kaspersky

Kaspersky Embedded Systems Security 4.1 für Windows

© 2026 AO Kaspersky Lab

Inhalt

Kaspersky Embedded Systems Security für Windows
- Neuerungen
- Behobene Probleme
- Lieferumfang
- Hard- und Softwarevoraussetzungen
- Unterstützte Versionen von Kaspersky Security Center
- Funktionale Anforderungen und Einschränkungen
  - Programm installieren und deinstallieren
  - Überwachung der Systemintegrität
  - Firewall
  - Einschränkungen für veraltete Windows-Versionen
  - Integration in Kaspersky Security Center
  - Andere Einschränkungen
- Kompatibilität mit anderen Programmen

Programm installieren und deinstallieren
- Installation planen
  - Administrations-Tools auswählen
  - Installationstyp auswählen
- Installation und Deinstallation des Programms mit dem Assistenten
  - Installation mit dem Installationsassistenten
    - Installation von Kaspersky Embedded Systems Security
    - Installation der Konsole für Kaspersky Embedded Systems Security
    - Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Gerät
      - Anonymen Remote-Zugriff auf COM-Anwendungen erlauben
      - Netzwerkverbindungen für Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security erlauben
    - Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
      - Update-Aufgabe für Datenbanken und Programm-Module starten und konfigurieren
      - Untersuchung wichtiger Bereiche
  - Ändern des Pakets von Programmkomponenten und Reparieren von Kaspersky Embedded Systems Security
  - Deinstallation mit dem Installationsassistenten
    - Deinstallation von Kaspersky Embedded Systems Security
    - Deinstallation der Konsole für Kaspersky Embedded Systems Security
- Installation und Deinstallation des Programms aus der Befehlszeile
  - Über die Installation und Deinstallation von Kaspersky Embedded Systems Security aus der Befehlszeile
  - Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer
  - Installations- und Wiederherstellungseinstellungen und Befehlszeilenoptionen für Windows Installer
  - Beispiele von Befehlen für die Installation von Kaspersky Embedded Systems Security
  - Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
  - Komponenten hinzufügen und entfernen. Beispiele für Befehle
  - Deinstallation von Kaspersky Embedded Systems Security. Beispiele für Befehle
  - Rückgabecodes

- Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center
  - Allgemeine Informationen zur Installation über Kaspersky Security Center
  - Rechte zur Installation bzw. Deinstallation von Kaspersky Embedded Systems Security
  - Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center
  - Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
  - Installation der Programmkonsole über das Kaspersky Security Center
  - Deinstallation von Kaspersky Embedded Systems Security über Kaspersky Security Center
  - Änderung der Auswahl der Programmkomponenten mithilfe von Kaspersky Security Center
- Installation und Deinstallation des Programms über Active Directory-Gruppenrichtlinien
  - Installation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory
  - Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
  - Deinstallation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory
- Installations- und Deinstallationsprotokolle für Kaspersky Embedded Systems Security
- Systemänderungen nach der Installation von Kaspersky Embedded Systems Security
- Prozesse von Kaspersky Embedded Systems Security
- Überprüfung der Funktionen von Kaspersky Embedded Systems Security Verwendung des EICAR-Testvirus
  - EICAR-Testvirus
  - Echtzeitschutz für Dateien und Funktionen der Untersuchung auf Befehl testen

Upgrade älterer Versionen von Kaspersky Embedded Systems Security auf Version 4.1

- Kaspersky Embedded Systems Security aktualisieren
- Administrations-Tools von Kaspersky Embedded Systems Security aktualisieren
- Migration von Richtlinien und Aufgaben
- Migration von Einstellungen der zu aktualisierenden Programmversion
- Vergleich der Komponenten und Aufgaben in Kaspersky Embedded Systems Security Version 3.4 und 4.1

Programmoberfläche

Arbeiten mit dem Verwaltungs-Plug-in

- Verwaltung von Kaspersky Embedded Systems Security über Kaspersky Security Center
- Programmeinstellungen verwalten
  - Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center
    - Einstellungen der Benutzeroberfläche und Untersuchungseinstellungen in Kaspersky Security Center konfigurieren
    - Sicherheitseinstellungen in Kaspersky Security Center anpassen
    - Verbindungseinstellungen über Kaspersky Security Center anpassen
    - Konfigurieren des Ausführungsmodus für lokale Aufgaben
  - Backup-Einstellungen in Kaspersky Security Center konfigurieren
- Erstellen und Einrichten von Richtlinien
  - Richtlinie erstellen
  - Anpassen einer Richtlinie
  - Indikator des Schutzniveaus
- Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center
  - Über die Erstellung von Aufgaben in Kaspersky Security Center
  - Aufgabe mithilfe von Kaspersky Security Center erstellen
  - Zu den lokalen Aufgabeneinstellungen und den allgemeinen Programmeinstellungen für einen einzelnen Computer wechseln
  - Gruppenaufgaben in Kaspersky Security Center anpassen
    - Aufgabe zur Programmaktivierung
    - Update-Aufgabe
    - Integritätsprüfung für Programme
  - Aufgaben planen

- Berichte in Kaspersky Security Center
- Echtzeit-Schutzstatus

Verwendung der Konsole für Kaspersky Embedded Systems Security

- Anwendungskonsole starten
- Benutzeroberfläche der Konsole für Kaspersky Embedded Systems Security
  - Fenster "Konsole für Kaspersky Embedded Systems Security"
  - Taskleistensymbol im Infobereich
- Allgemeine Einstellungen konfigurieren (in der Anwendungskonsole)
- Aufgaben von Kaspersky Embedded Systems Security verwalten
  - Aufgabenkategorien von Kaspersky Embedded Systems Security
  - Manuelles Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe
  - Aufgaben planen
  - Verwendung von Benutzerkonten für den Aufgabenstart
    - Über die Verwendung eines Benutzerkontos für den Aufgabenstart
    - Benutzerkonto für den Aufgabenstart festlegen
  - Import und Export von Einstellungen
    - Über den Import und Export von Einstellungen
    - Einstellungen exportieren
    - Einstellungen importieren
- Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen
- So konfigurieren Sie die Backup-Einstellungen (in der Anwendungskonsole)

Arbeiten mit dem Web-Plug-in der Web Console und der Cloud Console

- Kaspersky Embedded Systems Security über die Web Console und Cloud Console verwalten
- Einschränkungen für Web Plug-in
- Programmeinstellungen verwalten
  - Allgemeine Programmeinstellungen im Web-Plug-in konfigurieren
    - Schnittstelle und Untersuchungseinstellungen im Web-Plug-in konfigurieren
    - Einstellungen für Sicherheit und Zuverlässigkeit im Web-Plug-in konfigurieren
    - Anpassen der Verbindungseinstellungen im Web-Plug-in
    - Geplanten Starts lokaler Aufgaben im Web-Plug-in konfigurieren
  - Backup-Einstellungen im Web-Plug-in konfigurieren
- Erstellen und Einrichten von Richtlinien
- Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center
  - Zur Erstellung von Aufgaben im Web-Plug-in
  - Eine Aufgabe im Web-Plug-in erstellen
  - Gruppenaufgaben im Web-Plug-in anpassen
    - Aufgabe zur Programmaktivierung im Web-Plug-in konfigurieren
    - Update-Aufgabe im Web-Plug-in konfigurieren
  - Aufgaben planen
- Berichte in Kaspersky Security Center

