getrennt

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	250
Ereignis-ID in Kaspersky Security Center	000007d3
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Teilnahme an KSN ist deaktiviert

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	2021
Ereignis-ID in Kaspersky Security Center	000007e5
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Verarbeitung einiger BS-Funktionen deaktiviert

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	245
Ereignis-ID in Kaspersky Security Center	000000f5
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Quarantäne-Speicher ist fast voll

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	344
Ereignis-ID in Kaspersky Security Center	00000158
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkverbindung blockiert

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	809
Ereignis-ID in Kaspersky Security Center	00000abe
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Backup-Kopie kann nicht angelegt werden

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Verhaltensanalyse Schutz vor Verschlüsselung Programm-Überwachung Schadsoftware-Untersuchung
Windows-Ereignis-ID	310
Ereignis-ID in Kaspersky Security Center	00000136
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt nicht verarbeitet

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen Programm-Überwachung AMSI-Schutz Schadsoftware-Untersuchung
Windows-Ereignis-ID	314
Ereignis-ID in Kaspersky Security Center	0000013a
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt verschlüsselt

Zustand	⚠
Komponente	Programm-Überwachung
Windows-Ereignis-ID	320
Ereignis-ID in Kaspersky Security Center	00000140
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Objekt ist beschädigt

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Programm-Überwachung Schadsoftware-Untersuchung

Windows-Ereignis-ID	321
Ereignis-ID in Kaspersky Security Center	00000141
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Es wurde legitime Software gefunden, mit der Angreifer Ihren Computer oder persönliche Daten beschädigen können. (lokale Datenbanken)

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen Programm-Überwachung AMSI-Schutz Verhaltensanalyse Schutz vor Verschlüsselung Schutz vor Verschlüsselung Schadsoftware-Untersuchung
Windows-Ereignis-ID	303
Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Hash des Objekts (SHA256). • GNRL_EA_PARAM_2 ist der Name des Objekts. • GNRL_EA_PARAM_5 ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. EICAR-Test-File. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (type).
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Es wurde legitime Software gefunden, mit der Angreifer Ihren Computer oder persönliche Daten beschädigen können (KSN)

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen Programm-Überwachung AMSI-Schutz Verhaltensanalyse Schutz vor Verschlüsselung Schutz vor Verschlüsselung Schadsoftware-Untersuchung
Windows-Ereignis-ID	303
Ereignis-ID in Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Hash des Objekts (SHA256). • GNRL_EA_PARAM_2 ist der Name des Objekts. • GNRL_EA_PARAM_5 ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. EICAR-Test-File. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (type).
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt gelöscht

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen Programm-Überwachung Exploit-Prävention Verhaltensanalyse Schutz vor Verschlüsselung Schadsoftware-Untersuchung
Windows-Ereignis-ID	`307`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_OBJECT_DELETED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_2` ist der Name des Objekts. • `GNRL_EA_PARAM_5` ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_8` ist der Typ der Bedrohung (`type`). • `GNRL_EA_PARAM_9` sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (`engine`). Technologien zum Erkennen von Bedrohungen (`method`). Bedrohung wurde erkannt von Kaspersky Private Security Network (`blacklist`): `true` oder `false`. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt desinfiziert

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen Programm-Überwachung Schadsoftware-Untersuchung
Windows-Ereignis-ID	`306`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_OBJECT_CURED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_2` ist der Name des Objekts. • `GNRL_EA_PARAM_5` ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_8` ist der Typ der Bedrohung (`type`). • `GNRL_EA_PARAM_9` sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (`engine`). Technologien zum Erkennen von Bedrohungen (`method`). Bedrohung wurde erkannt von Kaspersky Private Security Network (`blacklist`): `true` oder `false`. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wird beim Neustart desinfiziert

Zustand	⚠
Komponente	Programm-Überwachung Schutz vor bedrohlichen Dateien Schadsoftware-Untersuchung
Windows-Ereignis-ID	324
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Objekt wird beim Neustart gelöscht

Zustand	⚠
Komponente	Verhaltensanalyse Schutz vor Verschlüsselung Exploit-Prävention Programm-Überwachung Schutz vor bedrohlichen Dateien Schadsoftware-Untersuchung
Windows-Ereignis-ID	323
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Objekt wurde gemäß den Einstellungen gelöscht

Zustand	⚠
Komponente	Schutz vor E-Mail-Bedrohungen
Windows-Ereignis-ID	342
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Rollback ausgeführt

Zustand	⚠
Komponente	Schutz vor bedrohlichen Dateien Verhaltensanalyse Schutz vor Verschlüsselung Exploit-Prävention Schadsoftware-Untersuchung
Windows-Ereignis-ID	455
Ereignis-ID in Kaspersky Security Center	000001c7
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler beim Entfernen der vorhergehenden Programmversion

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	`246`
Ereignis-ID in Kaspersky Security Center	`000000f6`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Download des Objekts wurde verboten

Zustand	⚠
Komponente	Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	`341`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_OBJECT_BLOCKED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist der Hash des Objekts (SHA256). • `GNRL_EA_PARAM_2` ist der Name des Objekts. • `GNRL_EA_PARAM_5` ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. `EICAR-Test-File`. • `GNRL_EA_PARAM_7` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_8` ist der Typ der Bedrohung (`type`). • `GNRL_EA_PARAM_9` sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (`engine`). Technologien zum Erkennen von Bedrohungen (`method`). Bedrohung wurde erkannt von Kaspersky Private Security Network (`blacklist`): `true` oder `false`. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Fehler bei der Autorisierung der Tastatur

Zustand	⚠
Komponente	Schutz vor BadUSB-Angriffen
Windows-Ereignis-ID	`2052`
Ereignis-ID in Kaspersky Security Center	`00000804`
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Ergebnis der Objektuntersuchung wurde an eine Drittanbieter-Anwendung übermittelt

Zustand	⚠
Komponente	AMSI-Schutz
Windows-Ereignis-ID	`1512`

Ereignis-ID in Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Hash des Objekts (SHA256). • GNRL_EA_PARAM_2 ist der Name des Objekts. • GNRL_EA_PARAM_5 ist der Name der Bedrohung gemäß der Kaspersky-Klassifizierung, z. B. EICAR-Test-File. • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_8 ist der Typ der Bedrohung (type). • GNRL_EA_PARAM_9 sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (engine). Technologien zum Erkennen von Bedrohungen (method). Bedrohung wurde erkannt von Kaspersky Private Security Network (blacklist): true oder false. EDR-Version. Bedrohungs-ID in EDR. MD5-Hash des Objekts.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aufgabeneinstellungen erfolgreich übernommen

Zustand	⚠
Komponente	Programmkontrolle
Windows-Ereignis-ID	708
Ereignis-ID in Kaspersky Security Center	000002c4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Warnung über unerwünschten Inhalt (lokale Datenbanken)

Zustand	⚠
Komponente	Web-Kontrolle
Windows-Ereignis-ID	708
Ereignis-ID in Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Ereignisparameter	• GNRL_EA_PARAM_1 ist die URL. • GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_3 ist der Name der Regel der „Web-Kontrolle".
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Warnung über unerwünschten Inhalt (KSN)

Zustand	⚠
Komponente	Web-Kontrolle
Windows-Ereignis-ID	708
Ereignis-ID in Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
Ereignisparameter	• GNRL_EA_PARAM_1 ist die URL. • GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_3 ist der Name der Regel der „Web-Kontrolle".
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Es wurde trotz Warnung auf unerwünschte Inhalte zugegriffen

Zustand	⚠
Komponente	Web-Kontrolle
Windows-Ereignis-ID	754
Ereignis-ID in Kaspersky Security Center	000002f2
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Temporärer Zugriff auf das Gerät aktiviert

Zustand	⚠
Komponente	Gerätekontrolle
Windows-Ereignis-ID	803
Ereignis-ID in Kaspersky Security Center	000002f2
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Vorgang vom Benutzer abgebrochen

Zustand	⚠
Komponente	Update
Windows-Ereignis-ID	1016
Ereignis-ID in Kaspersky Security Center	000003f8
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1306
Ereignis-ID in Kaspersky Security Center	0000051a
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Anwenden von Verschlüsselungs-/Entschlüsselungsregeln für Dateien wurde abgebrochen

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	903
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung von Dateien wurde abgebrochen

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	914
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung des Gerätes wurde abgebrochen

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1303
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Installation oder das Upgrade der Treiber für die Kaspersky-Festplattenverschlüsselung im WinRE-Image ist fehlgeschlagen

Zustand	⚠
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1345
Ereignis-ID in Kaspersky Security Center	00000541
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Überprüfung der Modul-Signatur fehlgeschlagen

Zustand	⚠
Komponente	Prüfung der Systemintegrität
Windows-Ereignis-ID	2002
Ereignis-ID in Kaspersky Security Center	000007d2
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Programmstart wurde blockiert

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2105
Ereignis-ID in Kaspersky Security Center	00000839
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Öffnen eines Dokuments wurde blockiert

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2106
Ereignis-ID in Kaspersky Security Center	0000083a
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Prozess wurde vom Administrator des Servers für Kaspersky Anti Targeted Attack Platform beendet

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2112
Ereignis-ID in Kaspersky Security Center	00000840
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Programm wurde vom Administrator des Servers für Kaspersky Anti Targeted Attack Platform beendet

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2113
Ereignis-ID in Kaspersky Security Center	00000841
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Datei oder Stream wurde vom Administrator des Kaspersky Anti Targeted Attack Platform-Servers gelöscht

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2111
Ereignis-ID in Kaspersky Security Center	0000083f
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Datei wurde vom Administrator aus der Quarantäne des Kaspersky Anti Targeted Attack Platform-Servers wiederhergestellt

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2110
Ereignis-ID in Kaspersky Security Center	0000083e
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Datei wurde vom Administrator in die Quarantäne des Kaspersky Anti Targeted Attack Platform-Servers verschoben

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2109
Ereignis-ID in Kaspersky Security Center	0000083d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkaktivität aller Dritthersteller-Programme wurde blockiert

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2107
Ereignis-ID in Kaspersky Security Center	0000083b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Netzwerkaktivität aller Dritthersteller-Programme wurde freigegeben

Zustand	⚠
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2108
Ereignis-ID in Kaspersky Security Center	0000083c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wird nach dem Neustart gelöscht (Sandbox)

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2605
Ereignis-ID in Kaspersky Security Center	00000a2d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die zulässige Gesamtgröße der Untersuchungsaufgaben wurde überschritten

Zustand	⚠
Komponente	Sandbox
Windows-Ereignis-ID	2612
Ereignis-ID in Kaspersky Security Center	00000a34
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objektstart erlaubt, Ereignis protokolliert

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2553
Ereignis-ID in Kaspersky Security Center	000009fa
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Prozess-Start erlaubt, Ereignis protokolliert

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2554
Ereignis-ID in Kaspersky Security Center	000009f8
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wird nach dem Neustart gelöscht (Endpoint Detection and Response)

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2558
Ereignis-ID in Kaspersky Security Center	000009fe
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkisolation

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2700
Ereignis-ID in Kaspersky Security Center	00000a8c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ende der Netzwerkisolation

Zustand	⚠
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2701
Ereignis-ID in Kaspersky Security Center	00000a8d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zum Fertigstellen der Aufgabe ist ein Neustart erforderlich

Zustand	⚠
Komponente	Systemaudit
Windows-Ereignis-ID	225
Ereignis-ID in Kaspersky Security Center	0000057b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aufgrund einer Benutzerentscheidung wurde eine Verbindung zu einer Website mit einem nicht vertrauenswürdigen Zertifikat hergestellt

Zustand	⚠
Komponente	Network Detection and Response (KATA)
Windows-Ereignis-ID	70
Ereignis-ID in Kaspersky Security Center	00000046
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Nachricht an den Administrator über Verbot des Programmstarts

Zustand	⚠
Komponente	Programmkontrolle
Windows-Ereignis-ID	503
Ereignis-ID in Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
Ereignisparameter	• GNRL_EA_DESCRIPTION ist die Nachricht an den Benutzer. • GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_6 ist der Name der ausführbaren Datei der Anwendung (z. B. chrome.exe). • GNRL_EA_PARAM_7 ist der Pfad der ausführbaren Datei. • GNRL_EA_PARAM_8 ist der Hash des Objekts (SHA256). • GNRL_EA_PARAM_9 ist die Version der Anwendung, die der Benutzer auszuführen versucht.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Nachricht an den Administrator über Zugriffsverbot auf Gerät

Zustand	⚠
Komponente	Gerätekontrolle
Windows-Ereignis-ID	804
Ereignis-ID in Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
Ereignisparameter	• c_er_descr ist die Nachricht an den Benutzer. • GNRL_EA_PARAM_1 ist die Hardware-ID (HWID). • GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Nachricht an den Administrator über Zugriffsverbot auf Webseite

Zustand	⚠
Komponente	Web-Kontrolle
Windows-Ereignis-ID	`755`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_WC_USER_REQUEST`
Ereignisparameter	• `GNRL_EA_DESCRIPTION` ist die Nachricht an den Benutzer. • `GNRL_EA_PARAM_1` ist die URL. • `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Verbindung mit dem Gerät wurde blockiert

Zustand	⚠
Komponente	Gerätekontrolle
Windows-Ereignis-ID	`807`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_DEVCTRL_DEV_PLUG_DENIED`
Ereignisparameter	• `GNRL_EA_PARAM_1` ist die Hardware-ID (HWID). • `GNRL_EA_PARAM_2` ist der Name des Sitzungsbenutzers.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Nachricht an den Administrator über das Verbot einer Programmaktion

Zustand	⚠
Komponente	Adaptive Kontrolle von Anomalien
Windows-Ereignis-ID	`503`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_ADSEC_USER_REQUEST`
Ereignisparameter	• `GNRL_EA_DESCRIPTION` ist die Nachricht an den Benutzer. • `GNRL_EA_PARAM_1` ist der Name der Regel der „Adaptiven Kontrolle von Anomalien". • `GNRL_EA_PARAM_2` ist die ID der heuristischen Regel. • `GNRL_EA_PARAM_3` ist der Name des Sitzungsbenutzers. • `GNRL_EA_PARAM_4` ist der Quellprozess. • `GNRL_EA_PARAM_5` ist das Quellobjekt. • `GNRL_EA_PARAM_6` ist der Zielprozess. • `GNRL_EA_PARAM_7` ist das Zielobjekt. • `GNRL_EA_PARAM_8` sind zusätzliche Informationen über das erkannte Objekt: Hashs des Quellprozesses bzw. -objekts und des Zielprozesses bzw. -objekts. Prozess wurde blockiert (`verdict_type`): `true` oder `false`. Benutzer-Sicherheits-ID (SID).
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Start der Client-App des Cloud-Dienstes wurde blockiert

Zustand	⚠
Komponente	Cloud Discovery
Windows-Ereignis-ID	`2212`

Ereignis-ID in Kaspersky Security Center	000008a4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Zugriff auf den Cloud-Dienst wurde verboten

Zustand	⚠
Komponente	Cloud Discovery
Windows-Ereignis-ID	2213
Ereignis-ID in Kaspersky Security Center	000008a5
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Änderung einer Datei oder eines Ordners wurde erkannt

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2950
Ereignis-ID in Kaspersky Security Center	00000b86
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Das Objekt ändert sich zu oft. Die Ereignisaggregation wurde gestartet

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2955
Ereignis-ID in Kaspersky Security Center	00000b8b
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Bericht über eine Objektänderung für den Aggregationszeitraum

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2956
Ereignis-ID in Kaspersky Security Center	00000b8c
Windows-Ereignisprotokoll (Standard)	–

Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Änderung der Registrierung wurde erkannt

Zustand	ⓘ / ⚠ / ⓔ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2951
Ereignis-ID in Kaspersky Security Center	00000b87
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Verbindung bzw. Trennung der Verbindung zu einem Gerät wurde erkannt

Zustand	ⓘ / ⚠ / ⓔ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2952
Ereignis-ID in Kaspersky Security Center	00000b88
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Der Überwachungsbereich enthält ungültige Objekte

Zustand	ⓘ / ⚠ / ⓔ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2903
Ereignis-ID in Kaspersky Security Center	00000b89
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Der verbotene Vorgang wurde im Testmodus erlaubt

Zustand	⚠
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2961
Ereignis-ID in Kaspersky Security Center	00000b91
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Seit über 30 Minuten ist keine Verbindung zum Integrationsserver möglich. Überprüfen Sie den Status des Integrationsservers und die Netzwerkeinstellungen

Zustand	⚠
Komponente	Light Agent
Windows-Ereignis-ID	3102
Ereignis-ID in Kaspersky Security Center	00000c1e
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Seit über 6 Stunden ist keine Verbindung zum Integrationsserver möglich. Überprüfen Sie den Status des Integrationsservers und die Netzwerkeinstellungen

Zustand	⚠
Komponente	Light Agent
Windows-Ereignis-ID	3103
Ereignis-ID in Kaspersky Security Center	00000c1f
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine Verbindung zum Integrationsserver ist nicht möglich. Überprüfen Sie den Status des Integrationsservers und die Netzwerkeinstellungen

Zustand	⚠
Komponente	Light Agent
Windows-Ereignis-ID	3101
Ereignis-ID in Kaspersky Security Center	00000c1d
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Vorlage für virtuelle Maschinen muss aktualisiert werden

Zustand	⚠
Komponente	Light Agent
Windows-Ereignis-ID	3181
Ereignis-ID in Kaspersky Security Center	00000c6d
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Standard-Lizenz wurde beendet. Die App wird im Rahmen der Enterprise-Lizenz ausgeführt

Zustand	⚠
Komponente	Light Agent
Windows-Ereignis-ID	3171
Ereignis-ID in Kaspersky Security Center	00000c64
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zustand	⚠
Komponente	Überwachung der Datei-Integrität
Windows-Ereignis-ID	2901
Ereignis-ID in Kaspersky Security Center	00000b55
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zustand	⚠
Komponente	Überwachung der Datei-Integrität
Windows-Ereignis-ID	2900
Ereignis-ID in Kaspersky Security Center	00000b54
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Informative Meldung

Programm wurde gestartet

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	235
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Programm wurde beendet

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	236
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Selbstschutz hat den Zugriff auf die geschützte Ressource beschränkt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	213
Ereignis-ID in Kaspersky Security Center	000000d5
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Bericht wurde gelöscht

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	217
Ereignis-ID in Kaspersky Security Center	000000d9
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Gruppenrichtlinie wurde deaktiviert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	220
Ereignis-ID in Kaspersky Security Center	000000dc
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Programmeinstellungen wurden geändert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	218
Ereignis-ID in Kaspersky Security Center	000000da
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Aufgabe gestartet

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	221
Ereignis-ID in Kaspersky Security Center	000000dd
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aufgabe abgeschlossen

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	223
Ereignis-ID in Kaspersky Security Center	000000df
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Alle Programmkomponenten, die gemäß Lizenz verwendet werden können, sind installiert und funktionieren normal

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	227
Ereignis-ID in Kaspersky Security Center	000000e3
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Abonnement-Einstellungen wurden geändert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	238
Ereignis-ID in Kaspersky Security Center	000000ee
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Abonnement wurde verlängert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	239
Ereignis-ID in Kaspersky Security Center	000000ef
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Objekt wurde aus dem Backup wiederhergestellt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	335
Ereignis-ID in Kaspersky Security Center	0000014f
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eingabe eines Benutzernamens und Kennworts

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	2000
Ereignis-ID in Kaspersky Security Center	000007d0
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Teilnahme an KSN ist aktiviert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	2020
Ereignis-ID in Kaspersky Security Center	000007e4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die KSN-Server sind verfügbar

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	2022
Ereignis-ID in Kaspersky Security Center	000007e6
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Programm funktioniert und verarbeitet Daten gemäß den entsprechenden Gesetzen, und es verwendet die passende Infrastruktur

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	2024
Ereignis-ID in Kaspersky Security Center	000007e8
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde aus der Quarantäne wiederhergestellt

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	345
Ereignis-ID in Kaspersky Security Center	00000159
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde aus der Quarantäne gelöscht

Zustand	
Komponente	Systemaudit
Windows-Ereignis-ID	347
Ereignis-ID in Kaspersky Security Center	0000015b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Eine Backup-Kopie des Objekts wurde angelegt

Zustand	
Komponente	Schutz vor bedrohlichen Dateien Schutz vor E-Mail-Bedrohungen Verhaltensanalyse Schutz vor Verschlüsselung Programm-Überwachung Sandbox Schadsoftware-Untersuchung
Windows-Ereignis-ID	308
Ereignis-ID in Kaspersky Security Center	00000134
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Objekt wurde durch eine früher desinfizierte Kopie ersetzt

Zustand	
Komponente	Schutz vor bedrohlichen Dateien Programm-Überwachung Schadsoftware-Untersuchung
Windows-Ereignis-ID	327
Ereignis-ID in Kaspersky Security Center	00000147
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Kennwortgeschütztes Archiv gefunden

Zustand	
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Programm-Überwachung Schadsoftware-Untersuchung
Windows-Ereignis-ID	322
Ereignis-ID in Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
Ereignisparameter	• GNRL_EA_PARAM_2 ist der Name des Objekts. • GNRL_EA_PARAM_3 ist das Erstellungsdatum des Objekts (optional). • GNRL_EA_PARAM_7 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_9 sind zusätzliche Informationen über das erkannte Objekt: Anwendungskomponente (engine). Technologien zum Erkennen von Bedrohungen (method). Bedrohung wurde erkannt von „Private KSN“ (denylist): true oder false.

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Informationen über das gefundene Objekt

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Programm-Überwachung Schadsoftware-Untersuchung
Windows-Ereignis-ID	332
Ereignis-ID in Kaspersky Security Center	0000014c
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Objekt steht auf der Allow-Liste von Kaspersky Private Security Network

Zustand	ⓘ
Komponente	Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Programm-Überwachung Schadsoftware-Untersuchung
Windows-Ereignis-ID	340
Ereignis-ID in Kaspersky Security Center	00000154
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt umbenannt

Zustand	ⓘ
Komponente	Schutz vor E-Mail-Bedrohungen Exploit-Prävention Verhaltensanalyse Schutz vor Verschlüsselung Schadsoftware-Untersuchung
Windows-Ereignis-ID	329
Ereignis-ID in Kaspersky Security Center	00000149
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt verarbeitet

Zustand	ⓘ
Komponente	Programm-Überwachung Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen Schadsoftware-Untersuchung
Windows-Ereignis-ID	301

Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Objekt übersprungen

Zustand	ⓘ
Komponente	Programm-Überwachung Schutz vor bedrohlichen Dateien AMSI-Schutz Schadsoftware-Untersuchung
Windows-Ereignis-ID	315
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Archiv gefunden

Zustand	ⓘ
Komponente	Programm-Überwachung Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Schadsoftware-Untersuchung
Windows-Ereignis-ID	318
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Gepacktes Objekt gefunden

Zustand	ⓘ
Komponente	Programm-Überwachung Schutz vor bedrohlichen Dateien Schutz vor Web-Bedrohungen Schutz vor E-Mail-Bedrohungen AMSI-Schutz Schadsoftware-Untersuchung
Windows-Ereignis-ID	319
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Link wurde verarbeitet

Zustand	ⓘ
Komponente	Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	361
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Programmstart erlaubt

Zustand	ⓘ
Komponente	Programmkontrolle
Windows-Ereignis-ID	701
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Update-Quelle wurde ausgewählt

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1001
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Proxyserver wurde ausgewählt

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1002
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Link steht auf der Allow-Liste von Kaspersky Private Security Network

Zustand	ⓘ
Komponente	Schutz vor Web-Bedrohungen
Windows-Ereignis-ID	370
Ereignis-ID in Kaspersky Security Center	00000172
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Programm wurde in die vertrauenswürdige Gruppe verschoben

Zustand	ⓘ
Komponente	Programm-Überwachung
Windows-Ereignis-ID	401
Ereignis-ID in Kaspersky Security Center	00000191

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Programm wurde in die beschränkte Gruppe verschoben

Zustand	ⓘ
Komponente	Programm-Überwachung
Windows-Ereignis-ID	402
Ereignis-ID in Kaspersky Security Center	00000192
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Komponente Programm-Überwachung wurde ausgelöst

Zustand	ⓘ
Komponente	Programm-Überwachung
Windows-Ereignis-ID	403
Ereignis-ID in Kaspersky Security Center	00000193
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Datei wiederhergestellt

Zustand	ⓘ
Komponente	Verhaltensanalyse Schutz vor Verschlüsselung Exploit-Prävention Programm-Überwachung
Windows-Ereignis-ID	457
Ereignis-ID in Kaspersky Security Center	000001c9
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Registrierungswert wiederhergestellt

Zustand	ⓘ
Komponente	Verhaltensanalyse Exploit-Prävention
Windows-Ereignis-ID	458
Ereignis-ID in Kaspersky Security Center	000001ca
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Registrierungswert gelöscht

Zustand	ⓘ
Komponente	Verhaltensanalyse Exploit-Prävention

Windows-Ereignis-ID	459
Ereignis-ID in Kaspersky Security Center	000001cb
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Aktion eines Prozesses übersprungen

Zustand	ⓘ
Komponente	Adaptive Kontrolle von Anomalien
Windows-Ereignis-ID	2201
Ereignis-ID in Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Name der Regel der „Adaptiven Kontrolle von Anomalien“. • GNRL_EA_PARAM_2 ist die ID der heuristischen Regel. • GNRL_EA_PARAM_3 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_4 ist der Quellprozess. • GNRL_EA_PARAM_5 ist das Quellobjekt. • GNRL_EA_PARAM_6 ist der Zielprozess. • GNRL_EA_PARAM_7 ist das Zielobjekt. • GNRL_EA_PARAM_8 sind zusätzliche Informationen über das erkannte Objekt: Hashs des Quellprozesses bzw. -objekts und des Zielprozesses bzw. -objekts. Prozess wurde blockiert (verdict_type): true oder false. Benutzer-Sicherheits-ID (SID).
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Tastatur autorisiert

Zustand	ⓘ
Komponente	Schutz vor BadUSB-Angriffen
Windows-Ereignis-ID	2050
Ereignis-ID in Kaspersky Security Center	00000802
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Netzwerkaktivität erlaubt

Zustand	ⓘ
Komponente	Firewall
Windows-Ereignis-ID	601
Ereignis-ID in Kaspersky Security Center	00000259
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Programmstart im Testmodus verboten

Zustand	ⓘ
Komponente	Programmkontrolle
Windows-Ereignis-ID	703

Ereignis-ID in Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Ereignisparameter	• GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_3 ist die ID der manuell erstellten Kategorie. • GNRL_EA_PARAM_4 ist die Kontosicherheits-ID (SID). • GNRL_EA_PARAM_5 sind Informationen über die digitale Signatur der Anwendung. • GNRL_EA_PARAM_6 ist der Name der ausführbaren Datei der Anwendung (z. B. chrome.exe). • GNRL_EA_PARAM_7 ist der Pfad der ausführbaren Datei. • GNRL_EA_PARAM_8 ist der Hash des Objekts (SHA256). • GNRL_EA_PARAM_9 ist die Version der Anwendung, die der Benutzer auszuführen versucht.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Programmstart im Testmodus erlaubt

Zustand	ⓘ
Komponente	Programmkontrolle
Windows-Ereignis-ID	704
Ereignis-ID in Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
Ereignisparameter	• GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_3 ist die ID der manuell erstellten Kategorie. • GNRL_EA_PARAM_4 ist die Kontosicherheits-ID (SID). • GNRL_EA_PARAM_5 sind Informationen über die digitale Signatur der Anwendung.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Eine erlaubte Seite wurde geöffnet

Zustand	ⓘ
Komponente	Web-Kontrolle
Windows-Ereignis-ID	751
Ereignis-ID in Kaspersky Security Center	000002f4
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Vorgang mit dem Gerät erlaubt

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	801
Ereignis-ID in Kaspersky Security Center	00000321
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Dateivorgang ausgeführt

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	808
Ereignis-ID in Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
Ereignisparameter	• GNRL_EA_PARAM_1 ist der Dateivorgang (Schreiben oder Löschen). • GNRL_EA_PARAM_2 ist der Pfad der Datei. • GNRL_EA_PARAM_3 ist der Name des Gerätes. • GNRL_EA_PARAM_4 ist der Name des Sitzungsbenutzers. • GNRL_EA_PARAM_5 ist die Hardware-ID (HWID).
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Es sind keine Updates verfügbar

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1020
Ereignis-ID in Kaspersky Security Center	000003fc
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Update-Verteilung wurde erfolgreich abgeschlossen

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1022
Ereignis-ID in Kaspersky Security Center	000003fe
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Dateien werden heruntergeladen

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1003
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Datei wurde heruntergeladen

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1004
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Datei installiert

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1005
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Datei wurde aktualisiert

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1006
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Datei wurde wegen eines Update-Fehlers zurückgesetzt

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1007
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Dateien werden aktualisiert

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1008
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Updates werden verteilt

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1009
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Dateien werden zurückgesetzt

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1010
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Download-Liste wird erstellt

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	1013
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Patches werden heruntergeladen

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	2150
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Patch wird installiert

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	2151
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Patch wurde installiert

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	2152
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Patch wird rückgängig gemacht

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	2154
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Patch wurde rückgängig gemacht

Zustand	ⓘ
Komponente	Update
Windows-Ereignis-ID	2155
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Anwenden von Verschlüsselungs-/Entschlüsselungsregeln für Dateien wurde gestartet

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	901
Ereignis-ID in Kaspersky Security Center	00000385
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Anwenden von Verschlüsselungs-/Entschlüsselungsregeln für Dateien wurde abgeschlossen

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	902
Ereignis-ID in Kaspersky Security Center	00000386
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Das Anwenden von Verschlüsselungs-/Entschlüsselungsregeln für Dateien wurde fortgesetzt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	905
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung von Dateien wurde gestartet

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	910
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung von Dateien wurde abgeschlossen

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	911
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Dateiverschlüsselung wurde nicht ausgeführt, weil die Datei als Ausnahme gilt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	913
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der portable Modus wurde aktiviert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	950
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der portable Modus wurde deaktiviert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	952
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung des Gerätes wurde gestartet

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1301
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung des Gerätes wurde abgeschlossen

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1302
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Verschlüsselung/Entschlüsselung des Gerätes wurde fortgesetzt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1304
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Gerät wurde nicht verschlüsselt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1307
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Vorgang zur Verschlüsselung/Entschlüsselung des Geräts wurde in den aktiven Modus umgestellt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1308
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Vorgang zur Verschlüsselung/Entschlüsselung des Geräts wurde in den passiven Modus umgestellt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1309
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Verschlüsselungsmodul wurde geladen

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1310
Ereignis-ID in Kaspersky Security Center	0000051e
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Authentifizierungsagentenkonto erstellt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1330
Ereignis-ID in Kaspersky Security Center	00000532
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Benutzerkonto des Authentifizierungsagenten wurde gelöscht

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1331
Ereignis-ID in Kaspersky Security Center	00000533
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Kennwort für das Benutzerkonto des Authentifizierungsagenten wurde geändert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1332
Ereignis-ID in Kaspersky Security Center	00000534

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Erfolgreiche Anmeldung im Authentifizierungsagenten

Zustand	
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1333
Ereignis-ID in Kaspersky Security Center	00000535
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die Anmeldung im Authentifizierungsagenten ist fehlgeschlagen

Zustand	
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1334
Ereignis-ID in Kaspersky Security Center	00000536
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Zugriff auf die Festplatte wurde mithilfe einer Zugriffsanfrage für verschlüsselte Geräte gewährt

Zustand	
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1335
Ereignis-ID in Kaspersky Security Center	00000537
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Ein Versuch, mithilfe einer Zugriffsanfrage für verschlüsselte Geräte Zugriff auf die Festplatte zu erhalten, ist fehlgeschlagen

Zustand	
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1336
Ereignis-ID in Kaspersky Security Center	00000538
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Benutzerkonto wurde nicht hinzugefügt. Dieses Benutzerkonto ist bereits vorhanden

Zustand	
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1337
Ereignis-ID in Kaspersky Security Center	00000539

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Benutzerkonto wurde nicht geändert. Dieses Benutzerkonto ist nicht vorhanden

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1338
Ereignis-ID in Kaspersky Security Center	0000053a
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Das Benutzerkonto wurde nicht gelöscht. Dieses Benutzerkonto ist nicht vorhanden

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1339
Ereignis-ID in Kaspersky Security Center	0000053b
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Die vollständige Festplattenverschlüsselung wurde erfolgreich aktualisiert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1341
Ereignis-ID in Kaspersky Security Center	0000053d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Upgrade der vollständigen Festplattenverschlüsselung erfolgreich zurückgerollt

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1343
Ereignis-ID in Kaspersky Security Center	0000053f
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Deinstallation der Treiber für die Kaspersky-Festplattenverschlüsselung aus dem WinRE-Image ist fehlgeschlagen

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1346
Ereignis-ID in Kaspersky Security Center	00000542

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

BitLocker-Wiederherstellungsschlüssel wurde geändert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1370
Ereignis-ID in Kaspersky Security Center	0000055a
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

BitLocker-Kennwort/PIN wurde geändert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1371
Ereignis-ID in Kaspersky Security Center	0000055b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

BitLocker-Wiederherstellungsschlüssel wurde auf einem Wechseldatenträger gespeichert

Zustand	ⓘ
Komponente	Datenverschlüsselung
Windows-Ereignis-ID	1372
Ereignis-ID in Kaspersky Security Center	0000055c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aufgaben vom Server für Kaspersky Anti Targeted Attack Platform werden nicht verarbeitet

Zustand	ⓘ
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2103
Ereignis-ID in Kaspersky Security Center	00000837
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Endpoint Sensor ist mit dem Server verbunden

Zustand	ⓘ
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2101
Ereignis-ID in Kaspersky Security Center	00000835

Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Verbindung mit dem Server für Kaspersky Anti Targeted Attack Platform wurde wiederhergestellt

Zustand	ⓘ
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2102
Ereignis-ID in Kaspersky Security Center	00000836
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Aufgaben des Servers für Kaspersky Anti Targeted Attack Platform werden verarbeitet

Zustand	ⓘ
Komponente	Endpoint Sensor
Windows-Ereignis-ID	2104
Ereignis-ID in Kaspersky Security Center	00000838
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt gelöscht

Zustand	ⓘ
Komponente	Daten löschen
Windows-Ereignis-ID	2251
Ereignis-ID in Kaspersky Security Center	000008cb
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Aufgabenstatistik zurücksetzen

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises)
Windows-Ereignis-ID	2853
Ereignis-ID in Kaspersky Security Center	00000b25
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zustand	ⓘ
Komponente	Daten löschen
Windows-Ereignis-ID	2253
Ereignis-ID in Kaspersky Security Center	000008cd
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde in die Quarantäne verschoben (Sandbox)

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	2602
Ereignis-ID in Kaspersky Security Center	00000a2a
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde gelöscht (Sandbox)

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	2604
Ereignis-ID in Kaspersky Security Center	00000a2c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

IOC-Untersuchung gestartet

Zustand	ⓘ
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2652
Ereignis-ID in Kaspersky Security Center	00000a5c
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

IOC-Untersuchung abgeschlossen

Zustand	ⓘ
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2653
Ereignis-ID in Kaspersky Security Center	00000a5d
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde in die Quarantäne verschoben (Endpoint Detection and Response)

Zustand	ⓘ
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2555
Ereignis-ID in Kaspersky Security Center	000009fb
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Objekt wurde gelöscht (Endpoint Detection and Response)

Zustand	ⓘ
Komponente	Endpoint Detection and Response
Windows-Ereignis-ID	2557
Ereignis-ID in Kaspersky Security Center	000009fd
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Auswahl der Programmkomponenten wurde erfolgreich geändert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	1402
Ereignis-ID in Kaspersky Security Center	0000057a
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	2606
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	2609
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	2610
Ereignis-ID in Kaspersky Security Center	–
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	2616
Ereignis-ID in Kaspersky Security Center	–

Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	–

Der Administrationsserver, mit dem Ihr Gerät verbunden ist, wurde als vertrauenswürdig eingestuft

Zustand	ⓘ
Komponente	Schutz der Verbindung zum Administrationsserver
Windows-Ereignis-ID	`3300`
Ereignis-ID in Kaspersky Security Center	`00000ce4`
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ihr Gerät ist mit einem neuen vertrauenswürdigen Administrationsserver verbunden

Zustand	ⓘ
Komponente	Schutz der Verbindung zum Administrationsserver
Windows-Ereignis-ID	`3302`
Ereignis-ID in Kaspersky Security Center	`00000ce6`
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Administrationsserver, mit dem Ihr Gerät verbunden ist, gilt nicht mehr als vertrauenswürdig

Zustand	ⓘ
Komponente	Schutz der Verbindung zum Administrationsserver
Windows-Ereignis-ID	`3303`
Ereignis-ID in Kaspersky Security Center	`00000ce7`
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Asynchrone Erkennung durch "Sandbox

Zustand	ⓘ
Komponente	Sandbox
Windows-Ereignis-ID	`2619`
Ereignis-ID in Kaspersky Security Center	`GNRL_EV_APP_INCIDENT_OCCURED`
Ereignisparameter	• `GNRL_EA_PARAM_1` sind Parameter der Komponenten von Sandbox. • `GNRL_EA_PARAM_2` ist der Pfad des Objekts. • `GNRL_EA_PARAM_3` ist die Vorfall-ID. • `GNRL_EA_PARAM_4` ist der Hash des Objekts (SHA256).
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Untersuchungsaufgabe wurde vom Benutzer erfolgreich an Sandbox gesendet

Zustand	ⓘ
Komponente	Sandbox

Windows-Ereignis-ID	2622
Ereignis-ID in Kaspersky Security Center	00000a3e
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Verbindung mit dem Gerät wurde hergestellt

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	805
Ereignis-ID in Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
Ereignisparameter	• GNRL_EA_PARAM_1 ist die Hardware-ID (HWID). • GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Die Verbindung mit dem Gerät wurde getrennt

Zustand	ⓘ
Komponente	Gerätekontrolle
Windows-Ereignis-ID	806
Ereignis-ID in Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
Ereignisparameter	• GNRL_EA_PARAM_1 ist die Hardware-ID (HWID). • GNRL_EA_PARAM_2 ist der Name des Sitzungsbenutzers.
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Erfolgreiche Verbindung zum EDR Expert-Server

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises)
Windows-Ereignis-ID	2853
Ereignis-ID in Kaspersky Security Center	00000b25
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Erfolgreiche Verbindung zum Reaktionsserver von EDR Expert

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2853
Ereignis-ID in Kaspersky Security Center	00000b25
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Erfolgreiche Verbindung zum EDR Expert-Telemetrie-Erfassungsserver

Zustand	ⓘ
Komponente	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows-Ereignis-ID	2857
Ereignis-ID in Kaspersky Security Center	00000b26
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Erfolgreiche Verbindung zum NDR-Server

Zustand	ⓘ
Komponente	Network Detection and Response (KATA)
Windows-Ereignis-ID	3083
Ereignis-ID in Kaspersky Security Center	00000c0b
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Start der Client-App des Cloud-Dienstes wurde erlaubt

Zustand	ⓘ
Komponente	Cloud Discovery
Windows-Ereignis-ID	2210
Ereignis-ID in Kaspersky Security Center	000008a2
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Der Zugriff auf den Cloud-Dienst wurde erlaubt

Zustand	ⓘ
Komponente	Cloud Discovery
Windows-Ereignis-ID	2211
Ereignis-ID in Kaspersky Security Center	000008a3
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Zugriff auf den Schutzbereich

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	2004
Ereignis-ID in Kaspersky Security Center	000007d4
Windows-Ereignisprotokoll (Standard)	✓
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Änderung einer Datei oder eines Ordners wurde erkannt

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2950
Ereignis-ID in Kaspersky Security Center	00000b86
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Das Objekt ändert sich zu oft. Die Ereignisaggregation wurde gestartet

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2955
Ereignis-ID in Kaspersky Security Center	00000b8b
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Bericht über eine Objektänderung für den Aggregationszeitraum

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2956
Ereignis-ID in Kaspersky Security Center	00000b8c
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Änderung der Registrierung wurde erkannt

Zustand	ⓘ / ⚠ / ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2951
Ereignis-ID in Kaspersky Security Center	00000b87
Windows-Ereignisprotokoll (Standard)	–

Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Verbindung bzw. Trennung der Verbindung zu einem Gerät wurde erkannt

Zustand	ⓘ / ⚠ / !
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2952
Ereignis-ID in Kaspersky Security Center	00000b88
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Der Überwachungsbereich enthält ungültige Objekte

Zustand	ⓘ / ⚠ / !
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2903
Ereignis-ID in Kaspersky Security Center	00000b89
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Baseline erstellt

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2957
Ereignis-ID in Kaspersky Security Center	00000b8d
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Baseline aktualisiert

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität

Windows-Ereignis-ID	2958
Ereignis-ID in Kaspersky Security Center	00000b8e
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein Vorgang wird von dem vertrauenswürdigen Benutzer ausgeführt

Zustand	ⓘ
Komponente	Überwachung der Systemintegrität
Windows-Ereignis-ID	2962
Ereignis-ID in Kaspersky Security Center	00000b92
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Um die Aufbewahrungsdauer für dieses Ereignis zu konfigurieren, gehen Sie zum Abschnitt **Konfiguration von Ereignissen** der Richtlinie und legen Sie die Aufbewahrungsdauer für das allgemeine Ereignis Überwachung der Systemintegrität *Änderung einer Datei oder eines Ordners wurde erkannt* fest.