Lizenzverwaltung des Programms

- Über den Endbenutzer-Lizenzvertrag
- Über die Lizenz
- Über das Lizenzzertifikat
- Über den Schlüssel
- Über die Schlüsseldatei
- Über den Aktivierungscode

Vergleich der Programmfunktionalität abhängig vom Lizenztyp
Aktivieren des Programms mit einer Schlüsseldatei
Aktivieren des Programms mit einem Aktivierungscode
Aufrufen von Informationen über die aktive Lizenz
Verlängerung der Lizenz
Löschen des Schlüssels
Starten und Beenden von Kaspersky Embedded Systems Security
Programm starten und beenden
Anhalten und Fortsetzen von Computerschutz und -kontrolle
Kompaktes Diagnosefenster
Über das kompakte Diagnosefenster
Status von Kaspersky Embedded Systems Security mithilfe des kompakten Diagnosefensters überprüfen
Überprüfung der Sicherheitsereignis-Statistik
Aktuelle Programmaktivität überprüfen
Anwendungsnachverfolgung und die Aufzeichnung von Speicherauszugsdateien konfigurieren
Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security
Selbstschutz-Mechanismus aktivieren und deaktivieren
Unterstützung der AM-PPL-Technologie
Betriebssystemdienste schützen
Benutzerberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security konfigurieren
Benutzerzugriffsberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security Service konfigurieren
Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security
Benachrichtigungen des sicheren Desktops
Vertrauenswürdige Zone
Erstellung von Untersuchungsausnahmen
Erkennbare Objekttypen wählen
Liste mit vertrauenswürdigen Programmen erstellen
Lokale vertrauenswürdige Zone erstellen
Vertrauenswürdige Zone exportieren und importieren
Vertrauenswürdigen Zertifikatspeicher des Systems verwenden
Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme
Echtzeitschutz für Dateien
Über den Schutzbereich von Aufgaben und Sicherheitseinstellungen
Vordefinierte Schutzbereiche
Über vordefinierte Sicherheitsstufen
Dateierweiterungen, die von der Komponente Echtzeitschutz für Dateien standardmäßig untersucht werden
Komponente Echtzeitschutz für Dateien konfigurieren
Schutzbereich für die Komponente Echtzeitschutz für Dateien konfigurieren
Sicherheitseinstellungen manuell anpassen
Container untersuchen
Verwendung von KSN
Verwendung von Kaspersky Security Network aktivieren
Status der Verwendung von Kaspersky Security Network
Einschränkungen von Kaspersky Private Security Network
KSN Proxy-Einstellungen

Exploit-Prävention
Modus der Exploit-Prävention
Exploit-Prävention aktivieren und deaktivieren
Schutz des Arbeitsspeichers aktivieren und deaktivieren
Liste der geschützten Prozesse erstellen
Rollback von schädlichen Aktionen
Verhaltensanalyse
Verschlüsselungsschutz für lokale Ordner aktivieren oder deaktivieren
Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern
Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern aktivieren und deaktivieren
Schutzbereich bearbeiten
Vertrauenswürdige Computer für die externe Datenverschlüsselung hinzufügen
Sperrdauer für einen nicht vertrauenswürdigen Computer konfigurieren
Exportieren und Importieren einer Liste der Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern
Schutz vor Netzwerkbedrohungen
Schutz vor Netzwerkbedrohungen aktivieren und konfigurieren
Eine Ausnahme von der Sperrung erstellen
Exportieren und Importieren einer Liste der Ausnahmen für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern
AMSI-Untersuchung
AMSI-Scanner aktivieren und deaktivieren
Einstellungen für den AMSI-Scanner
Kontrolle des Programmstarts
Über die Regeln für die Kontrolle des Programmstarts
Über die Kontrolle der Software-Verteilung
Über den Regelgenerator für die Anwendungsstartkontrolle
Kontrolle des Programmstarts aktivieren und konfigurieren
Konfiguration der Kontrolle für Installationspakete
Regeln der Kontrolle des Programmstarts verwenden
Regeln zur Kontrolle des Programmstarts hinzufügen
Auslösebedingungen für die Regel der Kontrolle des Programmstarts hinzufügen
Ausnahmen für den Gültigkeitsbereich einer Regel für die Kontrolle des Programmstarts hinzufügen
Ausführung aller Programme erlauben
Regeln für die Kontrolle des Programmstarts exportieren
Generieren einer txt-Datei mit einer Auswahl von Kaspersky Security Center-Ereignissen über blockierte Programme
Gruppenaufgabe zum Erstellen von Regeln zur Kontrolle des Programmstarts konfigurieren
Erstellen von Regeln mithilfe einer Gruppenaufgabe des Typs „Erstellen von Regeln zur Kontrolle des Programmstarts“
Gerätekontrolle
Regeln für den Zugriff auf Geräte
Zugriff auf Geräte nach Typ verwalten
Kontrolle von WLAN-Verbindungen
Druckerüberwachung
Kontrolle von Eingabegeräten (HID)
Zugriff auf Mobilgeräte verwalten
Überwachung der Nutzung von Wechseldatenträgern
Zugriff auf Bluetooth-Geräte verwalten

- Unterscheidung der Benutzerzugriffsrechte auf Geräte
- Informationen zum Erstellen von Regeln für die Gerätekontrolle
- Vertrauenswürdige Geräte hinzufügen
- Liste mit vertrauenswürdigen Geräten exportieren und importieren

Firewall
- Über Firewall-Regeln
- Firewall konfigurieren
  - Allgemeine Firewall-Einstellungen konfigurieren
  - Firewall-Regeln erstellen und konfigurieren
  - Firewall-Regeln aktivieren und deaktivieren

Schutz vor modifizierten USB-Geräten

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

Protokollanalyse
- Benutzerdefinierte Regeln hinzufügen
- Vordefinierte Regeln konfigurieren

Untersuchung auf Befehl
- Über Aufgaben zur Untersuchung auf Befehl
- Über den Untersuchungsbereich von Aufgaben und Sicherheitseinstellungen
- Vordefinierte Untersuchungsbereiche
- Untersuchung von Dateien im Online-Speicher
- Über vordefinierte Sicherheitsstufen
- Untersuchung von Wechseldatenträgern
- Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl
- Aufgaben zur Untersuchung auf Befehl verwalten
  - Erstellen einer Aufgabe zur Untersuchung auf Befehl
    - Ausführung einer Aufgabe im Hintergrund zur Untersuchung auf Befehl
    - Registrierung der Ausführung der Untersuchung wichtiger Bereiche
  - Untersuchungsbereich für die Aufgabe „Untersuchung auf Befehl“ konfigurieren
  - Einstellungen für die Aufgabe „Untersuchung auf Befehl“ konfigurieren
  - Untersuchung von Wechseldatenträgern anpassen
  - Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen
  - Sicherheitseinstellungen manuell anpassen
  - Statistik von Aufgaben zur Untersuchung auf Befehl