Mit SVM verbunden

Zustand	ⓘ
Komponente	Light Agent
Windows-Ereignis-ID	3152
Ereignis-ID in Kaspersky Security Center	00000c50
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Ein neues temporäres Kennwort wurde generiert

Zustand	ⓘ
Komponente	Systemaudit
Windows-Ereignis-ID	265
Ereignis-ID in Kaspersky Security Center	00000109
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Mit dem Integrationsserver verbunden

Zustand	ⓘ
Komponente	Light Agent
Windows-Ereignis-ID	3105
Ereignis-ID in Kaspersky Security Center	00000c21
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Verbindung zum Integrationsserver wird wiederhergestellt

Zustand	ⓘ
Komponente	Light Agent
Windows-Ereignis-ID	3104
Ereignis-ID in Kaspersky Security Center	00000c20
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Erfolgreiche Verbindung zum KUMA-Server

Zustand	ⓘ
Komponente	KUMA-Integration
Windows-Ereignis-ID	2857
Ereignis-ID in Kaspersky Security Center	00000b29
Windows-Ereignisprotokoll (Standard)	–
Ereignisprotokoll von Kaspersky Security Center (Standard)	✓

Anhang 7. Unterstützte Dateierweiterungen für die Ausführungsverhinderung

Kaspersky Endpoint Security ermöglicht es, dass Dateien im Office-Format in bestimmten Programmen nicht geöffnet werden können. Die Informationen zu unterstützten Dateierweiterungen und Anwendungen sind in der folgenden Tabelle aufgeführt.

Unterstützte Dateierweiterungen für die Ausführungsverhinderung

Name des Programms	Ausführbare Datei	Dateierweiterung
Microsoft Word	winword.exe	rtf doc Punkt docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw

Name des Programms	Ausführbare Datei	Dateierweiterung
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Anhang 8. Unterstützte Skript-Interpreter für die Ausführungsprävention

Die Ausführungsverhinderung unterstützt die folgenden Skriptinterpreter:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe

- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

Die Ausführungsverhinderung unterstützt die Arbeit mit Java-Anwendungen in der Java-Laufzeitumgebung (java.exe- und javaw.exe-Prozesse).

Anhang 9. IOC-Untersuchungsbereich in der Registrierung (RegistryItem)

Wenn Sie den Datentyp **Windows-Registrierung – RegistryItem** zum IOC-Untersuchungsbereich hinzufügen, untersucht Kaspersky Endpoint Security standardmäßig die folgenden Registrierungsschlüssel:

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile
```

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Anhang 10. Anforderungen für IOC-Dateien

Beachten Sie bei der Erstellung von IOC-Untersuchungsaufgaben die folgenden Anforderungen und Beschränkungen für IOC-Dateien:

- Für die Beschreibung von Kompromittierungsindikatoren unterstützt das Programm IOC-Dateien mit den IOC- und XML-Erweiterungen im offenen OpenIOC-Standard Version 1.0 und 1.1.
- Nachdem Sie IOC-Dateien hochgeladen haben, können Sie die Dateien im integrierten Editor direkt in den Aufgabeneigenschaften manuell bearbeiten. Kaspersky Endpoint Security unterstützt die Bearbeitung von IOC-Dateien, die dem OpenIOC 1.1-Standard entsprechen. Der Inhalt von IOC-Dateien, die der OpenIOC Version 1.0 entsprechen, kann nicht geändert werden.
- Wenn Sie über die Befehlszeile eine Aufgabe des Typs *IOC-Untersuchung* erstellen und dabei IOC-Dateien hochladen, von denen einige nicht unterstützt werden, verwendet das Programm bei der Ausführung der Aufgabe nur die unterstützten IOC-Dateien. Wenn Sie über die Befehlszeile eine Aufgabe *IOC-Untersuchung* erstellen und alle dabei hochgeladenen IOC-Dateien nicht unterstützt werden, kann die Aufgabe zwar ausgeführt werden, es werden jedoch keine Kompromittierungsindikatoren erkannt. Das Hochladen von nicht unterstützten IOC-Dateien über „Web Console“ oder „Cloud Console“ ist nicht möglich.
- Semantische Fehler und nicht unterstützte IOC-Ausdrücke und Tags führen nicht zu einem Fehlschlagen der Aufgabe. In solchen Fällen findet das Programm in den entsprechenden Abschnitten der IOC-Datei lediglich keine Übereinstimmung.
- Die Identifikatoren aller IOC-Dateien, die in einer einzelnen IOC-Untersuchungsaufgabe verwendet werden, müssen eindeutig sein. Das Vorhandensein von IOC-Dateien mit dem gleichen Identifikator kann sich auf die Ergebnisse der Aufgabenausführung auswirken.
- Eine einzelne IOC-Datei darf nicht größer sein als 2 MB. Die Verwendung größerer Dateien führt dazu, dass IOC-Untersuchungsaufgaben mit einem Fehler abgebrochen werden. Die Gesamtgröße aller zur IOC-Sammlung hinzugefügten Dateien darf 10 MB nicht überschreiten. Wenn die Gesamtgröße aller Dateien 10 MB überschreitet, müssen Sie die IOC-Sammlung aufteilen und mehrere Aufgaben *IOC-Untersuchung* erstellen.
- Es wird empfohlen, eine IOC-Datei pro Bedrohung zu erstellen. Dadurch können die Ergebnisse der Aufgabe *IOC-Untersuchung* einfacher analysiert werden.

Die Datei, die Sie über den unten stehenden Link herunterladen können, enthält eine Tabelle mit einer vollständigen Liste der IOC-Bedingungen gemäß OpenIOC-Standard.

DATEI „IOC_TERMS.XLSX“ HERUNTERLADEN

Die folgende Tabelle enthält die Merkmale und Beschränkungen für die Unterstützung des OpenIOC-Standards durch das Programm.

Unterstützte Bedingungen	OpenIOC 1.0:
	
	`is`
	`isnot` (als Ausnahme vom Set)
	`contains`
	`containsnot` (als Ausnahme vom Set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	Für Email/*-Ausdrücke werden nur die Bedingungen `contains` und `is` unterstützt. Damit die retrospektive IOC-Untersuchung in Verbindung mit der Bedingung `is` korrekt funktioniert, müssen E-Mail-Adressen in IOC-Dateien im folgenden Format angegeben werden: `"name@example.org" <SMTP:name@example.org>`. Wenn die Aufgabe *IOC-Untersuchung* wie gewöhnlich ausgeführt wird, reicht es aus, die E-Mail-Adresse im folgenden Format anzugeben: `name@example.org`.

Unterstützte Attribute von Bedingungen	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Unterstützte Operatoren	`AND` `OR`
Unterstützte Datentypen	`"date"`: Datum (zulässige Bedingungen: `is`, `greater-than`, `less-than`) `"int"`: Integer (zulässige Bedingungen: `is`, `greater-than`, `less-than`) `"string"`: String (zulässige Bedingungen: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: Dauer in Sekunden (zulässige Bedingungen: `is`, `greater-than`, `less-than`)

Merkmale der Interpretation von Datentypen	Die Datentypen `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"` und `"base64Binary"` werden als String interpretiert.
	
	Das Programm unterstützt die Einstellung `Content` für die Datentypen `int` und `date`, wenn diese in Intervallform angegeben ist:
	
	OpenIOC 1.0:
	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:
	Verwendung der Bedingungen `greater-than` und `less-than`
	Verwendung des Operators `TO` im Feld `Content`
	Die App unterstützt die Interpretation der Datentypen `date` und `duration`, wenn die Indikatoren das Format `ISO 8601, Zulu time zone, UTC` haben.

Anhang 11. API für EDR Threat Response

Kaspersky Endpoint Security 12.9 für Windows unterstützt jetzt Aktionen für EDR Threat Response (EDR responses) mithilfe der Kaspersky Security Center OpenAPI. Sie können also OpenAPI-Methoden verwenden, um die Reaktion auf EDR-Bedrohungen mithilfe von Python zu automatisieren. Sie können diese Methoden nutzen, wenn das Programm in SIEM-Lösungen integriert ist. *Kaspersky Unified Monitoring and Analysis Platform* ist die SIEM-Lösung von Kaspersky und unterstützt ab Version 3.4.1 die EDR Threat Response OpenAPI. Beispiele für Skripte finden Sie in der KUMA-Dokumentation.

Um Aktionen für EDR Threat Response auszuführen, müssen Sie eine Anfrage erstellen und diese mithilfe von KSC Open API (`AddIncident`) senden. Nachdem die Anfrage verarbeitet wurde, wird in der Kaspersky Security Center-Konsole eine spezielle Aufgabe erstellt.

Um bei der Reaktion auf EDR-Bedrohungen Aufgaben zu erstellen, müssen Sie eine Hintergrundverbindung zwischen dem Administrationsserver und Kaspersky Security Center Web Console herstellen. Der Dienst für die Hintergrundverbindung ist in Kaspersky Security Center Windows 14.2 oder höher und in Kaspersky Security Center Linux 15.2 oder höher verfügbar. Andere Konsolen werden nicht unterstützt, auch nicht die Konsolen von Kaspersky Detection and Response-Lösungen.

Für EDR Threat Response müssen Sie grundlegende Anfrageparameter angeben (beispielsweise im JSON-Format):

- `task` ist der Aufgabentyp (siehe unten).
- `targetHost` ist die ID des Computers, auf dem das Skript ausgeführt werden soll. Obligatorisches Argument. Das Skript ruft dieses Argument aus dem Ereignis ab.
- `responseEventIncidentArea` ist der Name des Programms, das das Skript ausgeführt hat (z. B. `KUMA`). Dieser Parameter wird dem Namen der erstellten Aufgabe hinzugefügt.

Um EDR Threat Response zu konfigurieren, müssen Sie die Aufgabeneinstellungen im JSON-Format im Parameter `"KLINCDT_BODY": json.dumps(data)` angeben. Daraufhin erstellt das Programm die Aufgabe `[Response] [KUMA] <task type> - <Date> <Time> - <ID>` in der Kaspersky Security Center-Konsole.

Mit Kaspersky Security Center OpenAPI verbinden

Als Teil von EDR Threat Response erstellt das Programm spezielle Aufgaben in der Konsole von Kaspersky Security Center. Um diese Aufgaben zu erstellen, muss eine Verbindung zwischen dem Computer und Kaspersky Security Center hergestellt werden. Dazu müssen in der Anfrage Verbindungseinstellungen für Kaspersky Security Center angegeben werden.

In Kaspersky XDR Version 2.1 wurde die Methode zur Autorisierung von Anfragen geändert. Kaspersky XDR verwendet PAT-Tokens anstelle der Authentifizierung mit Benutzername und Kennwort. Daher können in Kaspersky XDR keine Skripte ausgeführt werden. Weitere Informationen zu Autorisierungsanfragen finden Sie in der Hilfe zu Kaspersky XDR.

Verbindungseinstellungen für Kaspersky Security Center

Einstellung	Typ	Beschreibung
`kscHost`	`string`	Adresse des Administrationsservers von Kaspersky Security Center. Erforderlicher Parameter.
`kscPort`	`int`	Port für die Verbindung zum Administrationsserver. Erforderlicher Parameter.
`kscCert`	`string`	Pfad einer Zertifikatsdatei für die Verbindung mit dem Kaspersky Security Center-Administrationsserver. Dieser Parameter hat standardmäßig den Wert `False`.
`kscUser`	`string`	Name des Benutzerkontos. Erforderlicher Parameter.
`kscPassword`	`string`	Kennwort des Benutzerkontos. Erforderlicher Parameter.

Beispiel

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
```

```
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

Die Daten des Benutzerkontos sind nicht geschützt. Daher müssen Sie einen separaten Benutzer festlegen, der nur für diese Aktionen verwendet wird.

Datei anfordern – getFile

Einstellungen der Aufgabe Datei anfordern

Einstellung	Typ	Beschreibung
md5hash	string	MD5-Hash der Datei, die Sie abrufen möchten.
sha256hash	string	SHA256-Hash der Datei, die Sie abrufen möchten.
path	string	Pfad der Datei, die Sie abrufen möchten.

Beispiel

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

Datei löschen – deleteFile

Einstellungen der Aufgabe Datei löschen

Einstellung	Typ	Beschreibung
`md5hash`	`string`	MD5-Hash der Datei, die Sie löschen möchten.
`sha256hash`	`string`	SHA256-Hash der Datei, die Sie löschen möchten.
`path`	`string`	Pfad der Datei, die Sie löschen möchten.
`searchInSubfolders?`	`boolean`	In Unterordnern nach der Datei suchen, die Sie löschen möchten.

Beispiel

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

Datei in Quarantäne verschieben – quarantineFile

Einstellungen der Aufgabe Datei in Quarantäne verschieben

Einstellung	Typ	Beschreibung
`md5hash`	`string`	MD5-Hash der Datei, die Sie in die Quarantäne verschieben möchten.
`sha256hash`	`string`	SHA256-Hash der Datei, die Sie in die Quarantäne verschieben möchten.
`path`	`string`	Pfad der Datei, die Sie in die Quarantäne verschieben möchten.

Beispiel

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

IOC-Untersuchung – iocScan

Einstellungen der Aufgabe IOC-Untersuchung

Einstellung	Typ	Beschreibung
`ioc`	`string`	Pfad des zip-Archivs mit einer IOC-Datei, die Sie zur Untersuchung verwenden möchten.
`isolateHost`	`boolean`	Den Computer vom Netzwerk isolieren, wenn ein Kompromittierungsindikator erkannt wird. Dadurch wird die Ausbreitung der Bedrohung verhindert.
`scanCriticalAreas`	`boolean`	Aufgabe *Untersuchung wichtiger Bereiche* ausführen, wenn ein Kompromittierungsindikator gefunden wird.
`quarantineObject`	`boolean`	Das schädliche Objekt löschen, wenn ein Kompromittierungsindikator gefunden wird. Bevor das Objekts gelöscht wird, erstellt Kaspersky Endpoint Security eine Backup-Kopie für den Fall, dass das Objekt später wiederhergestellt werden muss. Kaspersky Endpoint Security verschiebt die Backup-Kopie in die Quarantäne.

Beispiel

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

Prozess starten – startProcess

Einstellungen der Aufgabe Prozess starten

Einstellung	Typ	Beschreibung
`executablePath`	`string`	Pfad der ausführbaren Datei, die zum Starten des Prozesses verwendet wird.
`arguments?`	`string`	Zusätzliche Befehlszeilenargumente zum Starten des Prozesses.
`workingFolder?`	`string`	Pfad des Arbeitsordners des Prozesses.

Beispiel

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

Prozess beenden – terminateProcess

Einstellungen der Aufgabe Prozess beenden

Einstellung	Typ	Beschreibung
`md5hash`	`string`	MD5-Hash der Datei, deren Prozess Sie beenden möchten.
`sha256hash`	`string`	SHA256-Hash der Datei, deren Prozess Sie beenden möchten.
`path`	`string`	Pfad der Datei, die Sie löschen möchten.
`caseSensitive`	`boolean`	Bei der Suche nach der Datei wird die Groß-/Kleinschreibung beachtet.

Beispiel

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Netzwerkisolation des Computers – isolateHost

Einstellungen der Netzwerkisolation des Computers

Einstellung	Typ	Beschreibung
`action`	`string`	Funktionsmodus der Netzwerkisolation.

Beispiel

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

Ausführungsprävention – preventExecution

Einstellungen der Ausführungsprävention

Einstellung	Typ	Beschreibung
hash	string	MD5-Hash der Datei, deren Ausführung Sie verhindern möchten.
path	string	Pfad der Datei, deren Ausführung Sie verhindern möchten.
caseSensitive	boolean	Bei der Suche nach der Datei wird die Groß-/Kleinschreibung beachtet.

Beispiel

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

Schadsoftware-Untersuchung – onDemandScan

Einstellungen der Aufgabe Schadsoftware-Untersuchung

Einstellung	Typ	Beschreibung
path	string	Durch Leerzeichen getrennte Liste mit Dateien und Ordnern für die benutzerdefinierte Untersuchung.
recursive	boolean	Rekursiver Untersuchungsmodus.
type	number	Untersuchungsbereich.

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

Beispiel

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
```

```
  responseEventIncidentArea: string;
};
```

Anhang 12. Benutzerkonten in Regeln für App-Komponenten

Zum Konfigurieren bestimmter App-Komponenten müssen Sie spezielle Regeln hinzufügen. Für die „Web-Kontrolle“ müssen Sie beispielsweise eine Regel mit einer Liste von Webadressen hinzufügen, die von der App blockiert werden sollen. In Regeln für App-Komponenten können Sie auch einen Zeitplan für die Komponente konfigurieren oder Benutzer auswählen, auf welche die Regel angewendet werden soll.

Regeln müssen hinzugefügt werden, um die folgenden App-Komponenten zu konfigurieren:

- Programmkontrolle.
- Web-Kontrolle.
- Gerätekontrolle.
- Protokollanalyse.
- Adaptive Kontrolle von Anomalien.
- Überwachung der Systemintegrität.

Ab Kaspersky Endpoint Security für Windows 12.5 können Sie Benutzer nicht nur aus Active Directory auswählen, sondern auch aus der Benutzerliste in Kaspersky Security Center. Sie können die Daten eines lokalen Benutzerkontos auch manuell eingeben. Das bedeutet, dass Sie Benutzer auf folgende Weise hinzufügen können:

- Active Directory (empfohlen)
- Liste der Benutzer in Kaspersky Security Center
- Lokales Benutzerkonto

Damit alle Methoden zur Benutzerauswahl einwandfrei funktionieren, müssen Sie die App Kaspersky Endpoint Security und das Verwaltungs-Plug-in auf Version 12.5 oder höher aktualisieren.

Kaspersky empfiehlt, lokale Benutzerkonten nur in besonderen Fällen zu verwenden, in denen keine Domänenbenutzerkonten verwendet werden können. Einzelheiten zu den Sicherheitsrisiken bei der Verwendung lokaler Benutzerkonten finden Sie in der Microsoft-Wissensdatenbank. Sie tragen die volle Verantwortung für die Sicherheit eines Computers, wenn lokale Benutzerkonten verwendet werden. Dazu gehört insbesondere die Verantwortung für die Kontrolle und Beschränkung des Zugriffs auf die Einstellungen von Kaspersky Endpoint Security.

Die App verwendet die SID (Security Identifier) des Benutzers, um Benutzer zu identifizieren. Wenn Benutzerkonten aus Active Directory oder aus der Benutzerliste von Kaspersky Security Center verwendet werden, ermittelt die App die SID auf dem Administrationsserver. Dies bedeutet, dass die App den Computer nicht zusätzlich belastet, um einen Benutzer zu identifizieren. Wenn Sie einer App-Regel mehr als 1.000 lokale Benutzerkonten hinzugefügt haben, wendet sich die App an den Domänencontroller, um den Benutzer zu identifizieren. Dadurch wird die Belastung des Computers erhöht. Um die Auswirkungen auf die Leistung des Computers zu optimieren, empfehlen wir die Verwendung von Benutzerkonten aus Active Directory oder aus der Benutzerliste von Kaspersky Security Center.

Das Programm verwendet NetBIOS-Namen, um manuell hinzugefügte Benutzerkonten in den Formaten `<username>` und `<hostname>\<username>` zu identifizieren. Ein NetBIOS-Name kann bis zu 16 Byte (15 Zeichen) lang sein. Wenn der Computername länger als 15 Zeichen ist, kann das Programm den Benutzer nicht identifizieren. In diesem Fall deaktiviert das Programm die Regel und generiert einen Fehler (z. B. *Web-Kontrolle: Regelauslösung ist deaktiviert für Benutzerkonten ohne passende Sicherheits-ID (SID)*). Damit die Regel funktioniert, müssen Sie den Computernamen manuell kürzen. Sie können Benutzerkonten aus Active Directory oder Kaspersky Security Center hinzufügen. In diesem Fall kürzt das Programm den Computernamen automatisch.

Kaspersky Endpoint Security unterstützt in Regeln auch integrierte Benutzer und Gruppen (z. B. die Gruppe „Alle“). Aufgrund der Ermittlungsmethode für die Benutzer-SID erlaubt das Programm nur die Verwendung von integrierten Benutzerkonten, die aus Active Directory oder aus der Benutzerliste in Kaspersky Security Center hinzugefügt wurden. Regeln, in denen ein integriertes Benutzerkonto lokal hinzugefügt wird, funktionieren nicht.

Rechtliche Informationen

Bereitstellung von Daten

Dieser Abschnitt enthält Informationen über die Daten, die Kaspersky Endpoint Security auf dem Gerät speichern und während des Betriebs automatisch an Kaspersky übertragen kann.

Kaspersky schützt die erhaltenen Informationen in Übereinstimmung mit geltenden gesetzlichen Bestimmungen und mit den aktuellen Richtlinien von Kaspersky. Die Daten werden über verschlüsselte Verbindungskanäle übertragen.

Bereitstellung von Daten im Rahmen des Endbenutzer-Lizenzvertrags

Wenn für die Aktivierung von Kaspersky Endpoint Security ein Aktivierungscode verwendet wird, stimmen Sie zu, dass automatisch die folgenden Informationen regelmäßig an Kaspersky übertragen werden, damit die Rechtmäßigkeit der Programmverwendung überprüft werden kann:

- Typ, Version und Sprachversion von Kaspersky Endpoint Security
- Versionen der installierten Updates für Kaspersky Endpoint Security
- ID des Computers und ID der Installation von Kaspersky Endpoint Security auf dem Computer
- Seriennummer und ID des aktiven Schlüssels
- Typ, Version und Bit-Version des Betriebssystems, Name der virtuellen Umgebung, falls das Programm Kaspersky Endpoint Security in einer virtuellen Umgebung installiert ist
- eindeutige Anfrage-ID für die Dienste des Rechteinhabers;
- IDs der Komponenten von Kaspersky Endpoint Security, die zum Zeitpunkt der Datenbereitstellung aktiv sind.

Kaspersky kann diese Informationen auch verwenden, um statistische Informationen über die Verbreitung und Verwendung von Kaspersky-Software zu erstellen.

Wenn Sie einen Aktivierungscode verwenden, stimmen Sie der automatischen Übertragung der oben genannten Daten zu. Wenn Sie es ablehnen, Kaspersky diese Informationen bereitzustellen, muss für die Aktivierung von Kaspersky Endpoint Security eine Schlüsseldatei verwendet werden.

Wenn Sie die Bedingungen des Lizenzvertrags akzeptieren, stimmen Sie der automatischen Weitergabe folgender Informationen zu:

- Beim Update von Kaspersky Endpoint Security:
  - Version von Kaspersky Endpoint Security
  - ID von Kaspersky Endpoint Security

- aktiver Schlüssel;
- einmalige ID für den Start der Update-Aufgabe
- einmalige ID der Installation von Kaspersky Endpoint Security.

- Beim Wechsel mithilfe von Links aus der Benutzeroberfläche von Kaspersky Endpoint Security:
  - Version von Kaspersky Endpoint Security
  - Version des Betriebssystems
  - Aktivierungsdatum von Kaspersky Endpoint Security
  - Ablaufdatum der Lizenz
  - Erstellungsdatum des Schlüssels
  - Installationsdatum von Kaspersky Endpoint Security
  - ID von Kaspersky Endpoint Security
  - ID der gefundenen Schwachstelle des Betriebssystems
  - ID des zuletzt installierten Updates für Kaspersky Endpoint Security
  - Hash der gefundenen Datei, die eine Bedrohung darstellt, und Bezeichnung dieses Objekts nach der Kaspersky-Klassifikation
  - Kategorie des Aktivierungsfehlers für Kaspersky Endpoint Security
  - Code des Aktivierungsfehlers für Kaspersky Endpoint Security
  - Anzahl der Tage bis zum Ablauf des Schlüssels
  - Anzahl der Tage, die seit dem Hinzufügen des Schlüssels vergangen sind
  - Anzahl der Tage, die seit dem Ablauf der Lizenz vergangen sind
  - Anzahl der Computer, auf die sich die aktuelle Lizenz erstreckt
  - aktiver Schlüssel;
  - Gültigkeitsdauer der Lizenz für Kaspersky Endpoint Security
  - aktueller Status der Lizenz
  - Typ der aktuellen Lizenz
  - Typ des Programms
  - einmalige ID für den Start der Update-Aufgabe

- einmalige ID der Installation von Kaspersky Endpoint Security auf dem Computer
- Sprache der Benutzeroberfläche von Kaspersky Endpoint Security

Kaspersky schützt die erhaltenen Informationen in Übereinstimmung mit geltenden gesetzlichen Bestimmungen und mit den aktuellen Richtlinien von Kaspersky. Die Daten werden über verschlüsselte Verbindungskanäle übertragen.

Ausführliche Angaben darüber, wie Informationen über die Programmverwendung empfangen, verarbeitet, gespeichert und gelöscht werden, nachdem der Lizenzvertrag und die Erklärung zu Kaspersky Security Network akzeptiert worden sind, finden Sie in den genannten Dokumenten und auf der Kaspersky-Website. Die Dateien license.txt und ksn_<ID der Sprache>.txt mit den Texten des Endbenutzer-Lizenzvertrags und der Erklärung zu Kaspersky Security Network gehören zum Lieferumfang des Programms.

Datenbereitstellung bei der Verwendung von Kaspersky Security Network

Der Datensatz, den Kaspersky Endpoint Security an Kaspersky sendet, hängt von der Art der Lizenz und den Nutzungseinstellungen des Kaspersky Security Network ab.

Verwendung von KSN unter Lizenz auf nicht mehr als 4 Computern

Wenn Sie die Erklärung zu Kaspersky Security Network akzeptieren, stimmen Sie der automatischen Übertragung folgender Informationen zu:

- Informationen über das Update der KSN-Konfiguration: ID der aktuellen Konfiguration, ID der erhaltenen Konfiguration, Fehlercode des Konfigurations-Updates.
- Informationen über untersuchte Dateien und Webadressen: Prüfsummen der untersuchten Datei (MD5, SHA2-256, SHA1) und der Dateimuster (MD5), Größe des Musters, Typ der gefundenen Bedrohung und Bedrohungsname gemäß der Klassifikation des Rechteinhabers, ID der Antiviren-Datenbanken, Webadresse, für welche die Reputation abgefragt wird, sowie Webadresse der Webseite, von welcher zu der untersuchten Webadresse gewechselt wurde, ID des Verbindungsprotokolls und Nummer des verwendeten Ports;
- ID der Untersuchungsaufgabe, die die Bedrohung entdeckt hat;
- Informationen über verwendete digitale Zertifikate, welche für ihre Authentifizierung erforderlich sind: Prüfsummen (SHA256) des Zertifikats, mit welchem das Untersuchungsobjekt signiert ist, und des öffentlichen Zertifikatschlüssels;
- ID der Software-Komponente, welche die Untersuchung ausführt.
- ID der Antiviren-Datenbanken und der Einträge in den Antiviren-Datenbanken.

- Informationen über die Aktivierung der Software auf dem Computer: signierter Header des Tickets vom Aktivierungsdienst (ID des regionalen Aktivierungszentrums, Prüfsumme des Aktivierungscodes, Prüfsumme des Tickets, Erstellungsdatum des Tickets, Ticketversion, Lizenzstatus, Datum und Uhrzeit für den Beginn und den Ablauf der Ticketgültigkeit, einmalige Lizenz-ID, Lizenzversion), ID des Zertifikats, mit dem der Ticket-Header signiert ist, Prüfsumme (MD5) der Schlüsseldatei;

- Informationen über den Rechteinhaber der Software: Typ und vollständige Programmversion von Kaspersky Endpoint Security, Version des verwendeten Protokolls für die Verbindung mit den Kaspersky-Diensten.

Nutzung von KSN unter Lizenz auf 5 oder mehr Computern

Wenn Sie die Erklärung zu Kaspersky Security Network akzeptieren, stimmen Sie der automatischen Übertragung folgender Informationen zu:

Ist das Kontrollkästchen **Kaspersky Security Network** aktiviert und das Kontrollkästchen **Erweiterten KSN-Modus aktivieren** deaktiviert, so werden die folgenden Informationen übertragen:

- Informationen über das Update der KSN-Konfiguration: ID der aktuellen Konfiguration, ID der erhaltenen Konfiguration, Fehlercode des Konfigurations-Updates.

- Informationen über untersuchte Dateien und Webadressen: Prüfsummen der untersuchten Datei (MD5, SHA2-256, SHA1) und der Dateimuster (MD5), Größe des Musters, Typ der gefundenen Bedrohung und Bedrohungsname gemäß der Klassifikation des Rechteinhabers, ID der Antiviren-Datenbanken, Webadresse, für welche die Reputation abgefragt wird, sowie Webadresse der Webseite, von welcher zu der untersuchten Webadresse gewechselt wurde, ID des Verbindungsprotokolls und Nummer des verwendeten Ports;

- ID der Untersuchungsaufgabe, die die Bedrohung entdeckt hat;

- Informationen über verwendete digitale Zertifikate, welche für ihre Authentifizierung erforderlich sind: Prüfsummen (SHA256) des Zertifikats, mit welchem das Untersuchungsobjekt signiert ist, und des öffentlichen Zertifikatschlüssels;

- ID der Software-Komponente, welche die Untersuchung ausführt.

- ID der Antiviren-Datenbanken und der Einträge in den Antiviren-Datenbanken.

- Informationen über die Aktivierung der Software auf dem Computer: signierter Header des Tickets vom Aktivierungsdienst (ID des regionalen Aktivierungszentrums, Prüfsumme des Aktivierungscodes, Prüfsumme des Tickets, Erstellungsdatum des Tickets, Ticketversion, Lizenzstatus, Datum und Uhrzeit für den Beginn und den Ablauf der Ticketgültigkeit, einmalige Lizenz-ID, Lizenzversion), ID des Zertifikats, mit dem der Ticket-Header signiert ist, Prüfsumme (MD5) der Schlüsseldatei;

- Informationen über den Rechteinhaber der Software: Typ und vollständige Programmversion von Kaspersky Endpoint Security, Version des verwendeten Protokolls für die Verbindung mit den Kaspersky-Diensten.

Sind die Kontrollkästchen **Kaspersky Security Network** und **Erweiterten KSN-Modus aktivieren** aktiviert, so werden zusätzlich zu den oben genannten Informationen auch die folgenden Informationen übertragen:

- Informationen zu den Ergebnissen der Kategorisierung der angeforderten Webressourcen, welche folgende Angaben enthält: untersuchte Webadresse und IP-Adresse des Hosts, Version der Software-Komponente, welche die Kategorisierung ausgeführt hat, Kategorisierungsmethode und Auswahl der Kategorien, welche für diese Webressource ermittelt wurden;

- Informationen über die auf dem Computer installierte Software: Name der Softwareanwendungen und Softwareanbieter, Registrierungsschlüssel und ihre Werte, Informationen über Dateien der installierten Softwarekomponenten (Prüfnummern (MD5, SHA2-256, SHA1), Name, Dateipfad auf dem Computer, Größe, Version und die digitale Signatur).

- Informationen über den Stand des Virenschutzes des Computers: die Versionen und die Versions-Zeitstempel der verwendeten Antiviren-Datenbanken, die ID der Aufgabe und die ID der Software, die die Untersuchung durchführt;

- Informationen über die Dateien, die vom Benutzer heruntergeladen wurden: Webadressen und IP-Adressen, von welchen der Download erfolgt ist, und Webadresse der Seite, von welcher auf die Seite für den Datei-Download gewechselt wurde, ID des Download-Protokolls und Nummer des Verbindungsports, Merkmal für die Schädlichkeit von Adressen; Attribute, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei; Informationen zum Prozess, welcher die Datei heruntergeladen hat (Prüfsummen (MD5, SHA2-256, SHA1), Zeitpunkt (Datum und Uhrzeit) der Erstellung und Verlinkung, Merkmal für das Vorhandensein im Autostart, Attribute, Namen von Packprogrammen, Informationen zur Signatur, Merkmal der ausführbaren Datei, Format-ID, Typ des Benutzerkontos, von welchem der Prozess gestartet wurde), Informationen zur Prozessdatei (Name, Pfad und Größe der Datei), Dateiname, Dateipfad auf dem Computer, digitale Signatur der Datei und Informationen über die Signierung, Webadresse, bei welcher der Fund erfolgte, Nummer des Skripts auf der Webseite, die als verdächtig oder schädlich eingestuft wurde;

- Informationen über gestartete Programme und deren Module: Daten über gestartete Prozesse im System (Prozess-ID im System (PID), Prozessname, Daten über das Benutzerkonto, von dem der Prozess gestartet wurde, Programm und Befehl, welcher den Prozess gestartet hat, Merkmal für die Vertrauenswürdigkeit des Programms oder des Prozesses, vollständiger Pfad der Prozessdateien und Prüfsummen (MD5, SHA2-256, SHA1), Befehlszeile für den Start, Integritätsniveau des Prozesses, Beschreibung des Produkts, zu welchem der Prozess gehört (Name des Produkts und Daten zum Herausgeber), sowie Daten über verwendete digitale Zertifikate und Informationen, die für ihre Authentifizierung erforderlich sind, oder Daten über das Fehlen einer digitalen Signatur für die Datei), sowie Informationen über die Module, welche in Prozesse geladen wurden (Name, Größe, Typ, Erstellungsdatum, Attribute, Prüfsummen (MD5, SHA2-256, SHA1), Pfad), Informationen zur Kopfzeile für PE-Dateien, Name des Packprogramms (falls die Datei gepackt ist);

- Informationen über alle potentiell schädlichen Objekte und Aktionen: Name des erkannten Objekts und vollständiger Pfad des Objekts auf dem Computer, Prüfsummen der verarbeiteten Objekte (MD5, SHA2-256, SHA1), Zeitpunkt (Datum und Uhrzeit) des Fundes; Namen, Größe und Pfade der verarbeiteten Dateien; Code der Pfadvorlage, Merkmal der ausführbaren Datei, Merkmal, ob das Objekt ein Container ist, Name des Packprogramms (falls die Datei gepackt war), Code des Dateityps, ID des Dateiformats, ID der Antiviren-Datenbanken und der Einträge in den Antiviren-Datenbanken, auf deren Basis die Entscheidung der Software getroffen wurde, Merkmal des potentiell schädlichen Objekts, Name der gefundenen Bedrohung gemäß der Klassifikation des Rechteinhabers, Gefahrenstufe, Status und Erkennungsmethode, Grund der Aufnahme in den analysierten Kontext und Ordnungsnummer der Datei im Kontext, Prüfsummen (MD5, SHA2-256, SHA1), Name und Attribute der ausführbaren Datei der Anwendung, über welche die infizierte Nachricht oder der Link eingedrungen ist, IP-Adressen (IPv4 und IPv6) des Hosts des blockierten Objekts, Datei-Entropie, Merkmal für das Vorhandensein der Datei im Autostart, Zeitpunkt (Datum und Uhrzeit) des ersten Fundes der Datei im System, Anzahl der Dateistarts seit dem letzten Senden einer Statistik, Compiler-Typ; Informationen über den Namen, die Prüfsummen (MD5, SHA2-256, SHA1) und die Größe des Mail-Clients, über welchen das schädliche Objekt empfangen wurde; ID der Software-Aufgabe, welche die Untersuchung ausgeführt hat; Merkmal für die Überprüfung der Reputation oder der Signatur der Datei, Ergebnis der Dateiverarbeitung, Prüfsumme (MD5) des für das Objekt erfasste Muster, Größe des Musters (in Bytes), technische Eigenschaften der eingesetzten Erkennungstechnologien;

- Informationen über untersuchte Objekte: zugewiesene Sicherheitsgruppe, in welche und/oder aus welcher die Datei verschoben wurde, Grund, aus welchem die Datei in diese Kategorie verschoben wurde, ID der Kategorie, Informationen über die Quelle der Kategorien und Version der Datenbank der Kategorien, Merkmal für das Vorhandensein eines vertrauenswürdigen Zertifikats der Datei, Name des Dateiherstellers, Dateiversion, Name und Version des Programms, zu welcher die Datei gehört;

- Informationen über gefundene Schwachstellen: ID der Schwachstelle in der Datenbank für Schwachstellen, Gefahrenklasse der Schwachstelle.

- Informationen über die Ausführung einer Emulation der ausführbaren Datei: Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei, Version der Emulationskomponente, Emulationstiefe, Vektor der Merkmale für logische Blöcke und Funktionen innerhalb logischer Blöcke, welche im Verlauf der Emulation erhalten wurden, Daten aus der Struktur der PE-Kopfzeile der ausführbaren Datei;

- IP-Adressen des angreifenden Computers (IPv4 und IPv6), Portnummer auf dem Computer, auf welchen der Netzwerkangriff gerichtet war, ID des Protokolls des IP-Pakets, das den Angriff enthielt, Angriffsziel (Name des Unternehmens, Website), Flag für die Reaktion auf den Angriff, Gewichtung des Angriffs, Vertrauensebene;

- Informationen über Angriffe, welche mit dem Spoofing von Netzwerkressourcen verbunden waren, DNS- und IP-Adressen (IPv4 oder IPv6) der besuchten Websites.