Datenbanken-Update und Update der Programm-Module für Kaspersky Embedded Systems Security
- Update der Datenbanken und Programm-Module
- Über Update-Aufgaben
- Update-Schemata für die Datenbanken und Module von Kaspersky Embedded Systems Security
- Einstellung von Update-Aufgaben
- SMU-Update der Anwendung
- Sicheres Kopieren der Programm-Datenbanken
- Sicheres Update der Programm-Datenbanken

- Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security
- Statistik zu Update-Aufgaben

Backup-Kopien von Objekten erstellen

- Backup-Kopien von Objekten erstellen. Datenverwaltung
  - Objekte im Backup anzeigen
  - Dateien aus Backup wiederherstellen
  - Dateien aus Backup löschen
  - Möglicherweise infizierte Quarantäneobjekte zur Analyse an Kaspersky einschicken
  - Backup-Einstellungen anpassen
  - Backup-Statistik
- Zugriff auf Netzwerkressourcen blockieren. Blockierte Netzwerksitzungen
  - Liste der blockierten Netzwerksitzungen
  - Liste der blockierten Netzwerksitzungen verwalten

Registrierung von Ereignissen. Berichte in Kaspersky Embedded Systems Security

- Möglichkeiten zur Registrierung der Dienste von Kaspersky Embedded Systems Security
- Einstellungen für Protokolle konfigurieren
  - Ereignisse im Protokoll sortieren
  - Ereignisse im Protokoll filtern
  - Ereignisse aus dem Protokoll löschen
  - Informationen aus dem Protokoll exportieren
- Systemaudit-Protokoll
- Komponenten- und Aufgabenprotokolle
- Ereignisbericht von Kaspersky Embedded Systems Security in der Ereignisanzeige anzeigen
- Über die SIEM-Integration
  - Anpassen der Einstellungen der SIEM-Integration
- Methoden zur Benachrichtigung von Administrator und Benutzer
  - Benachrichtigungen an Administrator und Benutzer anpassen
  - E-Mail-Benachrichtigungen konfigurieren
- Konfigurieren der Interaktion mit dem Administrationsserver

Verwaltung der vollständigen BitLocker-Laufwerkverschlüsselung

- 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

Integration mit Drittherstellersystemen

- Leistungsindikatoren für das Programm Systemmonitor
  - Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden
  - Anzahl der zur Bearbeitung eingereichten Anfragen
  - Anzahl der pro Sekunde verarbeiteten Objekte
  - Anzahl der Elemente in der Warteschlange für infizierte Objekte
  - Gesamtzahl der abgelehnten Anfragen
  - Gesamtzahl der übersprungenen Anfragen
  - Maximale Anzahl der Datenströme des File-Interception-Dispatchers
  - Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security
SNMP-Indikatoren in Kaspersky Embedded Systems Security
Leistungsindikatoren
Indikator für Backup
Allgemeine Indikatoren
Update-Indikatoren
Indikatoren für den Echtzeitschutz für Dateien
Leistungsindikatoren des AMSI-Scanners
SNMP-Traps und ihre Optionen in Kaspersky Embedded Systems Security
Beschreibungen und mögliche Werte der Optionen von SNMP-Traps in Kaspersky Embedded Systems Security
WMI-Integration
Managed Detection and Response
Konfiguration der MDR-Integration
Kaspersky Embedded Systems Security über die Befehlszeile verwalten
APPCONTROL. Regeln für die Kontrolle des Programmstarts importieren
APPCONTROL /CONFIG. Komponente Kontrolle des Programmstarts konfigurieren
APPCONTROL /GENERATE. Erstellen von Regeln für die Kontrolle des Programmstarts
CONFIG. Unterstützung der AM-PPL-Technologie
DEVCONTROL. Regeln für die Gerätekontrolle importieren
DUMP. Speicherabbilder aufzeichnen
EXITPOLICY. Deaktivieren der Richtlinie auf dem Gerät
EXPORT. Programmeinstellungen exportieren
FBRESET. iSwift-Datenbank leeren
FIM /BASELINE. Baseline-Überwachung der Systemintegrität
HELP. Anzeigen der Hilfe zu Befehlen
IMPORT. Programmeinstellungen importieren
KSN. Verwenden von KSN/KPSN
LICENSE. Aktivierung des Programms
MDR. Konfiguration der Integration von Managed Detection and Response
OMSINFO. Erstellen einer JSON-Datei mit Informationen über das Programm
Kennwort. Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security
PATCHCOMPATIBILITYRESET. Entfernen eines Patches aus der Liste der inkompatiblen Patches
REMOTEACCESS. Verwalten der Einstellungen für die Remote-Verbindung der Programmkonsole
RESETMDRMACHINEID. Zurücksetzen der Geräte-ID
ROLLBACK. Rollback des letzten Updates
RTP. Echtzeitschutz für Dateien
SCAN. Untersuchung auf Befehl
SCANCRITICAL. Untersuchung wichtiger Bereiche
SERVERBINDINGDISABLE. Schutz der Verbindung zum Administrationsserver deaktivieren
START. Starten des Programmdienstes
STARTPOLICY. Richtlinie aktivieren
STOP. Beenden des Programmdienstes
AUFGABE. Verwalten von Aufgaben
TRACE. Protokollierung der Anwendungsausführung
UPDATE. Update der Datenbanken und Programm-Module

Kontaktaufnahme mit dem Technischen Support
Wie Sie technischen Support erhalten
Technischer Support über Kaspersky CompanyAccount
Bereitstellung erweiterter Diagnoseinformationen für die Spezialisten des Technischen Supports
Protokollierung der Anwendungsausführung
Über die Zusammensetzung und Speicherung von Protokolldateien
Speicherabbilder aufzeichnen
Schutz von Dump- und Protokolldateien
Betriebssystemdaten abrufen (Kaspersky Get System Info)
Informationsquellen über Kaspersky Embedded Systems Security
Anhänge
Dateierweiterungen für die schnelle Untersuchung
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
Einhaltung der Gesetzgebung der Europäischen Union (DSGVO)
Informationen über den Code von Drittherstellern
Markenrechtliche Hinweise

Kaspersky Embedded Systems Security für Windows

Kaspersky Embedded Systems Security für Windows (im Folgenden auch „Kaspersky Embedded Systems Security“ genannt) schützt Computer und andere eingebettete Systeme unter Microsoft® Windows® (im Folgenden auch als geschützte Geräte bezeichnet) vor Viren und anderen Computerbedrohungen. Als Benutzer von Kaspersky Embedded Systems Security gelten die Netzwerkadministratoren von Unternehmen und Mitarbeiter, die für den Antiviren-Schutz des Unternehmensnetzwerks zuständig sind.

Die Anwendung ist nicht für den Einsatz im Rahmen technologischer Prozesse vorgesehen, die automatisierte Steuerungssysteme beinhalten. Für den Schutz von Geräten in derartigen Systemen empfehlen wir die Anwendung Kaspersky Industrial CyberSecurity for Nodes zu verwenden.