- DNS- und IP-Adressen (IPv4 oder IPv6) der angefragten Web-Ressource, Informationen über die Datei und den Web-Client, der auf die Web-Ressource zugreift, Name, Größe, Prüfsummen (MD5, SHA2-256, SHA1) der Datei, vollständiger Pfad der Datei und der Vorlagencode des Dateipfads, das Ergebnis der Überprüfung der digitalen Signatur und deren Status im KSN.

- Informationen über die Ausführung eines Rollbacks der Aktionen von Schadsoftware: Daten über die Datei, deren Aktivität rückgängig gemacht wurde (Name, vollständiger Pfad, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Datei), Daten über erfolgreiche und erfolglose Aktionen zur Löschung, Umbenennung und zum Kopieren von Dateien und zur Wiederherstellung von Registrierungswerten (Namen und Werte der Registrierungsschlüssel), Informationen über Systemdateien, welche von der Schadsoftware verändert wurden, vor und nach der Ausführung des Rollbacks.

- Informationen über die Ausnahmen, die für adaptive Abweichkontrollkomponente festgelegt sind: die ID und der Status der Regel, die ausgelöst wurde, die von der Software ausgeführte Aktion, wenn die Regel ausgelöst wurde, der Typ des Benutzerkontos, unter welchem der Prozess oder Thread verdächtige Aktivitäten durchführt, sowie über den Prozess, der Gegenstand von verdächtigen Aktivitäten war (Skript-ID oder Name der Prozessdatei, vollständiger Pfad zur Prozessdatei, Vorlagencode des Dateipfads, Prüfsummen (MD5, SHA2-256, SHA1) der Prozessdatei); Informationen über das Objekt, das die verdächtigen Aktionen ausgeführt hat sowie über das Objekt, das Gegenstand von verdächtigen Aktionen war (Name des Registrierschlüssels oder Dateiname, vollständiger Pfad zur Datei, Vorlagencode des Dateipfads und die Prüfsummen (MD5, SHA2-256, SHA1) der Datei).

- Informationen über geladene Software-Module: Name, Größe und Prüfsummen (MD5, SHA2-256, SHA1) der Moduldatei, vollständiger Pfad und Code der Pfadvorlage für die Datei, Parameter der digitalen Signatur der Moduldatei, Zeitpunkt (Datum und Uhrzeit) der Erstellung der Signatur, Name des Subjekts und Organisation, welche die Moduldatei signiert hat, ID des Prozesses, in welchen das Modul geladen wurde, Name des Modulherstellers, Ordnungsnummer des Moduls in der Ladeabfolge.

- Informationen über die Qualität der Softwareinteraktion mit den KSN-Diensten: Datum und Uhrzeit von Beginn und Ende der Periode, in der die Statistiken erzeugt wurden, Informationen über die Qualität der Anfragen und der Verbindung zu den einzelnen verwendeten KSN-Diensten (KSN-Dienstkennung, Anzahl der erfolgreichen Anfragen, Anzahl der Anfragen mit Antworten vom Cache, Anzahl nicht erfolgreicher Anfragen (Netzwerkprobleme, KSN wurde in den Softwareeinstellungen deaktiviert, fehlerhaftes Routing), verbrauchte Zeit der erfolgreichen Anfragen, verbrauchte Zeit der abgebrochenen Anfragen, verbrauchte Zeit der Anfragen mit überschrittener Zeit, Anzahl der Verbindungen zum KSN aus dem Cache, Anzahl der erfolgreichen Verbindungen zum KSN, Anzahl der nicht erfolgreichen Verbindungen zum KSN, Anzahl der erfolgreichen Transaktionen, Anzahl der nicht erfolgreichen Transaktionen, verbrauchte Zeit der erfolgreichen Verbindungen zum KSN, verbrauchte Zeit der nicht erfolgreichen Verbindungen zum KSN, verbrauchte Zeit der erfolgreichen Transaktionen, verbrauchte Zeit der nicht erfolgreichen Transaktionen).

- Wird ein potentiell schädliches Objekt erkannt, werden Informationen über die Daten im Prozessspeicher zur Verfügung gestellt: Elemente der Objekthierarchie des Systems (ObjectManager), Daten im UEFI-BIOS-Speicher sowie Namen von Registrierschlüsseln und deren Werte;

- Informationen über Ereignisse in Systemprotokollen: Ereigniszeitpunkt, Name des Protokolls, in welchem das Ereignis gefunden wurde, Typ und Kategorie des Ereignisses, Name und Beschreibung der Ereignisquelle;

- Informationen über Netzwerkverbindungen: Version und Prüfsummen (MD5, SHA2-256, SHA1) der Prozessdatei, des geöffneten Ports, Pfad und digitale Signatur der Prozessdatei, lokale und Remote-IP-Adresse, Nummern des lokalen und des Remote-Verbindungsports, Verbindungszustand, Dauer, für welche der Port geöffnet war;

- Informationen über das Datum der Softwareinstallation und -aktivierung auf dem Computer: die ID des Partners, der die Lizenz verkauft hat, die Seriennummer der Lizenz, der signierte Header des Tickets vom Aktivierungsdienst (die ID eines regionalen Aktivierungszentrums, die Prüfsumme des Aktivierungscodes, die Prüfsumme des Tickets, das Erstellungsdatum des Tickets, die eindeutige ID des Tickets, die Ticketversion, der Lizenzstatus, das Datum und die Uhrzeit des Ticketbeginns und -endes, die eindeutige ID der Lizenz, die Lizenzversion), die ID des Zertifikats, das zum Signieren des Ticketheaders verwendet wurde, die Prüfsumme (MD5) der Schlüsseldatei, die eindeutige ID der Softwareinstallation auf dem Computer, der Typ und die ID des Programms, die aktualisiert wird, die ID der Update-Aufgabe;

- Informationen über die Zusammensetzung aller installierten Updates sowie über die Zusammensetzung der zuletzt installierten und/oder gelöschten Updates, Typ des Ereignisses, aufgrund dessen Informationen über Updates gesendet wurden, Zeitraum, welcher seit der Installation des letzten Updates vergangen ist, Informationen über die Antiviren-Datenbanken, die zum Zeitpunkt der Datenbereitstellung geladen waren.

- Informationen über die Verwendung der Software auf dem Computer: Daten über die Prozessornutzung (CPU), Daten über die Nutzung des Arbeitsspeichers (Private Bytes, Non-Paged Pool, Paged Pool), Anzahl der aktiven Ströme im Software-Prozess und der Ströme im Wartezustand, Arbeitsdauer der Software bis zum Auftreten des Fehlers, Merkmal für die Verwendung der Software im interaktiven Modus.

- Anzahl der Software-Dumps und der System-Dumps (BSOD) ab dem Zeitpunkt der Software-Installation und ab dem Zeitpunkt des letzten Updates, ID und Version des Software-Moduls, in welchem die Störung aufgetreten ist, Speicherstapel im Produktprozess und Informationen über die Antiviren-Datenbanken zum Zeitpunkt der Störung;

- Daten zum System-Dump (BSOD): Merkmal für das Auftreten des BSOD auf dem Computer, Name des Treibers, welcher den BSOD hervorgerufen hat, Adresse und Speicherstapel im Treiber, Merkmal für die Dauer der Sitzung des Betriebssystems bis zum Auftreten des BSOD, Speicherstapel des Treiberabsturzes, Typ des gespeicherten Arbeitsspeicher-Dumps, Merkmal für die Tatsache, dass die Sitzung des Betriebssystems bis zum BSOD länger als 10 Minuten gedauert hat, einmalige Dump-ID, Zeitpunkt (Datum und Uhrzeit), zu welchem der BSOD aufgetreten ist.

- Informationen über Fehler oder Leistungsprobleme, die bei der Ausführung von Softwarekomponenten aufgetreten sind: Status-ID der Software, Typ, Code und Zeitpunkt des auftretenden Fehlers, IDs der Komponente, des Moduls und des Produktprozesses, in welchem der Fehler aufgetreten ist, ID der Aufgabe oder der Update-Kategorie, in welcher der Fehler aufgetreten ist, Protokolle der von der Software verwendeten Treiber (Fehlercode, Modulname, Name der Quelldatei und Zeile, in welcher der Fehler aufgetreten ist).

- Informationen über die Updates der Antiviren-Datenbanken und der Software-Komponenten: Name, Datum und Uhrzeit der Indexdateien, die beim letzten Update heruntergeladen wurden und beim laufenden Update heruntergeladen werden;

- Informationen über die Abstürze der Software: Erstellungszeitpunkt (Datum und Uhrzeit) und Typ des Dumps, Typ des Ereignisses, welches den Absturz der Software verursacht hat (unerwarteter Stromausfall, Absturz einer Dritthersteller-Anwendung), Zeitpunkt (Datum und Uhrzeit) des unerwarteten Stromausfalls.

- Informationen über die Kompatibilität der Treiber der Software mit der Hard- und Software: Informationen über die Betriebssystemeigenschaften, welche die Funktionalität der Softwarekomponenten beschränken (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), Typ der integrierten Boot-Software (UEFI, BIOS), Merkmal für das Vorhandensein eines Trusted Platform Module (TPM), Version der TPM-Spezifikation, Informationen über den auf dem Computer installierten Hauptprozessor (CPU), Modus und Einstellungen für Code Integrity und Device Guard, Modus der Treiber und Verwendungsgrund für den aktuellen Modus, Version der Treiber der Software, Status der Unterstützung von Treibern für die Soft- und Hardware-Virtualisierung des Computers.

- Informationen über Drittanbieterprogramm, welche einen Fehler verursacht haben: Name, Version und Sprachversion, Fehlercode und Informationen über den Fehler aus dem Systemprotokoll der Programme, Adresse und Speicherstapel für das Auftreten des Fehlers einer Drittanbieterprogramm, Merkmal für das Auftreten des Fehlers in einer Software-Komponente, Arbeitsdauer der Drittanbieterprogramm bis zum Auftreten des Fehlers, Prüfsummen (MD5, SHA2-256, SHA1) des Prozessmusters des Programms, in welcher der Fehler aufgetreten ist, Pfad dieses Prozessmusters des Programms und Code der Pfadvorlage, Informationen aus dem Systemprotokoll des Betriebssystems mit einer Beschreibung des Fehlers, welcher mit dem Programm verbunden war, Informationen über das Programm-Modul, in welchem der Fehler aufgetreten ist (Fehler-ID, Fehleradresse als Offset im Modul, Name und Version des Moduls, ID für den Absturz des Programms in einem Plug-in des Rechteinhabers und Speicherstapel für diesen Absturz, Arbeitsdauer des Programms bis zum Absturz);

- Version der Update-Komponente der Software, Anzahl der Abstürze der Update-Komponente der Software bei der Ausführung von Update-Aufgaben im Rahmen der Komponentenausführung, ID des Typs der Update-Aufgabe, Anzahl der Fehler bei den Update-Aufgaben der Update-Komponente der Software.

- Informationen über die Ausführung von Überwachungskomponenten des Softwaresystems: vollständige Versionen der Komponenten, Datum und Uhrzeit, wann die Komponenten gestartet wurden, Code des Ereignisses, das zum Überlaufen der Warteschlange für Ereignisse geführt hat, und Anzahl solcher Ereignisse, Gesamtzahl der Warteschlangenüberlaufe, Informationen über die Datei des Prozesses, der das Ereignis ausgelöst hat (Name und Pfad der Datei auf dem Computer, Vorlagencode des Dateipfads, Prüfsummen (MD5, SHA2-256, SHA1) des mit der Datei verbundenen Prozesses, Dateiversion), ID des Abfangvorgangs, vollständige Version des Abfangfilters, ID für den Typ des abgefangenen Ereignisses, Größe der Ereigniswarteschlange, und Anzahl der Ereignisse zwischen dem ersten Ereignis in der Warteschlange und dem aktuellen Ereignis, Anzahl überfälliger Ereignisse in der Warteschlange, Informationen über die Datei des Prozesses, der das aktuelle Ereignis ausgelöst hat (Name und Pfad der Datei auf dem Computer, Vorlagencode des Dateipfads, Prüfsummen (MD5, SHA2-256, SHA1) des mit der Datei verbundenen Prozesses), Dauer der Ereignisverarbeitung, Höchstdauer der Ereignisverarbeitung, Wahrscheinlichkeit für das Senden von Statistiken, Informationen über Ereignisse des Betriebssystems, für die die Verarbeitungszeit überschritten wurde (Datum und Uhrzeit des Ereignisses, Anzahl der wiederholten Initialisierungen der Antiviren-Datenbanken, Datum und Uhrzeit der letzten, wiederholten Initialisierung der Antiviren-Datenbanken nach ihrem Update, Verzögerungszeit der Verarbeitung eines Ereignisses für jede Systemüberwachungskomponente, Anzahl der Ereignisse in der Warteschlange, Anzahl der verarbeiteten Ereignisse, Anzahl der verzögerten Ereignisse des aktuellen Typs, Gesamtverzögerungszeit der Ereignisse des aktuellen Typs, Gesamtverzögerungszeit aller Ereignisse).

- Informationen von dem Windows-Tool zur Ereignisprotokollierung (Event Tracing for Windows, ETW) bei Problemen mit der Leistung der Software, Ereignisanbieter SysConfig / SysConfigEx / WinSATAssessment von Microsoft: Daten über den Computer (Modell, Hersteller, Formfaktor des Gehäuses, Version), Daten über die Windows-Leistungsindikatoren (WinSAT-Bewertungsdaten, Windows-Leistungsindex), Name der Domäne, Daten über die physischen und logischen Prozessoren (Anzahl der physischen und logischen Prozessoren, Hersteller, Modell, Stepping, Anzahl der Kerne, Taktfrequenz, Prozessor-ID (CPUID), Cache-Eigenschaften, Eigenschaften des logischen Prozessors, Merkmale für die Unterstützung der Modi und Anweisungen), Daten über die Module des Arbeitsspeichers (Typ, Formfaktor, Hersteller, Modell, Größe, Granularität der Speicherbelegung), Daten über Netzwerkschnittstellen (IP- und MAC-Adressen, Name, Beschreibung, Konfiguration der Netzwerkschnittstellen, Verteilung der Anzahl und der Größe von Netzwerkpaketen nach Typen, Geschwindigkeit des Netzwerkaustauschs, Verteilung der Anzahl der Netzwerkfehler nach Typen), Konfiguration des IDE-Controllers, IP-Adresse der DNS-Server, Daten über die Grafikkarte (Modell, Beschreibung, Hersteller, Kompatibilität, Größe des Grafikspeichers, Bildschirmauflösung, Anzahl der Bits pro Pixel, BIOS-Version), Daten über verbundene Plug-and-Play-Geräte(Name, Beschreibung, Geräte-ID [PnP, ACPI], Daten über Laufwerke und Speichergeräte (Anzahl der Laufwerke oder Flash-Laufwerke, Hersteller, Modell, Größe des Laufwerks, Anzahl der Zylinder, Anzahl der Spuren pro Zylinder, Anzahl der Sektoren pro Spur, Größe des Sektors, Cache-Eigenschaften, Ordnungszahl, Partitionsanzahl, Konfiguration des SCSI-Controllers), Daten über die logischen Laufwerke (Ordnungszahl, Größe der Partition, Volume-Größe, Volume-Buchstabe, Typ der Partition, Typ des Dateisystems, Anzahl der Cluster, Cluster-Größe, Anzahl der Sektoren pro Cluster, Anzahl der belegten und freien Cluster, Boot-Volume-Buchstabe, Adresse-Abweichung der Partition bezüglich des Anfangs des Laufwerks), Daten über das BIOS der Hauptplatine (Hersteller, Veröffentlichungsdatum, Version), Daten über die Hauptplatine (Hersteller, Modell, Typ), Daten über den physischen Speicher (gesamter und freier Platz), Daten über die Dienste des Betriebssystems (Name, Beschreibung, Status, Tag, Daten über Prozesse [Name und PID-ID]), Energieoptionen des Computers, Konfiguration des Interrupt Controllers, Pfade der Windows-Systemordner (Windows und System32), Daten über das Betriebssystem (Version, Build, Veröffentlichungsdatum, Name, Typ, Installationsdatum), Größe der Auslagerungsdatei, Daten über die Monitore (Anzahl, Hersteller, Bildschirmauflösung, Auflösungsvermögen, Typ), Daten über den Treiber der Grafikkarte (Hersteller, Veröffentlichungsdatum, Version).

- Informationen von ETW, Anbieter von EventTrace/EventMetadata-Ereignissen von Microsoft: Informationen über die Abfolge von Systemereignissen (Typ, Uhrzeit, Datum, Zeitzone), Metadaten über die Datei mit Ablaufverfolgungsergebnissen (Name, Struktur, Ablaufverfolgungseinstellungen, Aufgliederung der Anzahl von Ablaufverfolgungsvorgängen nach Typ), Informationen über das Betriebssystem (Name, Typ, Version, Build, Veröffentlichungsdatum, Startzeit);

- Informationen von ETW, Bereitstellung von Process/Microsoft Windows Kernel Process/Microsoft Windows Kernel Processor Power Ereignisse von Microsoft: Informationen über gestartete und abgeschlossene Prozesse (Name, PID, Startparameter, Befehlszeile, Rückgabecode, Energieverwaltungsparameter, Start- und Fertigstellungszeit, Typ des Zugriffstoken, SID, SessionID, Anzahl der installierten Deskriptoren), Informationen über Änderungen der Thread-Prioritäten (TID, Priorität, Uhrzeit), Informationen über Laufwerkoperationen des Prozesses (Typ, Uhrzeit, Kapazität, Anzahl), Verlauf der Änderungen der Struktur und Kapazität der nutzbaren Speicherprozesse.

- Informationen von ETW, Bereitstellung von StackWalk/Perfinfo Ereignissen von Microsoft: Informationen über Leistungsindikatoren (Leistung von einzelnen Codeabschnitten, Sequenz von Funktionsaufrufen, PID, TID, Adressen und Attribute von ISRs und DPCs).

- Informationen von ETW, Bereitstellung von KernelTraceControl-ImageID Ereignissen von Microsoft: Informationen über ausführbare Dateien und dynamische Bibliotheken (Name, Bildgröße, vollständiger Pfad), Informationen zu PDB-Dateien (Name, ID), VERSIONINFO Ressourcendaten für ausführbare Dateien (Name, Beschreibung, Ersteller, Ort, Programmversion und -ID, Dateiversion und -ID);

- Informationen von ETW, Bereitstellung von FileIo/DiskIo/Image/Windows Kernel Disk Ereignissen von Windows: Informationen zu Datei- und Laufwerkoperationen (Typ, Kapazität, Startzeit, Fertigstellungszeit, Dauer, Status der Fertigstellung, PID, TID, Funktionsaufrufadressen des Treibers, E/A-Anfragepaket (IRP), Windows-Dateiobjektattribute), Informationen über Dateien, die in Datei- und Laufwerkoperationen involviert sind (Name, Version, Größe, vollständiger Pfad, Attribute, Offset, Prüfsumme des Bildes, Optionen für das Öffnen und Zugreifen).

- Informationen von ETW, Bereitstellung von PageFault Ereignissen von Microsoft: Informationen über Zugriffsfehler der Speicherseiten (Adresse, Uhrzeit, Kapazität, PID, TID, Attribute von Windows-Dateiobjekten, Parameter der Speicherzuordnung).

- Informationen von ETW, Bereitstellung von Thread Ereignissen von Microsoft: Informationen über Thread-Erstellung/-Fertigstellung, Informationen gestartete Threads (PID, TID, Größe des Stacks, Prioritäten und Zuordnungen von CPU-Ressourcen, E/A-Ressourcen, Speicherseiten zwischen Threads, Stack-Adresse, Adresse der Initialisierungsfunktion, Adresse des Thread Environment Block (TEB), Windows Service-Tag).

- Informationen von ETW, Bereitstellung von Microsoft Windows Kernel Memory Ereignissen von Microsoft: Informationen über Speicherverwaltungsoperationen (Status der Fertigstellung, Uhrzeit, Anzahl, PID), Struktur der Speicherzuordnung (Typ, Kapazität, SessionID, PID).