Sie können Kaspersky Embedded Systems Security auf verschiedenen eingebetteten Systemen unter Windows installieren, darunter folgende Gerätetypen:

- Geldautomaten (ATM)
- Verkaufsorte

Kaspersky Embedded Systems Security kann auf folgende Arten verwaltet werden:

- Über die Programmkonsole, die auf einem geschützten Gerät mit Kaspersky Embedded Systems Security oder auf einem anderen Gerät installiert ist.
- Mithilfe eines Befehls in der Befehlszeile
- Über die Kaspersky Security Center Verwaltungskonsole

Sie können das Programm Kaspersky Security Center verwenden, das der zentralisierten Verwaltung des Schutzes mehrerer geschützter Geräte dient, auf denen Kaspersky Embedded Systems Security ausgeführt wird.

Sie können die Leistungsindikatoren von Kaspersky Embedded Systems Security für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps analysieren.

Komponenten und Funktionen von Kaspersky Embedded Systems Security

Im Lieferumfang des Programms sind folgende Komponenten enthalten:

- **Echtzeitschutz für Dateien**. Kaspersky Embedded Systems Security untersucht Objekte, wenn darauf zugegriffen wird. Kaspersky Embedded Systems Security untersucht die folgenden Objekte:
  - Dateien
  - Alternative Datenströme der Dateisysteme (NTFS-Streams)
  - Master Boot Records und Bootsektoren von lokalen Festplatten und Wechseldatenträgern

- **Untersuchung auf Befehl**. Kaspersky Embedded Systems Security überprüft den angegebenen Bereich einmalig auf Viren und andere Bedrohungen der Computersicherheit. Die Anwendung scannt Dateien, RAM und Autorun-Objekte auf einem geschützten Gerät.

- **Kontrolle des Programmstarts**. Die Komponente überwacht die Versuche des Benutzers, Programme zu starten, und reguliert den Start von Programmen auf dem geschützten Gerät.

- **Gerätekontrolle**. Die Komponente ermöglicht eine Kontrolle der Registrierung und der Verwendung von externen Geräten, um das Gerät vor Bedrohungen für die Computersicherheit zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können.

- **Firewall**. Abhängig vom Modus überwacht die Komponente die Filterung des Datenverkehrs durch die Windows-Firewall; zeichnet nur Ereignisse über die Netzwerkaktivität des geschützten Computers im Komponentenprotokoll auf; oder filtert den Netzwerkverkehr gemäß den Firewall-Einstellungen.

- **Überwachung der Datei-Integrität**. Kaspersky Embedded Systems Security erkennt Änderungen in Dateien im in den Aufgabeneinstellungen festgelegten Überwachungsbereich. Diese Änderungen können auf eine Sicherheitsverletzung auf dem geschützten Gerät hinweisen.

- **Protokollanalyse**. Diese Komponente führt eine Integritätsprüfung des geschützten Mittwochs auf Grundlage der Ergebnisse der Protokollanalyse von Windows-Ereignissen aus.

Das Programm verfügt über folgenden Funktionen:

- **Update**. Für den Download von Updates der Programm-Datenbanken und Programm-Module verwendet Kaspersky Embedded Systems Security die FTP- oder HTTP-Update-Server von Kaspersky, den Kaspersky Security Center Administrationsserver oder andere Update-Quellen.

- **Quarantäne**. Objekte, die von Kaspersky Embedded Systems Security als möglicherweise infiziert eingestuft wurden, werden unter Quarantäne gestellt, d. h., die Objekte werden von ihrem ursprünglichen Speicherort in den Ordner *Quarantäne* verschoben. Aus Sicherheitsgründen werden Objekte im Quarantäneordner in verschlüsselter Form gespeichert.

- **Backup**. Bevor ein Objekt mit dem Status *Infiziert* desinfiziert oder gelöscht wird, speichert Kaspersky Embedded Systems Security eine verschlüsselte Kopie im *Backup*.

- **Benachrichtigungen an den Administrator und die Benutzer**. Sie können die Anwendung so konfigurieren, dass sie den Administrator und die Benutzer, die auf das geschützte Gerät zugreifen, über die Ereignisse informiert, die mit der Ausführung von Kaspersky Embedded Systems Security und dem Status des Virenschutzes auf dem Gerät in Zusammenhang stehen.

- **Import und Export von Einstellungen**. Sie können die Einstellungen von Kaspersky Embedded Systems Security in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Embedded Systems Security importieren. In einer Konfigurationsdatei können entweder alle Einstellungen des Programms oder nur die Einstellungen bestimmter Programmkomponenten gespeichert werden.

- **Verwendung von Vorlagen**. Sie können die Sicherheitseinstellungen eines Knotens in der Struktur oder in der Liste der Dateiressourcen des geschützten Geräts manuell konfigurieren und die angepassten Einstellungswerte in einer Vorlage für Einstellungen speichern. Sie können diese Vorlage später beim Angeben der Sicherheitseinstellungen anderer Knoten in den Schutz- und Untersuchungsaufgaben von Kaspersky Embedded Systems Security verwenden.

- **Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security**. Sie können die Rechte für die Verwaltung von Kaspersky Embedded Systems Security und der Windows-Dienste, die das Programm registriert, für Benutzer und Benutzergruppen konfigurieren.

- **Protokollieren von Ereignissen im Windows-Ereignisprotokoll**. Kaspersky Embedded Systems Security protokolliert Informationen über die Einstellungen von Softwarekomponenten, den aktuellen Aufgabenstatus, Ereignisse, die bei der Aufgabenausführung eintreten, Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security sowie Informationen, die für die Fehlerdiagnose in Kaspersky Embedded Systems Security erforderlich sind.

- **Vertrauenswürdige Zone**. Sie können eine Liste mit Ausnahmen aus dem Schutzbereich bzw. Untersuchungsbereich anlegen, die Kaspersky Embedded Systems Security bei der Ausführung der Aufgaben zur Untersuchung auf Befehl und zum Echtzeit-Computerschutz anwendet.

- **Exploit-Prävention**. Sie können den Prozessspeicher vor Exploits schützen, indem Sie einen Schutzagenten in den Prozess injizieren.

Die Update-Funktionalität (einschließlich der Bereitstellung von Antiviren-Signatur-Updates und Codebase-Updates) sowie die KSN-Funktionalität sind in den USA möglicherweise nicht in der Software verfügbar.

Neuerungen

Update 4.1

Kaspersky Embedded Systems Security 4.1 für Windows bietet die folgenden neuen Funktionen und Verbesserungen:

- Die Verwaltung der Windows-BitLocker-Verschlüsselung ist jetzt verfügbar. Das Programm unterstützt die Verwendung von Kaspersky Security Center, um die Festplatten geschützter Geräte zu ver- und entschlüsseln und den Zugriff auf verschlüsselte Laufwerke wiederherzustellen.

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

- Sie können jetzt Aufgaben zur Untersuchung auf Befehl für ein ausgewähltes Zeitintervall anhalten, beispielsweise um routinemäßige Wartungsarbeiten durchzuführen.

- Die Ereignisse „*Vorgänge mit dem Gerät sind bis zum Start von Kaspersky Embedded Systems Security verboten*“ und „*Verbindung mit dem Gerät ist bis zum Start von Kaspersky Embedded Systems Security blockiert*“ sind jetzt verfügbar. Wenn das Gerät vor dem Start des Programms gesperrt wird, wird jetzt das entsprechende Ereignis generiert und an den Administrationsserver gesendet.

- Die folgenden Betriebssysteme werden jetzt unterstützt:

  - Windows 11 26H2

  - Windows 11 IoT 25H2

- Die Leistung des Festplatten-Subsystems auf dem geschützten Gerät wurde durch die Verringerung der Anzahl der E/A-Vorgänge optimiert.

- Bei der Entwicklung dieser Version von Kaspersky Embedded Systems Security haben wir die Änderungen der folgenden privaten Patches berücksichtigt: PF23074, PF23088, PF23089, PF23099, PF23102, PF23104, PF23105.

Update 4.0

Kaspersky Embedded Systems Security 4.0 bietet die folgenden Funktionen und Verbesserungen:

- Stark modernisierte Benutzeroberfläche der Anwendungskonsole und der Plug-ins für die Verwaltung des Programms mit Kaspersky Security Center.
- Unterstützung für Windows 11 24H2.
- Sie können jetzt den Port ändern, den die Anwendungskonsole für die Verbindung mit einem Computer verwendet, auf dem das Programm installiert ist.
- In der *vertrauenswürdigen Zone* können Sie:
  - Vertrauenswürdige Prozesse genauer konfigurieren.
  - Den vertrauenswürdigen Zertifikatspeicher verwenden.
- Neue Einstellungen für Benutzer- und Gruppenrechte zur Verwaltung des Programms.
- Neue *Anti-Rootkit*-Komponente. Standardmäßig ist die Komponente aktiviert, wenn der *Echtzeitschutz für Dateien* aktiviert ist. Sie können die Komponente während der Installation des Programms mithilfe der Aufgabe *Programmkomponenten von Kaspersky Embedded Systems Security ändern* oder in den Eigenschaften des Installationspakets des Programms deaktivieren.
- In den Einstellungen der *Exploit-Prävention* kann das Programm jetzt geschützte Prozesse automatisch erkennen.
- Neue Komponente zum *Rollback von schädlichen Aktionen*.
- Die Komponente Schutz vor Netzwerkbedrohungen kann den Netzwerkverkehr überwachen, um Port-Scans und Netzwerkanforderungen, die sehr intensiv sind, zu erkennen.
- Das Programm ist jetzt mit der Windows-Firewall kompatibel. Sie müssen die Windows-Firewall nicht mehr entfernen, um das Programm zu installieren.
- Die Komponente *Verhaltensanalyse* überwacht sowohl freigegebene Ordner als auch lokale Ordner.
- Überarbeitete Komponente zur *Kontrolle des Programmstarts*:
  - Wesentliche Änderungen in der Struktur der Komponenteneinstellungen.
  - Um die Auslösebedingungen und Ausnahmen für die Kontrolle des Programmstarts festzulegen, können Sie jetzt den Laufwerkstyp, die KL-Kategorien und die KSN-Gruppen verwenden.
- Überarbeitete Komponente zur *Gerätekontrolle*:
  - Standardmäßig ist die Komponente *Gerätekontrolle* so konfiguriert, dass der Anschluss aller Geräte möglich ist.
  - *WLAN-Kontrolle* ist keine separate Komponente mehr und gehört jetzt zur Gerätekontrolle.

- Die Möglichkeit, angeschlossene Geräte abhängig vom Verbindungsbus zu kontrollieren, wurde hinzugefügt.

- Die Migration der Einstellungen für den Zugriff auf Wechseldatenträger beim Upgrade von älteren Programmversionen auf Version 4.0 wurde hinzugefügt.

- Die Komponente *Firewall-Verwaltung* wurde zur Komponente *Firewall* überarbeitet, die neben ihrer Funktion als Schnittstelle zur Windows-Firewall jetzt auch als Firewall fungiert.

- Die Funktionalität der Komponenten *Überwachung der Datei-Integrität* und *Überwachung des Registrierungszugriffs* wurde in die neue Komponente *Überwachung der Systemintegrität* integriert. Diese Verbesserung ermöglicht es Ihnen, Änderungen im Dateisystem und in der Windows-Registrierung effizient zu verfolgen und so den Schutz vor unbefugten Datenänderungen zu erhöhen.

- Das Programm unterstützt die Zeitplanung für einzelne Komponenten nicht. Aktivierte Komponenten werden weiterhin ausgeführt, während das Programm ausgeführt wird.

- Kaspersky Security Center Windows 15.1 wird jetzt unterstützt.

- Hinzugefügte Gruppenaufgaben:

  - *Schutz der Verbindung zum Administrationsserver*

  - *Auswahl der Komponenten von Kaspersky Embedded Systems Security ändern*

  - *Überwachung der Baseline für Systemintegrität* anstelle von *Überwachung der Baseline-Integrität*

  - *Update* anstelle von *Update-Verteilung*, *Update der Programm-Datenbanken* und *Update der Programm-Module*

  - *Update-Rollback* anstelle von *Rollback des Updates der Programm-Datenbanken*

  - *Schlüssel entfernen*

- Das Programm überprüft die Konfiguration der Kontrollkomponenten, bevor die Einstellungen gespeichert werden. Die Überprüfung wurde für die Komponenten Kontrolle des Programmstarts, 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. Beispiel: Wenn Sie für die Kontrolle des Programmstarts 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.

- Jetzt ist es möglich, automatisch Erlaubnisregeln für die Kontrolle des Programmstarts zu erstellen und diese Regeln in eine Datei zu exportieren. Starten Sie dazu die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* und aktivieren Sie die automatische Erstellung von auf laufenden Programmen basierenden Erlaubnisregeln sowie den Export von Erlaubnisregeln. Sie können die erhaltene Datei verwenden, um die auf dem Gerät installierte Software zu inventarisieren.

- Neue Komponente: *Schutz vor modifizierten USB-Geräten*. Die Komponente „Schutz vor BadUSB-Angriffen" verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden. Wenn ein USB-Gerät, das vom Betriebssystem als Tastatur erkannt wird, an den Computer angeschlossen wird, fordert das Programm den Benutzer auf, auf dieser Tastatur zu tippen, um die sie zu autorisieren.

- Der *Indikator „Sicherheitsstufe"* wurde hinzugefügt. Der Indikator für die Sicherheitsstufe wird oben im Eigenschaftenfenster der Richtlinie angezeigt und gib an, inwieweit die Sicherheitseinstellungen mit den Empfehlungen von Kaspersky Lab übereinstimmen. Mithilfe des Indikators „Sicherheitsstufe" können Sie die Richtlinie schnell konfigurieren und die erforderlichen Schutzkomponenten aktivieren.