- Informationen zu Softwareoperationen im Falle von Leistungsproblemen: ID der Softwareinstallation, Typ und Wert des Leistungsabfalls, Informationen über die Sequenz von Ereignissen innerhalb der Software (Uhrzeit, Zeitzone, Typ, Status der Fertigstellung, ID der Softwarekomponenten, ID des Softwareoperationsszenarios, TID, PID, Funktionsaufrufadressen), Informationen zu den zu überprüfenden Netzwerkverbindungen (URL, Richtung der Verbindung, Größe des Netzwerkpakets), Informationen zu PDB-Dateien (Name, ID, Bildgröße der ausführbaren Datei), Informationen über zu prüfende Dateien (Name, vollständiger Pfad, Prüfsumme), Überwachungsparameter der Softwareleistung.

- Informationen über den letzten fehlgeschlagenen Neustart des Betriebssystems: Anzahl der fehlgeschlagenen Neustarts seit der Installation des Betriebssystems, Daten zum System-Dump (Code und Parameter des Fehlers, Name, Version und Prüfsumme (CRC32) des Moduls, welches den Fehler bei der Arbeit des Betriebssystem hervorgerufen hat, Fehleradresse als Offset im Modul, Prüfsummen (MD5, SHA2-256, SHA1) des System-Dumps).

- Informationen für die Authentizitätsprüfung der Zertifikate, mit welchen die Dateien signiert sind: Fingerabdruck des Zertifikats, Algorithmus zur Berechnung der Prüfsumme, öffentlicher Schlüssel und Seriennummer des Zertifikats, Name des Zertifikatausstellers, Ergebnis der Zertifikatuntersuchung und ID der Zertifikatdatenbank;

- Informationen zum Prozess, welcher einen Angriff auf den Selbstschutz der Software ausgeführt hat: Name, Größe, Prüfsummen (MD5, SHA2-256, SHA1), vollständiger Pfad und Code der Pfadvorlage der Prozessdatei, Zeitpunkt (Datum und Uhrzeit) der Erstellung und Verlinkung der Prozessdatei, Merkmal der ausführbaren Datei, Attribute der Prozessdatei, Informationen zum Zertifikat, mit welchem die Prozessdatei signiert ist, Code des Benutzerkontos, in deren Namen der Prozess gestartet wurde, ID der Vorgänge, welche für den Zugriff auf den Prozess ausgeführt wurden, Typ der Ressourcen, von welchen der Vorgang ausgeführt wurde (Prozess, Datei, Registrierungsobjekt, Suche des Fensters mithilfe der Funktion FindWindow), Name der Ressource, mit welcher der Vorgang ausgeführt wird, Merkmal für die erfolgreiche Ausführung des Vorgangs, Status der Prozessdatei und ihr Status in KSN;

- Informationen über die Software des Rechteinhabers: Vollversion, Typ, Lokalisierung und Betriebszustand der verwendeten Software, Versionen der installierten Software-Komponenten und deren Betriebszustand, Informationen über die installierten Software-Updates, den Wert des TARGET-Filters, die Version des für die Verbindung zu den Diensten des Rechteinhabers verwendeten Protokolls;

- Informationen über die Hardware, welche auf dem Computer installiert ist: Typ, Name, Modell, Firmware-Version, Merkmale von integrierten und verbundenen Geräten, einmalige ID des Computers, auf welchem die Software installiert ist.

- Informationen über die Versionen des Betriebssystems und der installierten Updates, Bit-Version, Edition und Einstellungen für den Ausführungsmodus des Betriebssystems, Version und Prüfsummen (MD5, SHA2-256, SHA1) der Kernel-Datei des Betriebssystems und Datum und Uhrzeit, an dem das Betriebssystem gestartet wurde;

- Ausführbare und nicht ausführbare Dateien, entweder ganz oder teilweise;

- Abschnitte aus dem Arbeitsspeicher des Computers;
- Sektoren, die am Ladeprozess des Betriebssystems beteiligt sind
- Datenpakete des Netzwerkverkehrs
- Webseiten und E-Mail-Nachrichten, die verdächtige und schädliche Objekte enthalten
- Beschreibung der Klassen und Exemplarklassen des WMI-Speichers
- Berichte über Aktivitäten der Programme:
  - Name, Größe und Version der gesendeten Datei, ihre Beschreibung und Prüfsummen (MD5, SHA2-256, SHA1), Kennung des Dateiformats, Name des Anbieters der Datei, Name des Produkts, zu dem die Datei gehört, vollständiger Pfad zu der Datei auf dem Computer, Vorlagencode des Pfads, Erstellungs- und Änderungszeitstempel der Datei;
  - Anfangs- und Enddatum/-zeit der Gültigkeitsdauer des Zertifikats (wenn die Datei eine digitale Signatur aufweist), Datum und Uhrzeit der Signatur, Name des Ausstellers des Zertifikats, Informationen über den Zertifikatsinhaber, Fingerabdruck, öffentlicher Schlüssel des Zertifikats und entsprechende Algorithmen sowie Seriennummer des Zertifikats;
  - Name des Kontos, von dem aus der Prozess ausgeführt wird;
  - Prüfsummen (MD5, SHA2-256, SHA1) des Namens des Computers, auf dem der Prozess läuft;
  - Titel der Prozessfenster;
  - ID der Antiviren-Datenbanken, Name der erkannten Bedrohung gemäß der Klassifizierung des Rechteinhabers;
  - Daten über die installierte Lizenz, deren ID, Typ und Ablaufdatum;
  - Ortszeit des Computers zum Zeitpunkt der Informationsbereitstellung;
  - Name und Pfade der Dateien, auf die der Prozess zugegriffen hat;
  - Name der Registrierungsschlüssel und ihrer Werte, auf die der Prozess zugegriffen hat;
  - URL und IP-Adressen, auf die durch den Prozess zugegriffen wurde;
  - URL und IP-Adressen, von denen die laufende Datei heruntergeladen wurde.

Bereitstellung von Daten beim Einsatz der Lösungen von Detection and Response

Auf Computern, auf denen Kaspersky Endpoint Security installiert ist, werden die Daten gespeichert, die zum automatischen Versand an die Server von Kaspersky Endpoint Detection and Response, Kaspersky Sandbox and Kaspersky Anti Targeted Attack Platform vorbereitet wurden. Die Dateien werden auf den Computern in einfacher, unverschlüsselter Form gespeichert.

Der spezifische Datensatz hängt von der Lösung ab, in der Kaspersky Endpoint Security verwendet wird.

Kaspersky Endpoint Detection and Response

Alle Daten, die von der App lokal auf dem Computer gespeichert werden, werden bei der Deinstallation von Kaspersky Endpoint Security vom Computer gelöscht.

Daten, die aufgrund der Ausführung der Aufgabe IOC-Untersuchung (Standardaufgabe) empfangen werden

Kaspersky Endpoint Security übermittelt automatisch Daten über die Ausführungsergebnisse der Aufgabe *IOC-Untersuchung* an Kaspersky Security Center.

Die Daten in den Ausführungsergebnissen der Aufgabe *IOC-Untersuchung* können die folgenden Informationen enthalten:

- IP-Adresse aus der ARP-Tabelle
- Physikalische Adresse aus der ARP-Tabelle
- Typ und Name des DNS-Eintrags
- IP-Adresse des geschützten Computers
- Physikalische Adresse (MAC-Adresse) des geschützten Computers
- ID im Ereignisprotokolleintrag
- Name der Datenquelle im Protokoll
- Protokollname
- Ereigniszeitpunkt
- MD5- und SHA256-Hashwerte der Datei
- Vollständiger Name der Datei (einschließlich Pfad)
- Dateigröße
- Remote-IP-Adresse und Port, mit denen während der Untersuchung eine Verbindung hergestellt wurde
- Lokale IP-Adresse des Adapters
- Port, der auf dem lokalen Adapter geöffnet ist
- Protokoll als Zahl (gemäß IANA-Standard)
- Prozessname
- Prozess-Argumente

- Pfad der Prozessdatei
- Windows-ID (PID) des Prozesses
- Windows-ID (PID) des übergeordneten Prozesses
- Benutzerkonto, das den Prozess gestartet hat
- Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
- Dienstname
- Dienstbeschreibung
- Pfad und Name des DLL-Dienstes (für svchost)
- Pfad und Name der ausführbaren Dienstdatei
- Windows-ID (PID) des Dienstes
- Diensttyp (z. B. ein Kerneltreiber oder Adapter)
- Dienststatus
- Startmodus des Dienstes
- Name des Benutzerkontos.
- Volume-Name
- Volume-Buchstabe
- Volume-Typ
- Windows-Systemregistrierungswert
- Registrierungstrukturwert
- Registrierungsschlüsselpfad (ohne Struktur- und Wertname)
- Registrierungseinstellung
- System (Umgebung)
- Name und Version des auf dem Computer installierten Betriebssystems
- Netzwerkname des geschützten Computers
- Domäne oder Gruppe, zu welcher der geschützte Computer gehört
- Browsername
- Browserversion
- Zeitpunkt des letzten Zugriffs auf die Webressource

- URL aus der HTTP-Anforderung
- Name des Benutzerkontos, das für die HTTP-Anforderung verwendet wurde
- Dateiname des Prozesses, der die HTTP-Anforderung gestellt hat
- Vollständiger Pfad der Datei des Prozesses, der die HTTP-Anforderung gestellt hat
- Windows-ID (PID) des Prozesses, der die HTTP-Anforderung gestellt hat
- HTTP-Referenz (Quell-URL der HTTP-Anforderung)
- URI der über HTTP angeforderten Ressource
- Informationen über den HTTP-Benutzeragenten (die Anwendung, die die HTTP-Anforderung gestellt hat)
- Ausführungszeit der HTTP-Anforderung
- Eindeutige ID des Prozesses, der die HTTP-Abfrage gestellt hat

Daten zum Erstellen einer Bedrohungsentwicklungskette

Daten zum Erstellen einer Bedrohungsentwicklungskette werden standardmäßig sieben Tage lang gespeichert. Die Daten werden automatisch an Kaspersky Security Center gesendet.

Daten zum Erstellen einer Bedrohungsentwicklungskette können die folgenden Informationen enthalten:

- Datum und Uhrzeit des Vorfalls
- Erkennungsname
- Untersuchungsmodus
- Status der letzten Aktion im Zusammenhang mit der Erkennung
- Grund, aus dem die Erkennungsverarbeitung fehlgeschlagen ist
- Typ des erkannten Objekts
- Name des erkannten Objekts
- Bedrohungsstatus, nachdem das Objekt verarbeitet wurde
- Grund, aus dem die Ausführung von Aktionen für das Objekt fehlgeschlagen ist
- Aktionen, die ausgeführt wurden, um schädliche Aktionen rückgängig zu machen
- Informationen zum verarbeiteten Objekt:
  - Eindeutige ID des Prozesses
  - Eindeutige ID des übergeordneten Prozesses

- Eindeutige ID der Prozessdatei
- Windows-Prozess-ID (PID)
- Prozess-Befehlszeile
- Benutzerkonto, das den Prozess gestartet hat
- Code der Anmeldesitzung, in der der Prozess ausgeführt wird
- Typ der Sitzung, in der der Prozess ausgeführt wird
- Integritätsstufe des zu verarbeitenden Prozesses
- Mitgliedschaft des Benutzerkontos, das den Prozess gestartet hat, in den privilegierten lokalen und Domänengruppen
- ID des verarbeiteten Objekts
- Vollständiger Name des verarbeiteten Objekts
- ID des geschützten Geräts
- Vollständiger Name des Objekts (lokaler Dateiname oder Webadresse der heruntergeladenen Datei)
- MD5- oder SHA256-Hashwerte des verarbeiteten Objekts
- Typ des verarbeiteten Objekts
- Erstellungsdatum des verarbeiteten Objekts
- Datum der letzten Änderung des verarbeiteten Objekts
- Größe des verarbeiteten Objekts
- Attribute des verarbeiteten Objekts
- Unternehmen, das das verarbeitete Objekt signiert hat
- Ergebnis der Verifizierung des digitalen Zertifikats des verarbeiteten Objekts
- Sicherheits-ID (SID) des verarbeiteten Objekts
- Zeitzonen-ID des verarbeiteten Objekts
- Webadresse des verarbeiteten Objekt-Downloads (nur bei Dateien auf einem Datenträger)
- Name der Anwendung, die die Datei heruntergeladen hat
- MD5- und SHA256-Hashwerte der Anwendung, die die Datei heruntergeladen hat
- Name der Anwendung, die die Datei zuletzt geändert hat
- MD5- und SHA256-Hashwerte der Anwendung, die die Datei zuletzt geändert hat

- Anzahl der verarbeiteten Objektstarts
- Datum und Uhrzeit des ersten Starts des verarbeiteten Objekts
- Eindeutige IDs der Datei
- Vollständiger Name der Datei (lokaler Dateiname oder Webadresse der heruntergeladenen Datei)
- Pfad der verarbeiteten Windows-Registrierungsvariable
- Name der verarbeiteten Windows-Registrierungsvariable
- Wert der verarbeiteten Windows-Registrierungsvariable
- Typ der verarbeiteten Windows-Registrierungsvariable
- Indikator für die Mitgliedschaft des verarbeiteten Registrierungsschlüssels im AutoAusführen-Punkt
- Webadresse der verarbeiteten Webanfrage
- Quelle des Links der verarbeiteten Webanfrage
- Benutzer-Agent der verarbeiteten Webanfrage
- Art der verarbeiteten Web-Anfrage (`GET` oder `POST`)
- Lokaler IP-Port der verarbeiteten Webanfrage
- Remote-IP-Port der verarbeiteten Webanfrage
- Verbindungsrichtung (eingehend oder ausgehend) der verarbeiteten Webanfrage
- ID des Prozesses, in den der Schadcode eingebettet war

Kaspersky Sandbox

Alle Daten, die von der App lokal auf dem Computer gespeichert werden, werden bei der Deinstallation von Kaspersky Endpoint Security vom Computer gelöscht.

Dienstdaten

Kaspersky Endpoint Security speichert die folgenden Daten, die im Rahmen der automatischen Antwort verarbeitet werden:

- Verarbeitete Dateien und Daten, die vom Benutzer während der Konfiguration des integrierten Agenten von Kaspersky Endpoint Security eingegeben wurden:
  - Dateien in Quarantäne
  - Öffentlicher Schlüssel des Zertifikats, das für die Integration mit Kaspersky Sandbox verwendet wird

- Cache des integrierten Agenten von Kaspersky Endpoint Security:
  - Zeitpunkt, zu dem Untersuchungsergebnisse in den Cache geschrieben wurden
  - MD5-Hash der Untersuchungsaufgabe
  - ID der Untersuchungsaufgabe
  - Untersuchungsergebnis für das Objekt
- Warteschlange der Anfragen zur Objektuntersuchung:
  - ID des Objekts in der Warteschlange
  - Zeitpunkt, zu dem das Objekt in die Warteschlange gestellt wurde
  - Verarbeitungsstatus des Objekts in der Warteschlange
  - ID der Benutzersitzung im Betriebssystem, in der die Objektuntersuchungsaufgabe erstellt wurde
  - System-ID (SID) des Betriebssystembenutzers, dessen Benutzerkonto zum Erstellen der Aufgabe verwendet wurde
  - MD5-Hash der Objektuntersuchungsaufgabe
- Informationen zu den Aufgaben, für die der integrierte Agent von Kaspersky Endpoint Security auf Untersuchungsergebnisse von Kaspersky Sandbox wartet:
  - Zeitpunkt, zu dem die Objektuntersuchungsaufgabe empfangen wurde
  - Status der Objektverarbeitung
  - ID der Benutzersitzung im Betriebssystem, in der die Objektuntersuchungsaufgabe erstellt wurde
  - ID der Objektuntersuchungsaufgabe
  - MD5-Hash der Objektuntersuchungsaufgabe
  - System-ID (SID) des Betriebssystembenutzers, dessen Benutzerkonto zum Erstellen der Aufgabe verwendet wurde
  - XML-Schema des automatisch erstellten IOC
  - MD5- oder SHA256-Hash des untersuchten Objekts
  - Verarbeitungsfehler
  - Namen der Objekte, für welche die Aufgabe erstellt wurde
  - Untersuchungsergebnis für das Objekt

Daten in Anfragen an Kaspersky Sandbox

Die folgenden Daten aus Anfragen des integrierten Agenten von Kaspersky Endpoint Security an Kaspersky Sandbox werden lokal auf dem Computer gespeichert:

- MD5-Hash der Untersuchungsaufgabe
- ID der Untersuchungsaufgabe
- Untersuchtes Objekt und alle zugehörigen Dateien

Daten, die aufgrund der Ausführung der Aufgabe IOC-Untersuchung (eigenständige Aufgabe) empfangen werden

Kaspersky Endpoint Security übermittelt automatisch Daten über die Ausführungsergebnisse der Aufgabe *IOC-Untersuchung* an Kaspersky Security Center.

Die Daten in den Ausführungsergebnissen der Aufgabe *IOC-Untersuchung* können die folgenden Informationen enthalten:

- IP-Adresse aus der ARP-Tabelle
- Physikalische Adresse aus der ARP-Tabelle
- Typ und Name des DNS-Eintrags
- IP-Adresse des geschützten Computers
- Physikalische Adresse (MAC-Adresse) des geschützten Computers
- ID im Ereignisprotokolleintrag
- Name der Datenquelle im Protokoll
- Protokollname
- Ereigniszeitpunkt
- MD5- und SHA256-Hashwerte der Datei
- Vollständiger Name der Datei (einschließlich Pfad)
- Dateigröße
- Remote-IP-Adresse und Port, mit denen während der Untersuchung eine Verbindung hergestellt wurde
- Lokale IP-Adresse des Adapters
- Port, der auf dem lokalen Adapter geöffnet ist
- Protokoll als Zahl (gemäß IANA-Standard)

- Prozessname
- Prozess-Argumente
- Pfad der Prozessdatei
- Windows-ID (PID) des Prozesses
- Windows-ID (PID) des übergeordneten Prozesses
- Benutzerkonto, das den Prozess gestartet hat
- Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
- Dienstname
- Dienstbeschreibung
- Pfad und Name des DLL-Dienstes (für svchost)
- Pfad und Name der ausführbaren Dienstdatei
- Windows-ID (PID) des Dienstes
- Diensttyp (z. B. ein Kerneltreiber oder Adapter)
- Dienststatus
- Startmodus des Dienstes
- Name des Benutzerkontos.
- Volume-Name
- Volume-Buchstabe
- Volume-Typ
- Windows-Systemregistrierungswert
- Registrierungstrukturwert
- Registrierungsschlüsselpfad (ohne Struktur- und Wertname)
- Registrierungseinstellung
- System (Umgebung)
- Name und Version des auf dem Computer installierten Betriebssystems
- Netzwerkname des geschützten Computers
- Domäne oder Gruppe, zu welcher der geschützte Computer gehört
- Browsername

- Browserversion
- Zeitpunkt des letzten Zugriffs auf die Webressource
- URL aus der HTTP-Anforderung
- Name des Benutzerkontos, das für die HTTP-Anforderung verwendet wurde
- Dateiname des Prozesses, der die HTTP-Anforderung gestellt hat
- Vollständiger Pfad der Datei des Prozesses, der die HTTP-Anforderung gestellt hat
- Windows-ID (PID) des Prozesses, der die HTTP-Anforderung gestellt hat
- HTTP-Referenz (Quell-URL der HTTP-Anforderung)
- URI der über HTTP angeforderten Ressource
- Informationen über den HTTP-Benutzeragenten (die Anwendung, die die HTTP-Anforderung gestellt hat)
- Ausführungszeit der HTTP-Anforderung
- Eindeutige ID des Prozesses, der die HTTP-Abfrage gestellt hat

Kaspersky Endpoint Detection and Response Expert (on-premises)

Alle Daten, die von der App lokal auf dem Computer gespeichert werden, werden bei der Deinstallation von Kaspersky Endpoint Security vom Computer gelöscht.