Behobene Probleme

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

Liste der in Version 4.1 behobenen Probleme

Kennzeichnung	Problembeschreibung
9986614	In der Web Console und der Kaspersky Security Center Verwaltungskonsole kann keine Liste vertrauenswürdiger Geräte aus einer TXT-Datei importiert werden, die eine Auswahl von Kaspersky Security Center-Ereignissen zu gesperrten Geräten enthält und aus der Web Console exportiert wurde.
10700703	Auf der Benutzeroberfläche der Komponenten Überwachung der Systemintegrität, Vertrauenswürdige Zone, Kontrolle des Programmstarts und Gerätekontrolle ist nicht sofort ersichtlich, wie Listenelemente ausgewählt werden müssen, um den Befehl **Ausgewählte exportieren** auszuführen. Die Beschreibung in der Hilfe zum Programm wurde erweitert.
10720231	Der Zähler für vertrauenswürdige Geräte wird im Abschnitt **Gerätekontrolle** der Richtlinie in der Kaspersky Security Center Verwaltungskonsole nicht angezeigt.
10729552	Ereignisse zu Dateivorgängen auf Wechseldatenträgern werden nicht generiert, obwohl die Protokollierung solcher Ereignisse aktiviert ist.
10752491	In der Web Console kann keine Liste vertrauenswürdiger Geräte aus einer TXT-Datei importiert werden, die eine Auswahl von Kaspersky Security Center-Ereignissen zu gesperrten Geräten enthält und aus der Verwaltungskonsole exportiert wurde.

Lieferumfang

Der Lieferumfang umfasst ein Begrüßungsprogramm, von dem aus folgende Aktionen möglich sind:

- Start des Setup-Assistenten für Kaspersky Embedded Systems Security.
- Start des Setup-Assistenten für die Konsole von Kaspersky Embedded Systems Security.
- Start des Kaspersky Virus Removal Tools.
- Lesen von Informationen über diese Version von Kaspersky Embedded Systems Security.
- Öffnen der Hilfe zu Kaspersky Embedded Systems Security 4.1.
- Zur Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky wechseln.
- Besuchen der Kaspersky-Website.
- Besuchen der Website des Technischen Supports.

Die Dateien aus dem Lieferumfang befinden sich je nach ihrem Zweck in verschiedenen Ordnern (s. Tabelle unten).

Dateien im Lieferumfang von Kaspersky Embedded Systems Security

Datei	Ziel
autorun.inf	Autostart-Datei für den Setup-Assistenten von Kaspersky Embedded Systems Security bei der Programm-Installation von einem Wechseldatenträger.
setupui.exe	Startdatei des Begrüßungsbildschirm des Programms.
ess_win.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation des Programms über Kaspersky Security Center.
\console\esstools.msi	Installationspaket für das Windows-Installationsprogramm; installiert die Konsole für Kaspersky Embedded Systems Security Console auf den geschützten Geräten.
\console\setup_esstool.exe	Datei, die den Assistenten zur Installation der Konsole von Kaspersky Embedded Systems Security für Windows startet. Die Installationspaketdatei esstools.msi wird mit den im Assistenten festgelegten Installationseinstellungen gestartet.
\console\license.txt	Textdatei mit dem Endbenutzer-Lizenzvertrag und der Datenschutzerklärung für die Management-Konsole von Kaspersky Embedded Systems Security.
\exec\bases.cab	Archiv der zum Zeitpunkt der Veröffentlichung des Programms aktuellen Antiviren-Datenbanken.
\exec\cleaner_v2.cab \exec\cleanerapi_v2.cab	Dateien für die Deinstallation von inkompatibler Software.
\exec\ess.cab	Dateien für die grafische Oberfläche der Anwendung.
\exec\ess_win.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation des Programms über Kaspersky Security Center.
\exec\ess_win.msi	Installationspaket für das Windows-Installationsprogramm: Es installiert Kaspersky Embedded Systems Security auf dem geschützten Gerät.
\exec\incompatible.txt	Kaspersky übernimmt keine Garantie für die Kompatibilität von Kaspersky Embedded Systems Security mit den in der Datei aufgeführten Programmen.
\exec\installer.ini	Datei, die interne Parameter des Programmpakets enthält.
\exec\klcfginst.msi	Installationsprogramm für das Verwaltungs-Plug-in von Kaspersky Embedded Systems Security, verfügbar über Kaspersky Security Center. Installieren Sie das Verwaltungs-Plug-in auf allen geschützten Geräten, auf denen die Kaspersky Security Center-Verwaltungskonsole installiert ist, wenn Sie diese für die Verwaltung von Kaspersky Embedded Systems Security verwenden möchten.
\exec\ksn_en.txt	Datei mit dem Text der KSN-Erklärung.
\exec\license.txt	Textdatei des Endbenutzer-Lizenzvertrags und der Datenschutzerklärung für Kaspersky Embedded Systems Security
\exec\package.kcat	Datei mit den Signaturen der Dateien des Verteilungspakets.
\exec\setup_ess.exe	Datei, die den Assistenten zur Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät startet; sie startet die Installationspaketdatei „ess_win.msi“ mit den Installationseinstellungen, die im Assistenten angegeben wurden.
\kvrt\KVRT.exe	Installationsprogramm für Kaspersky Virus Removal Tool.
\product_long_term\cleaner_v2.cab \product_long_term\cleanerapi_v2.cab	Dateien für die Deinstallation von inkompatibler Software.
\product_long_term\ess.cab	Dateien für die grafische Oberfläche der Anwendung.
\product_long_term\ess_win.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation des Programms über Kaspersky Security Center.
\product_long_term\ess_win.msi	Installationspaket für Windows Installer. Es installiert Kaspersky Embedded Systems Security für Windows mit der Konfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** auf dem geschützten Gerät.
\product_long_term\incompatible.txt	Kaspersky übernimmt keine Garantie für die Kompatibilität von Kaspersky Embedded Systems Security mit den in der Datei aufgeführten Programmen.
\product_long_term\installer.ini	Datei, die interne Parameter des Programmpakets enthält.
\product_long_term\klcfginst.exe	Installationsprogramm für das Verwaltungs-Plug-in von Kaspersky Embedded Systems Security, verfügbar über Kaspersky Security Center. Installieren Sie das Verwaltungs-Plug-in auf allen geschützten Geräten, auf denen die Kaspersky Security Center-Verwaltungskonsole installiert ist, wenn Sie diese für die Verwaltung von Kaspersky Embedded Systems Security verwenden möchten.
\product_long_term\ksn_en.txt	Datei mit dem Text der KSN-Erklärung in russischer Sprache.

Datei	Ziel
\product_long_term\license.txt	Textdatei des Endbenutzer-Lizenzvertrags und der Datenschutzerklärung für Kaspersky Embedded Systems Security
\product_long_term\package.kcat	Datei mit den Signaturen der Dateien des Verteilungspakets.
\product_long_term\setup_ess.exe	Datei, die den Assistenten zur Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät startet; sie startet die Installationspaketdatei „ess_win.msi" mit den Installationseinstellungen, die im Assistenten angegeben wurden.
\setup\images	Ordner mit den Startdateien für den Begrüßungsbildschirm des Programms.
\setup\setup.hta	Startdatei des Begrüßungsbildschirm des Programms.
\setup\SETUP_STRINGS.JS	Datei mit Ressourcen im String-Format für das Programm.