Dienstdaten

Der integrierte Agent von Kaspersky Endpoint Security speichert die folgenden Daten lokal:

- Daten, die für die Integration in die Komponente „EDR Expert (on-premises)“ erforderlich sind:
  - Adresse und Port zur Verbindung mit dem KATA Central Node-Server
  - Adresse und Port zur Verbindung mit dem Telemetrie-Übertragungsserver
  - Adresse und Port zur Verbindung mit dem Reaktionsserver
  - Informationen zu Zertifikaten, die für die Integration in KATA Central Node verwendet werden
  - Informationen zu Zertifikaten, die für die Integration mit dem Telemetrie-Übertragungsserver verwendet werden
  - Informationen zu Zertifikaten, die für die Integration in den Antwortserver verwendet werden
- Dateien in Quarantäne

Daten aus übertragenen Telemetrie-Ereignissen

- **Telemetriedaten**
  - Daten zu Dateien:
    - Eindeutige IDs der Datei
    - Dateityp
    - Vollständiger Dateipfad
    - Dateigröße
    - Datei-Attribute
    - ID der Zone
    - Datum und Uhrzeit der Erstellung der Datei
    - Datum und Uhrzeit der letzten Änderung der Datei
    - Ursprünglicher Dateiname
    - Name des Programms
    - Programmversion
    - Programmhersteller
    - Dateibeschreibung
    - Dateiversion.
    - MD5- und SHA256-Hashwerte des Objekts
    - Überprüfungsergebnis für die Dateisignatur
    - Name des Zertifikatausstellers
    - Name des Zertifikatinhabers
    - Seriennummer des Zertifikats
  - Daten über die AMSI-Untersuchung:
    - Eindeutige ID des Prozesses, der die Aktivität initiiert hat
    - Inhaltstyp des an AMSI übertragenen Objekts
    - Inhalt des an AMSI übertragenen Objekts

    - Name des Objekts
    - MD5- und SHA256-Hashwerte des Objekts
- Daten über die Sperrung des Programms:
    - Eindeutige ID des Prozesses, der die Sperrung des Programms initiiert hat
    - Eindeutige ID des übergeordneten Prozesses
    - Eindeutige System-ID des Prozesses
    - Befehl, der zum Starten eines Prozesses verwendet wurde
    - Anmeldesitzungs-ID
    - Prozess-Integritätsstufe
    - Prozess-Status
    - Eindeutige ID der Prozessdatei
    - Prozess-Befehlszeile
    - Liste der eindeutigen IDs von interpretierten Dateien
- Daten über das Verbot zum Öffnen einer Datei:
    - Eindeutige ID des Prozesses, der das Öffnen einer Datei initiiert hat
    - Eindeutige IDs der Datei
- Daten über das Laden eines Treibers:
    - Eindeutige ID des geladenen Treibers
- Daten über Ereignisse:
    - Eindeutige Ereignis-ID
    - Datum und Uhrzeit des Ereignisses
- Daten über die Änderung einer Datei:
    - Eindeutige ID des Prozesses, der die Änderung einer Datei initiiert hat
    - Eindeutige IDs der Datei
    - Art des Änderungsvorgangs
    - Kennzeichen, das angibt, dass die Datei nach dem Neustart des Computers gelöscht wird
    - Eindeutige ID der geänderten Datei
    - Eindeutige Datei-ID vor der Änderung

    - Satz von Bit-Kennzeichen, die angeben, wie die Datei geöffnet wurde
    - Daten über Vorgänge in der Zugriffssteuerungsliste
    - Daten über Änderungen des Eigentümers oder der übergeordneten Gruppe der Datei
- Daten über die Anmeldesitzung:
    - Anmeldesitzungs-ID
    - Name des Benutzers, der sich angemeldet hat
    - Typ des Benutzerkontos
    - Sitzungstyp
- Daten über Netzwerkverbindungen:
    - Eindeutige ID des Prozesses, der die Verbindung initiiert hat
    - Lokale IP-Adresse, über die die Verbindung initiiert wurde
    - Remote-IP-Adresse des Verbindungsendpunkts
    - Verbindungsrichtung
    - Datenübertragungsprotokoll
    - HTTP-Methode
    - Pfad ohne Hostname
    - Hostname
    - Dynamischer Prozess-Status zum Zeitpunkt der Verbindung
    - Kennzeichen, das angibt, dass die Verbindung auf Raw-Socket-Ebene geöffnet ist
    - TLS-Version, die in der Verbindungssitzung verwendet wurde
    - Name des TLS-Servers
    - MD5- und SHA1-Hashes des TLS-Serverzertifikats
    - Liste der alternativen Antragstellernamen (SAN) des Zertifikats
    - Name des TLS-Zertifikatausstellers
    - Seriennummer des Zertifikats
    - Verwendeter Verschlüsselungsalgorithmus
    - Anfangs- und Ablaufdatum des Zertifikats

    - JA3-Fingerabdruck des TLS-Clients
    - JA3S-Fingerabdruck des Servers
- Daten, die beim Überwachen eines Netzwerkports erfasst wurden:
    - Eindeutige ID des Prozesses, der die Verbindung initiiert hat
- Eingabedaten aus der Befehlszeile:
    - Eindeutige ID des Prozesses, der die Konsoleneingabe initiiert hat
    - Art der Konsoleneingabe
    - Text, der von einem Benutzer oder Prozess eingegeben wurde
- Daten über das Beenden des Erstellung:
    - Eindeutige ID des Prozesses
    - Eindeutige ID des übergeordneten Prozesses
    - Eindeutige System-ID des Prozesses
    - Befehl, der zum Starten eines Prozesses verwendet wurde
    - Anmeldesitzungs-ID
    - Prozess-Integritätsstufe
    - Eindeutige ID der Prozessdatei
    - Liste der eindeutigen IDs von interpretierten Dateien
    - Prozesstyp
- Daten über das vom Prozess geladene Modul:
    - Eindeutige ID des Prozesses, der den Download initiiert hat
    - Vollständiger Pfad der Datei, die in den Prozess hochgeladen wurde
    - Eindeutige ID der Moduldatei
    - Vollqualifizierter Name der .NET-Assembly, wenn die geladene Datei ein .NET-Modul ist
    - Kennzeichen der .NET-Assembly, die im Manifest definiert sind
- Daten über das Beenden des Prozesses:
    - Eindeutige ID des beendeten Prozesses

- Daten über eine Registrierungsänderung:
  - Eindeutige ID des Prozesses, der die Registrierungsänderung initiiert hat
  - Art des Registrierungsvorgangs
  - Vollständiger Pfad des Registrierungsschlüssels
  - Name des Werts in einem Registrierungsschlüssel
  - Typ der Daten, die im Registrierungsschlüsselwert gespeichert sind
  - Daten, die im Registrierungsschlüsselwert angegeben sind
  - Name des Schlüssels vor dem Umbenennen
  - Informationen über eine Änderung des Eigentümers des Schlüssels oder der primären Schlüsselgruppe
  - Liste der Änderungen in der Zugriffssteuerungsliste (ACL) des Schlüssels
- Daten über die erkannte Bedrohung und deren Verarbeitung:
  - Kennzeichen, das angibt, dass die Bedrohungserkennung im Hintergrund ausgeführt wurde
  - Verdikt zur Bedrohung
  - Name des Verdikts
  - Eindeutige ID des Datenbankeintrags
  - Zeitpunkt, zu dem der Bedrohungsdatensatz in der Datenbank gespeichert wurde
  - Modus der Bedrohungsverarbeitung
  - Typ des infizierten Objekts
  - Name des infizierten Objekts
  - MD5- und SHA256-Hashwerte des Objekts
  - Eindeutige ID des infizierten Objekts
  - Eindeutige ID des Prozesses, der das infizierte Objekt aus dem Internet heruntergeladen hat
  - URL, von der das infizierte Objekt heruntergeladen wurde
  - E-Mail-Adresse des Absenders, von dem das infizierte Objekt gesendet wurde
  - Netzwerkprotokoll, über das das infizierte Objekt empfangen wurde
  - Lokale Adresse, von der das infizierte Objekt empfangen wurde
  - Externe Adresse, von der das infizierte Objekt empfangen wurde

    - Inhaltstyp des Objekts
    - Inhalt des Objekts
- Daten über den Zugriff auf Prozesse:
    - Eindeutige ID des Prozesses, der den Zugriffsversuch initiiert hat
    - Eindeutige ID des Zielprozesses, auf den zugegriffen wurde
    - Satz von Rechten, die vom Zielprozess angefordert wurden
    - Vorgangstyp
    - Satz von Aufrufen zum Zeitpunkt, als auf einen Prozess zugegriffen wurde
    - Beschreibung des Quellprozesses
    - Beschreibung des Zielprozesses
- Daten über DNS:
    - Eindeutige ID des Prozesses, der die DNS-Abfrage initiiert hat
    - IP-Adresse des DNS-Servers
    - Kennzeichen, die das Verhalten einer DNS-Abfrage steuern
    - Abschluss-Status der Anfrage
    - Vollqualifizierter Domänenname, der in der DNS-Abfrage angegeben wurde
    - Datentyp in der DNS-Abfrage
    - Antworten des DNS-Servers
- Daten über die Code-Injektion:
    - Eindeutige ID des Prozesses, der versucht hat, Code einzuschleusen
    - Verwendete Zugriffsmethode
    - Anzahl der Anrufe zum Zeitpunkt, als der injizierte Code erkannt wurde
    - Eindeutige ID des Zielprozesses, in den der Code hochgeladen wurde
    - Daten über Änderungen in der Befehlsfolge des Zielprozesses
    - Adresse des Zielprozesses
    - Name der DLL-Bibliothek, die in den Zielprozess hochgeladen wurde
    - Vollständiger Pfad der DDL-Datei

- Daten über Vorgänge mit benannten Kanälen:
  - Eindeutige ID des Prozesses, der den Kanal erstellt oder sich mit ihm verbunden hat
  - Vollständiger Name des benannten Kanals
  - Vorgangstyp (Erstellung oder Verbindung)
- Daten über WMI-Abfragen:
  - Eindeutige ID des Prozesses, der den WMI-Vorgang initiiert hat
  - Art des WMI-Vorgangs
  - Name des Zielgeräts für die WMI-Abfrage
  - Benutzerkonto, das die WMI-Abfrage initiiert hat
  - Text der WMI-Abfrage
  - Namespace, in dem die WMI-Abfrage ausgeführt wird
  - Name des WMI-Filters
  - Name des Consumer-Objekts
  - Text, der die Aktion des Consumer-Objekts beschreibt
- Daten über LDAP-Abfragen:
  - Eindeutige ID des Prozesses, der die LDAP-Abfrage gestellt hat
  - Suchbereich von LDAP-Abfragen
  - LDAP-Filter
  - Parameter, der die Active Directory-Partition angibt, an die die Abfrage gerichtet war
  - Attribute der LDAP-Suche
- Daten über angeschlossene USB-Geräte:
  - Modus des USB-Geräts
  - Typ des USB-Geräts
  - ID des USB-Gerätes
  - Name des USB-Geräts
  - Pfad des USB-Geräts
  - Kennzeichen, das angibt, dass es sich bei dem USB-Gerät um ein Systemlaufwerk handelt
- Daten über das Erstellen, Löschen und Ändern einer geplanten Aufgabe

- Daten über das Erstellen, Löschen und Ändern von Diensten
- Daten über das Einhängen/Aushängen des Dateisystems
- Daten über den Betrieb der Komponente „EDR Expert (on-premise)“:
  - Informationen zum Starten/Stoppen des Agenten
  - Informationen zur Installation/Deinstallation des Agenten
  - Eindeutige ID für den Start des Agenten
  - System-ID des Agentenprozesses
  - Eindeutige ID des Agentenprozesses
  - Grund für das Beenden des Agenten
  - Code für das Beenden des Agentenprozesses
- Einstellungen für Ereignisfilterung:
  - Modulnamen
  - Vollständige Pfade von Objekten
  - MD5- und SHA256-Hashes der Objekte
  - IDs der Einträge im Windows-Ereignisprotokoll
  - Einstellungen für digitale Zertifikate
  - Richtung des Datenverkehrs, IP-Adressen, Ports, Protokolle, vollständige Pfade der ausführbaren Dateien
  - Benutzernamen
  - Typen der Benutzeranmeldung
  - Arten von Telemetrie-Ereignissen, für die Filter angewendet werden

Daten aus Anfragen der EDR Expert-Komponente an den integrierten Agenten von Kaspersky Endpoint Security

- Allgemeine Aufgabeneinstellungen:
  - Aufgabentyp
  - Einstellungen für den Aufgabenzeitplan
  - Namen und Kennwörter der Benutzerkonten, unter denen die Aufgaben ausgeführt werden können
  - Versionen von Einstellungen

- IDs von isolierten Objekten
- Pfade der Objekte
- MD5- und SHA256-Hashes der Objekte
- Befehlszeile zum Starten des Prozesses mit den Argumenten
- Kennzeichen der zusätzlichen Aktionen, die nach dem Abschluss von Aufgaben durchgeführt werden
- Vom Server abzurufende IOC-Datei-IDs
- IOC-Dateien
- Dienstname
- Starttyp des Dienstes
- Ordner, für die die Ergebnisse der Aufgabe *Forensische Daten abrufen* empfangen werden müssen
- Masken der Objektnamen und Erweiterungen für die Aufgabe *Forensische Daten abrufen*

- Einstellungen der Netzwerkisolation:
  - Arten von Einstellungen
  - Versionen von Einstellungen
  - Listen mit Ausnahmen der Netzwerkisolation und Ausnahmeeinstellungen: Richtung des Datenverkehrs, IP-Adressen, Ports, Protokolle und vollständige Pfade der ausführbaren Dateien
  - Kennzeichen der zusätzlichen Aktionen
  - Zeitpunkt der Deaktivierung der automatischen Isolierung
- Einstellungen der Ausführungsprävention:
  - Arten von Einstellungen
  - Versionen von Einstellungen
  - Listen mit Ausführungsverhinderungsregeln und Regeleinstellungen: Pfade der Objekte, Objekttypen, MD5- und SHA256-Hashes von Objekten
  - Kennzeichen der zusätzlichen Aktionen

Daten aus Anfragen, die Kaspersky Endpoint Security an die EDR Expert-Komponente sendet

Bei der Integration in die Lösung „EDR Expert (on-premises)“ werden die folgenden Daten lokal auf den Computern gespeichert.

- Bei Synchronisationsanfragen:
  - Eindeutige ID
  - Grundlegender Teil der Webadresse der Servers
  - Computername
  - IP-Adresse des Computers
  - MAC-Adresse des Computers
  - Lokale Zeit auf dem Computer
  - Status des Selbstschutzes von Kaspersky Endpoint Security
  - Name und Version des auf dem Computer installierten Betriebssystems
  - Version von Kaspersky Endpoint Security
  - Versionen der App-Einstellungen und Aufgabeneinstellungen
  - Aufgabenstatus: Aufgaben-IDs, Ausführungsstatus, Fehlercodes
- Bei Anfragen zum Abrufen von Dateien von dem Server:
  - Eindeutige IDs von Dateien
  - Eindeutige ID von Kaspersky Endpoint Security
  - Eindeutige IDs von Zertifikaten
  - Grundlegender Teil der Webadresse des Servers mit installierter Central Node-Komponente
  - Host-IP-Adresse
- In den Berichten über die Ergebnisse der Aufgabenausführung:
  - Host-IP-Adresse
  - Informationen zu den während einer IOC-Untersuchung oder YARA-Untersuchung erkannten Objekten
  - Kennzeichen der zusätzlichen Aktionen, die nach dem Abschluss von Aufgaben durchgeführt werden
  - Fehler bei der Aufgabenausführung und Rückgabecodes
  - Abschlussstatus der Aufgabe

- Abschlusszeit der Aufgabe
- Versionen der Einstellungen, die für die Ausführung der Aufgaben verwendet werden
- Informationen zu isolierten Objekten, die an den Server gesendet wurden, und zu aus der Quarantäne wiederhergestellten Objekten: Pfade der Objekte, MD5- und SHA256-Hashes, IDs von isolierten Objekten
- Informationen über die auf Anforderung des Servers auf einem Computer gestarteten oder beendeten Prozesse: PID und UniquePID, Fehlercode, MD5- und SHA256-Hashwerte der Objekte
- Informationen über die Dienste, die auf Anfrage des Servers auf einem Computer gestartet oder beendet wurden: Dienstname, Starttyp, Fehlercode, MD5- und SHA256-Hashwerte von Dateiabbildern der Dienste
- Informationen zu den Objekten, für die ein Speicherabbild für eine YARA-Untersuchung erstellt wurde (Pfade, ID der Dump-Datei)
- Vom Server angeforderte Dateien

- Daten zu laufenden Prozessen:
  - Name der ausführbaren Datei, einschließlich vollständiger Pfad und Erweiterung
  - AutoAusführen-Parameter des Prozesses
  - Prozess-ID
  - Anmeldesitzungs-ID
  - Name der Anmeldesitzung
  - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
  - MD5- und SHA256-Hashwerte des Objekts
- Daten zu Dateien:
  - Dateipfad
  - Dateiname.
  - Dateigröße
  - Datei-Attribute
  - Datum und Uhrzeit der Erstellung der Datei
  - Datum und Uhrzeit der letzten Änderung der Datei
  - Dateibeschreibung
  - Name des Unternehmens
  - MD5- und SHA256-Hashwerte des Objekts
  - Registrierungsschlüssel (für AutoAusführen-Punkte)

- Daten in Fehlern, die beim Abrufen von Informationen zu Objekten aufgetreten sind:
  - Vollständiger Name des Objekts, das verarbeitet wurde, als ein Fehler auftrat
  - Fehlercode
- Daten in YARA-Untersuchungsergebnissen:

  Der integrierte Agent von Kaspersky Endpoint Security überträgt automatisch YARA-Untersuchungsergebnisse an Kaspersky Anti Targeted Attack Platform, um eine Bedrohungsentwicklungskette zu erstellen.

  Die Daten werden vorübergehend lokal in der Warteschlange gespeichert, um die Ergebnisse der Aufgabenausführung an den Kaspersky Anti Targeted Attack Platform-Server zu senden. Die Daten werden nach dem Absenden aus dem Zwischenspeicher gelöscht.
  - MD5- und SHA256-Hashwerte der Datei
  - Vollständiger Name der Datei
  - Dateipfad
  - Dateigröße
  - Prozessname
  - Prozess-Argumente
  - Pfad der Prozessdatei
  - Windows-ID (PID) des Prozesses
  - Windows-ID (PID) des übergeordneten Prozesses
  - Benutzerkonto, das den Prozess gestartet hat
  - Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
- Daten in IOC-Untersuchungsergebnissen:
  - IP-Adresse aus der ARP-Tabelle
  - Physikalische Adresse aus der ARP-Tabelle
  - Name des DNS-Eintrags
  - Typ des DNS-Eintrags
  - Hostname
  - IP-Adresse
  - Ereignis-ID im Protokoll
  - Name der Datenquelle im Protokoll
  - Protokollname

- Benutzername
- Datum und Uhrzeit der Ereignisgenerierung im ISO-Format
- MD5- und SHA256-Hashwerte der Datei
- Vollständiger Name der Datei
- Dateigröße
- Remote-IP-Adresse und Port, mit denen während der Untersuchung eine Verbindung hergestellt wurde
- IP-Adresse und Port des lokalen Adapters
- Protokoll
- Prozessname
- Prozess-Argumente
- Pfad der Prozessdatei
- Windows-ID (PID) des Prozesses
- Windows-ID (PID) des übergeordneten Prozesses
- Benutzerkonto, das den Prozess gestartet hat
- Zeitpunkt (Datum und Uhrzeit), zu dem der Prozess gestartet wurde
- Pfad des Registrierungsschlüssels
- Name des Registrierungsschlüssels
- Textwert des Registrierungsschlüssels
- Dienstname
- Dienstbeschreibung
- Pfad und Name des DLL-Dienstes
- Pfad und Name der ausführbaren Dienstdatei
- Windows-ID (PID) des Dienstes
- Typ des Dienstes
- Dienststatus
- Startmodus des Dienstes
- Name des Betriebssystems
- Version des Betriebssystems

- Name des Computernetzwerks ohne Domäne
- Domäne oder Arbeitsgruppe
- Benutzername
- Volume-Name
- Volume-Buchstabe
- Volume-Typ

Kaspersky Network Detection and Response (KATA)

Alle Daten, die von der App lokal auf dem Computer gespeichert werden, werden bei der Deinstallation von Kaspersky Endpoint Security vom Computer gelöscht.