Die Dateien des Verteilungs-Kits können von der Installations-CD gestartet werden. Wenn Sie die Dateien des Verteilungspakets zuvor auf das lokale Laufwerk kopiert haben, stellen Sie sicher, dass die Struktur der Verteilungspaketdateien nicht verändert wurde.

Hard- und Softwarevoraussetzungen

Softwarevoraussetzungen für das geschützte Gerät

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.

Für die ordnungsgemäße Installation und den ordnungsgemäßen Betrieb des Programms auf einem geschützten Gerät mit Microsoft Windows XP ist Windows Installer 3.1 erforderlich.

Um Kaspersky Embedded Systems Security auf geschützten Geräten mit eingebetteten Betriebssystemen zu installieren und zu verwenden, ist die Komponente „Filter Manager" (Filter Manager) erforderlich.

Für die korrekte Funktion von Kaspersky Embedded Systems Security ist die Unterstützung von SHA-2 in Microsoft Windows erforderlich. Ausführliche Informationen finden Sie in der Wissensdatenbank auf der Website des Technischen Supports.

Sie können Kaspersky Embedded Systems Security auf einem Gerät installieren, das unter einem der folgenden 32- oder 64-Bit-Betriebssysteme von Microsoft Windows läuft:

Workstations:

- Windows XP Professional SP2 (32-Bit / 64-Bit)
- Windows XP Professional SP3 (32-Bit)

- Windows Vista SP2 (32-Bit / 64-Bit)
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate (32-Bit / 64-Bit)
- Windows 8 Pro / Enterprise (32-Bit / 64-Bit)
- Windows 8.1 Pro / Enterprise (32-Bit / 64-Bit)
- Windows 10 TH1 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 TH2 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 RS1 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 RS2 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 RS3 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 RS4 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 RS5 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 RS6 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 19H2 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 20H1 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 20H2 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 21H1 Home / Pro / Pro für Workstation / Education / Enterprise (32-Bit / 64-Bit)
- Windows 10 21H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 10 22H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 11 21H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 11 22H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 11 23H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 11 24H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 11 25H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)
- Windows 11 26H2 Home / Pro / Pro für Workstation / Education / Enterprise (64-Bit)

Server-Betriebssysteme:

- Windows Server 2003 SP1 Standard / Enterprise (32-Bit / 64-Bit)
- Windows Server 2003 SP2 Standard / Enterprise (32-Bit / 64-Bit)
- Windows Server 2003 R2 SP2 Standard / Enterprise (64-Bit)

- Windows Server 2008 SP2 Standard / Enterprise (32-Bit / 64-Bit)
- Windows Server 2008 R2 SP2 Foundation / Standard / Enterprise (64-Bit)

Eingebettete Systeme:

- Windows XP Embedded Service Pack 3 (32-Bit)
- Windows Embedded POSReady 7 (32-Bit / 64-Bit)
- Windows Embedded Standard 7 Service Pack 1 (32-Bit / 64-Bit)
- Windows Embedded 8 Standard (32-Bit / 64-Bit)
- Windows Embedded 8.1 Industry Pro (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 1507 (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 1607 (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 1803 (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 1809 (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 1909 (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 21H2 (32-Bit / 64-Bit)
- Windows 10 IoT Enterprise Version 22H2 (32-Bit / 64-Bit)
- Windows 11 IoT Enterprise Version 21H2 (64-Bit)
- Windows 11 IoT Enterprise Version 22H2 (64-Bit)
- Windows 11 IoT Enterprise Version 23H2 (64-Bit)
- Windows 11 IoT Enterprise Version 24H2 (64-Bit)
- Windows 11 IoT Enterprise Version 25H2 (64-Bit)

Hardwarevoraussetzungen für das geschützte Gerät

Hardwarevoraussetzungen für das geschützte Gerät

Typ des Betriebssystems	Name des Betriebssystems	Minimale Voraussetzungen	Empfohlene Voraussetzungen
Workstations	Windows XP x86 / x64	• CPU: Single Core-Prozessor Pentium III mit 1.4 GHz (x32), Pentium IV (x64) • RAM: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 256 MB • Für die Installation aller Programmkomponenten: 512 MB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB • Für die Installation aller Programmkomponenten: 2 GB	• CPU: Quad Core mit 2,4 GHz • RAM: 2 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB • Für die Installation aller Programmkomponenten: 4 GB
	Windows 7 / 8 / 10 x86	• CPU: Single Core-Prozessor Pentium III mit 1.4 GHz (x32), Pentium IV (x64) • RAM: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 256 MB • Für die Installation aller Programmkomponenten: 1 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB • Für die Installation aller Programmkomponenten: 2 GB	• CPU: Quad Core mit 2,4 GHz • RAM: 2 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB • Für die Installation aller Programmkomponenten: 4 GB
	Windows 7 / 8 / 10 / 11 x64	• CPU: Single Core-Prozessor Pentium IV mit 1.4 GHz (x64) • RAM: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 256 MB • Für die Installation aller Programmkomponenten: 1 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB • Für die Installation aller Programmkomponenten: 2 GB	• CPU: Quad Core mit 2,4 GHz • RAM: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB • Für die Installation aller Programmkomponenten: 4 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB • Für die Installation aller Programmkomponenten: 4 GB

Typ des Betriebssystems	Name des Betriebssystems	Minimale Voraussetzungen	Empfohlene Voraussetzungen
Embedded	Windows XP Embedded	• CPU: Single Core-Prozessor Pentium III mit 1.4 GHz (x32), Pentium IV (x64) • RAM: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 256 MB • Für die Installation aller Programmkomponenten: 512 MB Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB • Für die Installation aller Programmkomponenten: 2 GB	• CPU: Quad Core mit 2,4 GHz • RAM: 2 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB • Für die Installation aller Programmkomponenten: 4 GB
	Windows 7 / 8 Embedded Windows 10 / 11 IoT	• CPU: Single Core-Prozessor Pentium IV mit 1.4 GHz (x64) • RAM: 256 MB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB • Für die Installation aller Programmkomponenten: 2 GB	• CPU: Quad Core mit 2,4 GHz • RAM: 2 GB • Freier Platz auf der Festplatte: • Nur für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB • Für die Installation aller Programmkomponenten: 4 GB

Unterstützte Versionen von Kaspersky Security Center

Kaspersky Embedded Systems Security ist mit den folgenden Versionen von Kaspersky Security Center kompatibel:

- Kaspersky Security Center Linux-Versionen 14.2, 15, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2, 16.3, 17.0. Kaspersky Embedded Systems Security kann über die Kaspersky Security Center Web Console verwaltet werden.
- Kaspersky Security Center Windows-Versionen 14.2, 15.1. Kaspersky Embedded Systems Security kann über die Kaspersky Security Center-Verwaltungskonsole und über die Kaspersky Security Center Web Console verwaltet werden.
- Kaspersky Security Center Windows-Versionen 10.5, 11. Kaspersky Embedded Systems Security, das auf Geräten mit dem Betriebssystem Microsoft Windows XP SP2 installiert ist, kann über die Kaspersky Security Center Verwaltungskonsole und die Kaspersky Security Center Web Console verwaltet werden.