Telemetriedaten

- **Daten über Dateien**
  - Eindeutige IDs der Datei
  - Dateityp
  - Vollständiger Dateipfad
  - Dateigröße
  - Datei-Attribute
  - ID der Zone
  - Datum und Uhrzeit der Erstellung der Datei
  - Datum und Uhrzeit der letzten Änderung der Datei
  - Ursprünglicher Dateiname
  - Name des Programms
  - Programmversion
  - Programmhersteller
  - Dateibeschreibung
  - Dateiversion.

- MD5- und SHA256-Hashwerte des Objekts
- Überprüfungsergebnis für die Dateisignatur
- Datum und Uhrzeit der Erstellung der Dateisignatur
- Zertifikatketten, die in der Signaturdatei verwendet wurden
- Typ der Zertifikatkette
- Zertifikate in der Kette
- Name des Zertifikatausstellers
- Name des Zertifikatinhabers
- Seriennummer des Zertifikats
- Algorithmus für den Fingerabdruck des Zertifikats
- Fingerabdruck des Zertifikats
- Gültigkeitsdauer des Zertifikats

- **Daten über die Anmeldesitzung**
  - Anmeldesitzungs-ID
  - Kontoname des Benutzers, der sich angemeldet hat
  - Typ des Benutzerkontos
  - Sitzungstyp
  - IP-Adresse des Computers, von dem aus der Anmeldeversuch erfolgte
  - IP-Adresse des lokalen Computers, für den der Anmeldeversuch ausgeführt wurde
  - Kennzeichen, das angibt, dass die Sitzung, auf die sich dieses Ereignis bezieht, erhöhte Berechtigungen und Administratorrechte hat
  - Parameter, der angibt, ob andere Sitzungen mit dieser Anmeldesitzung verknüpft sind
  - Protokoll, das für die Terminalsitzung verwendet wurde
  - IPv4-Protokoll, das für die Terminalsitzung verwendet wurde
- **Daten über die Netzwerkkommunikation**
  - Beginn und Ende des Zeitraums, während dem die Daten gesammelt wurden
  - Liste der Verbindungen
  - Lokale IP-Adresse des Computers

- Lokale MAC-Adresse des Computers
- Remote-IP-Adresse des Computers
- Remote-MAC-Adresse des Computers
- Gateway-IP-Adresse
- Anzahl der übertragenen Datenpakete
- Anzahl der empfangenen Datenpakete
- Gesamtzahl der übertragenen Bytes
- Datenübertragungsprotokoll
- EtherType-Feld des Ethernet-Frames
- Payload-Präfix des ersten Pakets im Intervall
- IPv4-Adresse der Netzwerkschnittstelle, über die die Kommunikation erfasst wurde

- **Daten über die Netzwerkverbindung**
  - Eindeutige ID des Prozesses, der die Verbindung initiiert hat
  - Datenübertragungsprotokoll
  - Lokale IP-Adresse, über die die Verbindung initiiert wurde
  - Remote-IP-Adresse des Verbindungsendpunkts
  - HTTP-Methode
  - Pfad ohne Hostname
  - Hostname
  - Dynamischer Prozess-Status zum Zeitpunkt der Verbindung
  - Verbindungsrichtung
  - Dynamischer Prozess-Status
  - EtherType-Feld des Ethernet-Frames
- **Daten, die beim Überwachen eines Netzwerkports erfasst wurden**
  - Eindeutige ID des Prozesses, der die Verbindung initiiert hat
  - Datenübertragungsprotokoll
  - Lokale Adresse
  - Dynamischer Prozess-Status zum Zeitpunkt der Verbindung

- **Ergebnis der Verbindungsüberprüfung**
  - Netzwerkeinstellungen des Hosts
  - Beschreibung der Netzwerkschnittstelle
  - Name der DNS-Domäne
  - Lokale MAC-Adresse des Computers
  - Metrikzahl der IP-Verbindung
  - Liste der IP-Adressen
  - IP-Adresse
  - Netzwerkmaske
  - Gateway-IP-Adresse
  - Gateway-MAC-Adresse
  - Liste der installierten Patches
  - Patch-Nummer
  - Patch-Installationsdatum
  - Gerätemodell
  - Gerätehersteller
  - Host-ID in Kaspersky Security Center
  - Beschreibung des installierten Kaspersky Anti-Virus
  - Name der Komponente des installierten Kaspersky Anti-Virus
  - Version der Komponente des installierten Kaspersky Anti-Virus
  - Version der Datenbank der installierten Komponente von Kaspersky Anti-Virus
  - Datum des letzten Datenbanken-Updates der installierten Komponente von Kaspersky Anti-Virus
  - Status der Komponente des installierten Kaspersky Anti-Virus
  - Liste der Lizenzschlüssel
  - Seriennummer des Schlüssels
  - Schlüsseltyp

- Ablaufdatum des Schlüssels
- Status des Schlüssels

- **Daten über die Prozess-Erstellung auf dem Host**
  - Eindeutige ID des Prozesses
  - Eindeutige ID des übergeordneten Prozesses
  - Eindeutige System-ID des Prozesses
  - Befehl, der zum Starten eines Prozesses verwendet wurde
  - Anmeldesitzungs-ID
  - Terminalsitzungs-ID
  - Eindeutige ID der Prozessdatei
  - Prozess-Integritätsstufe
  - Liste der Token für Prozessrechte
  - Rechte von Attributen
  - Liste der eindeutigen IDs von interpretierten Dateien
  - Prozess-Status
  - Befehl, der zum Starten eines Prozesses verwendet wurde
- **Daten über das Beenden des Prozesses**
  - Eindeutige ID des Prozesses
- **Daten über die erkannte Bedrohung**
  - Informationen über die Bedrohung
  - Verdikt zur Bedrohung
  - Nummer des AMR-Eintrags
  - Version der Antiviren-Datenbanken
  - Modus der Bedrohungserkennung
  - Eindeutige ID der Bedrohung
  - Schutztechnologie
  - Informationen über das infizierte Objekt
  - Typ des infizierten Objekts

- Name des infizierten Objekts
- MD5- und SHA256-Hashwerte des Objekts
- Eindeutige ID des infizierten Prozesses
- Eindeutige ID des infizierten Objekts
- Eindeutige ID des Prozesses, der das infizierte Objekt aus dem Internet heruntergeladen hat
- URL, von der das infizierte Objekt heruntergeladen wurde
- E-Mail-Adresse des Absenders, von dem das infizierte Objekt gesendet wurde
- Netzwerkprotokoll, über das das infizierte Objekt empfangen wurde
- Lokale Adresse, von der das infizierte Objekt empfangen wurde
- Externe Adresse, von der das infizierte Objekt empfangen wurde
- Inhaltstyp des Objekts
- Kontext der erkannten Bedrohung
- Inhalt des Objekts
- Kennzeichen, das angibt, dass die Bedrohungserkennung im Hintergrund ausgeführt wurde

- **Daten über die Verarbeitung der Bedrohung**
  - Informationen über die Bedrohung
  - Verdikt zur Bedrohung
  - Nummer des AMR-Eintrags
  - Version der Antiviren-Datenbanken
  - Modus der Bedrohungserkennung
  - Name des infizierten Objekts
  - MD5- und SHA256-Hashwerte des Objekts
  - Eindeutige ID des infizierten Prozesses
  - Eindeutige ID des infizierten Objekts
  - Netzwerkprotokoll, über das das infizierte Objekt empfangen wurde
  - Lokale Adresse, von der das infizierte Objekt empfangen wurde
  - Externe Adresse, von der das infizierte Objekt empfangen wurde
  - Status der Bedrohungsverarbeitung

- Grund, aus dem die Bedrohung nicht neutralisiert werden konnte
- Lokale physische Adresse

- **Daten über Benutzer**
  - Benutzer-SID
  - Benutzer-ID
  - Benutzername
  - Vollständiger Name des Benutzers
  - Beschreibung des Benutzers
  - Ob das Benutzerkonto aktiv oder gesperrt ist
  - Ob das Kennwort abgelaufen ist
  - Ob eine Kennwortänderung erforderlich ist
  - Ob die Kennwortänderung zulässig ist
  - Typ des Benutzerkontos
  - Ob die automatische Anmeldung für dieses Benutzername aktiviert ist
  - Liste der Gruppen, zu denen der Benutzer gehört

Integration in Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Alle Daten, die von der App lokal auf dem Computer gespeichert werden, werden bei der Deinstallation von Kaspersky Endpoint Security vom Computer gelöscht.

Bei der Integration in Kaspersky Unified Monitoring and Analysis Platform (KUMA) werden Daten der Verbindungseinstellungen sowie alle in den Windows-Protokollen registrierten Ereignisse übertragen.

Die wichtigsten Windows-Ereignisprotokolle sind System, Security, Application, ForwardedEvents und HardwareEvents. Benutzer können auch benutzerdefinierte Protokolle erstellen und damit arbeiten, um spezifische Anforderungen zu erfüllen.

Einhaltung der Gesetzgebung der Europäischen Union (DSGVO)

Kaspersky Endpoint Security kann unter den folgenden Szenarien Daten an Kaspersky übertragen:

- Verwendung von Kaspersky Security Network
- Aktivierung des Programms mit einem Aktivierungscode

- Update der Programm-Module und Antiviren-Datenbanken
- Klicken auf Links in der Programmoberfläche

Unabhängig von der Datenklassifikation und dem Territorium, aus dem die Daten stammen, hält Kaspersky hohe Standards für die Datensicherheit ein und setzt verschiedene rechtliche, organisatorische und technische Maßnahmen ein, um die Daten der Benutzer zu schützen, die Datensicherheit und Vertraulichkeit zu gewährleisten und auch die Erfüllung der durch die geltende Gesetzgebung garantierten Rechte der Benutzer sicherzustellen. Der Text der Datenschutzrichtlinie ist im Leistungsumfang des Programms enthalten und auf der Kaspersky-Website verfügbar.

Bevor Sie Kaspersky Endpoint Security verwenden, lesen Sie bitte sorgfältig die Beschreibung zu den übertragenen Daten im Endbenutzer-Lizenzvertrag und in der KSN-Erklärung. Wenn bestimmte Daten, die von Kaspersky Endpoint Security unter einem der beschriebenen Szenarien übertragen werden, gemäß Ihrer lokalen Gesetzgebung oder Norm als personenbezogene Daten eingestuft werden können, müssen Sie sicherstellen, dass diese Daten rechtmäßig verarbeitet werden und die Zustimmung der Endbenutzer für die Erfassung und Übertragung dieser Daten einholen.

Ausführliche Angaben darüber, wie Informationen über die Programmverwendung empfangen, verarbeitet, gespeichert und gelöscht werden, nachdem der Lizenzvertrag und die Erklärung zu Kaspersky Security Network akzeptiert worden sind, finden Sie in den genannten Dokumenten und auf der Kaspersky-Website. Die Dateien license.txt und ksn_<ID der Sprache>.txt mit den Texten des Endbenutzer-Lizenzvertrags und der Erklärung zu Kaspersky Security Network gehören zum Lieferumfang des Programms.

Wenn Sie keine Daten an Kaspersky übertragen möchten, können Sie die Datenbereitstellung deaktivieren.

Arbeiten mit dem Kaspersky Security Network

Durch die Nutzung des Kaspersky Security Network erklären Sie sich damit einverstanden, die in der KSN-Erklärung aufgeführten Daten automatisch zur Verfügung zu stellen. Wenn Sie nicht damit einverstanden sind, Kaspersky diese Daten zur Verfügung zu stellen, verwenden Sie Kaspersky Private Security Network (KPSN) oder deaktivieren Sie die Verwendung von KSN. Weitere Informationen über KPSN finden Sie in der Dokumentation zu Kaspersky Private Security Network.

Aktivieren des Programms mit einem Aktivierungscode

Durch die Verwendung eines Aktivierungscodes erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Wenn Sie es ablehnen, Kaspersky diese Informationen bereitzustellen, muss für die Aktivierung von Kaspersky Endpoint Security eine Schlüsseldatei verwendet werden.

Aktualisierung von Programm-Modulen und Antiviren-Datenbanken

Durch die Verwendung von Kaspersky-Servern erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Kaspersky benötigt diese Informationen, um zu überprüfen, ob Kaspersky Endpoint Security rechtmäßig verwendet wird. Wenn Sie nicht damit einverstanden sind, diese Informationen an Kaspersky weiterzugeben, verwenden Sie das Kaspersky Security Center für Datenbanken-Updates oder das Kaspersky Update-Dienstprogramm.

Folgende Links in der Programmoberfläche

Durch die Verwendung von Links in der Programmoberfläche erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Die genaue Liste der in jeder spezifischen Verbindung übertragenen Daten hängt davon ab, wo sich die Verbindung in der Programmoberfläche befindet und welches Problem damit gelöst werden soll. Wenn Sie nicht damit einverstanden sind, diese Daten Kaspersky zur Verfügung zu stellen, verwenden Sie die vereinfachte Programmoberfläche oder blenden Sie die Programmoberfläche aus.

Aufzeichnung von Dump-Dateien

Wenn Sie das Schreiben von Dump-Dateien aktiviert haben, erstellt Kaspersky Endpoint Security eine Dump-Datei, die alle Speicherdaten von Programmprozessen zum Zeitpunkt der Erstellung dieser Dump-Datei enthält.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, Reader und Shockwave sind eingetragene Markenzeichen oder Markenzeichen von Adobe in den USA und/oder anderen Ländern.

Amazon, Amazon Web Services, AWS sind Markenzeichen von Amazon.com, Inc. oder der verbundenen Unternehmen.

Apple, FireWire, iTunes, Mac und Safari sind Markenzeichen von Apple Inc.

Arm ist ein eingetragenes Markenzeichen von Arm Limited (oder seinen Tochterunternehmen) in den USA und/oder anderen Ländern.

AutoCAD ist ein Markenzeichen oder eingetragenes Markenzeichen von Autodesk, Inc. und/oder deren Tochterunternehmen und/oder verbundenen Unternehmen in den USA und/oder anderen Ländern.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Borland ist ein Markenzeichen oder ein eingetragenes Markenzeichen der Borland Software Corporation.

Cisco, Cisco AnyConnect, IOS sind eingetragene Markenzeichen oder Markenzeichen von Cisco Systems, Inc. und/oder der verbundenen Unternehmen in den USA und bestimmten anderen Ländern.

Citrix, Citrix Provisioning, Citrix Provisioning Services, Citrix Virtual Apps and Desktop, XenDesktop und XenServer sind eingetragene Markenzeichen oder Markenzeichen der Cloud Software Group, Inc. und/oder ihrer Tochterunternehmen in den USA und/oder anderen Ländern.

Cloudflare, Cloudflare Workers und das Cloudflare-Logo sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den USA und anderen Gerichtsbarkeiten.

Core ist das Markenzeichen der Intel Corporation oder ihrer Tochterunternehmen.

dBase ist eine Marke der dataBased Intelligence, Inc.

Dell Technologies, Dell, EMC und andere Markenzeichen sind Markenzeichen von Dell Inc. oder deren Tochterunternehmen.

Docker und das Docker-Logo sind Markenzeichen oder eingetragene Markenzeichen von Docker, Inc. in den USA und/oder anderen Ländern. Dabei können Docker, Inc. und andere Parteien auch Markenrechte an anderen hier verwendeten Bedingungen besitzen.

ESET ist ein Markenzeichen oder eingetragenes Markenzeichen von ESET spol. s r.o. oder der jeweiligen ESET-Einheit.

Foxit ist ein eingetragenes Markenzeichen der Foxit Corporation.

Radmin ist eine eingetragene Marke von Famatech.

Google, Android, Google Public DNS, Google Chrome, Chrome sind Markenzeichen von Google LLC.

HUAWEI, FusionCompute und FusionSphere sind eingetragene Markenzeichen von Huawei Technologies Co., Ltd.

ICQ ist ein Markenzeichen und/oder eine Handelsmarke von ICQ LLC.

Intel ist das Markenzeichen der Intel Corporation oder ihrer Tochterunternehmen.

IBM ist eine Marke der International Business Machines Corporation, die in vielen Ländern registriert ist.

Lenovo und Lenovo ThinkPad sind Markenzeichen von Lenovo in den USA und/oder anderen Ländern.

Linux ist eine in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragen Marke von Linus Torvalds.

Logitech ist eine in den Vereinigten Staaten von Amerika und (oder) in anderen Ländern eingetragene Marke oder eine Marke des Unternehmens Logitech.

LogMeIn Pro und Remotely Anywhere sind Markenzeichen von LogMeIn, Inc.

Mail.ru ist ein Markenzeichen von Mail.ru LLC.

McAfee ist ein Markenzeichen oder eingetragenes Markenzeichen von McAfee LLC oder deren Tochterunternehmen in den USA und/oder anderen Ländern.

Microsoft, Access, Active Directory, ActiveSync, Bing, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, LifeCam Cinema, Microsoft Edge, MSDN, MS-DOS, MultiPoint, Office 365, Outlook, PowerPoint, PowerShell, Skype, SQL Server, Surface, Visual Basic, Visual FoxPro, Windows, Windows Live, Windows PowerShell, Windows Server und Windows Store sind Markenzeichen der Microsoft-Unternehmensgruppe.

Mozilla, Firefox und Thunderbird sind Markenzeichen der Mozilla Foundation in den USA und anderen Ländern.

NetApp ist ein Markenzeichen oder ein eingetragenes Markenzeichen von NetApp, Inc. in den USA und/oder anderen Ländern.

OpenSSL ist ein Markenzeichen der OpenSSL Software Foundation.

OpenStack ist ein eingetragenes Markenzeichen der OpenStack Foundation in den Vereinigten Staaten von Amerika und anderen Ländern.

Oracle, Java und JavaScript sind eingetragene Markenzeichen von Oracle und/oder der verbundenen Unternehmen.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Realtek ist ein Markenzeichen von Realtek Semiconductor Corporation.

SAMSUNG ist ein Markenzeichen von SAMSUNG in den USA oder anderen Ländern.

Thawte ist ein Markenzeichen oder eingetragenes Markenzeichen der Symantec Corporation oder der verbundenen Unternehmen in den USA und anderen Ländern.

Trend Micro ist ein Markenzeichen oder eingetragenes Markenzeichen von Trend Micro Incorporated.

VERISIGN ist ein eingetragenes Markenzeichen in den USA und anderen Ländern oder ein nicht eingetragenes Markenzeichen von VeriSign, Inc. und seinen Tochterunternehmen.

VMware, VMware ESXi, VMware Horizon, VMware Workstation, VMware Tools, VMware vSphere sind eingetragene Markenzeichen und/oder Markenzeichen von VMware, Inc. in den USA und in anderen Ländern.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich im Installationsordner der App befindet.