Um Kaspersky Embedded Systems Security über Kaspersky Security Center zu verwalten, ist der Administrationsagent von Kaspersky Security Center erforderlich.

Der Administrationsagent von Kaspersky Security Center ist nicht im Lieferumfang von Kaspersky Embedded Systems Security enthalten. Sie können ihn auf der Seite zum Herunterladen von Programmen im Abschnitt **Kaspersky Security Center** herunterladen.

Funktionale Anforderungen und Einschränkungen

In diesem Abschnitt werden die zusätzlichen funktionalen Anforderungen und vorhandenen Einschränkungen der Komponenten von Kaspersky Embedded Systems Security beschrieben.

Programm installieren und deinstallieren

- Für die korrekte Funktion von Kaspersky Embedded Systems Security ist die Unterstützung von SHA-2 in Microsoft Windows erforderlich.
- Bei der Installation des Programms kann eine Warnung auf dem Bildschirm erscheinen, wenn der angegebene Pfad zum Installationsordner von Kaspersky Embedded Systems Security mehr als 150 Zeichen enthält. Die Warnung hat keinen Einfluss auf den Installationsprozess: Sie können Kaspersky Embedded Systems Security installieren und ausführen.
- Wenn Sie die Komponente zur Unterstützung des SNMP-Protokolls installieren möchten, müssen Sie den SNMP-Dienst nochmals neu starten, falls er bereits ausgeführt wird.
- Wenn Sie Kaspersky Embedded Systems Security auf einem Gerät mit einem eingebetteten Betriebssystem installieren und ausführen möchten, müssen Sie die Komponente Filter Manager installieren.
- Sie können die Verwaltungstools nicht über Microsoft Active Directory®-Gruppenrichtlinien installieren.
- Wenn Sie den Knoten "Antiviren-Schutz" aus der Liste der installierten Programmkomponenten ausschließen, verschwindet dieser Knoten nach Abschluss der Installation aus der Liste der verfügbaren Komponenten. Wenn Sie die Komponenten des Knotens "Antiviren-Schutz" installieren möchten, müssen Sie den Installationsassistenten aus dem Installationspaket starten, da das Installationspaket eine vollständige Komponentenliste enthält.
- Wenn die Administrationskonsole für Kaspersky Embedded Systems Security installiert ist, kann der Installationsassistent zum Neustart des Computers auffordern. Ein Neustart ist in diesem Fall nicht obligatorisch. Es ist ausreichend, die Sitzung des Benutzers, der die Verwaltungskonsole installiert hat, zu beenden und sich erneut am System anzumelden.
- Wenn Sie das Programm auf einem Gerät mit Windows XP oder Windows Vista installieren, müssen Sie möglicherweise das Zertifikat DigiCert Assured ID Root CA installieren, damit die Treibersignaturen überprüft werden können. Falls erforderlich, wird dieses Zertifikat automatisch aus dem Installationspaket des Programms im vertrauenswürdigen Stammzertifikatspeicher des Betriebssystems installiert.
- Wenn Sie das Programm auf Geräten mit Windows XP oder Windows Vista installieren, müssen Sie überprüfen, ob DigiCert High Assurance EV Root CA. vorhanden ist.

  Wenn dieses Stammzertifikat nicht installiert ist, funktioniert das Programm möglicherweise nicht ordnungsgemäß. Es wird empfohlen, das Zertifikat so bald wie möglich zu installieren.

- Die Installation des Programms wird mit einem Fehler beendet, wenn der Pfad des Installationsordners mindestens mit dem Pfad eines der folgenden Ordner übereinstimmt: Ordner für Programm-Datenbanken, Backup-Ordner, Ordner für die Wiederherstellung von Objekten aus der Quarantäne, Ordner für temporäre Dateien.

- Wenn Sie Kaspersky Embedded Systems 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.

Überwachung der Systemintegrität

Standardmäßig werden Änderungen an Systemordnern oder an Bereinigungsdateien des Dateisystems nicht von der Komponente „Überwachung der Systemintegrität“ überwacht. Dadurch wird eine Überladung der Aufgabenberichte vermieden, die durch Informationen über durch im Betriebssystem regelmäßig ausgeführte Dateiänderungen entstehen könnte. Sie können solche Ordner nicht zum Überwachungsbereich hinzufügen.

Die folgenden Ordner und Dateien werden aus dem Überwachungsbereich ausgeschlossen:

- NTFS Housekeeping-Dateien mit Datei-ID zwischen 0 und 33
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\

- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\Windows\TaskScheduler\

Das Programm schließt Verzeichnisse der obersten Ebene aus.

Die Komponente überwacht keine Dateiänderungen, die das ReFS/NTFS-Dateisystem umgehen (Dateiänderungen über BIOS, LiveCD und andere).

Firewall

- Sie müssen mehr als eine Adresse angeben. Andernfalls kann IPv6 nicht verwendet werden.
- Die vorkonfigurierten Regeln der Firewall unterstützen grundlegende Interaktionsszenarien zwischen den geschützten Geräten und dem Administrationsserver. Um alle Funktionen von Kaspersky Security Center zu verwenden, müssen Sie Portregeln konfigurieren. Informationen über Portnummern, Protokolle und deren Funktionen finden Sie in der Wissensdatenbank von Kaspersky Security Center.
- Nachdem das Programm installiert ist und die Firewall-Regeln konfiguriert wurden, überwacht das Programm die Änderungen an Windows-Firewall-Regeln und Regelgruppen, wenn die Komponente Firewall ausgeführt wird. Um den Status zu aktualisieren und die erforderlichen Windows-Firewall-Regeln hinzuzufügen, starten Sie die Komponente Firewall neu.
- Wenn Sie die Komponente Firewall starten, werden die Verbotsregeln und die Regeln zur Kontrolle des ausgehenden Datenverkehrs automatisch aus den Einstellungen der Windows-Firewall entfernt.
- Die Zeichen `*` und `?` sind in Programmpfaden und im Namen einer Firewall-Regel für Programme nicht zulässig.
- Wenn der Modus *Status der Windows-Firewall überwachen* ausgewählt ist, wird in den Windows-Firewalleinstellungen (**Einstellungen → Update und Sicherheit → Windows-Sicherheit → Firewall & Netzwerkschutz**) angezeigt, dass die Firewall von Kaspersky Embedded Systems Security deaktiviert ist. Wenn Sie auf die Schaltfläche zum Aktivieren der Firewall klicken, ändert sich ihr Funktionsmodus zu *Blockieren*.
- Wenn auf Computern unter Windows 7 und Windows Server 2008 R2 die Firewall-Regeln für den TermService-Dienst auf Basis von Dienstnamen konfiguriert wurden, wird der Zugriff über RDP nicht beschränkt.
- Wenn die Firewall im Modus **Blockieren** ausgeführt wird, verhindert das Programm, dass eine IP-Adresse vom DHCP-Server abgerufen wird. Um eine IP-Adresse abzurufen, konfigurieren Sie die Firewall so, dass der Systemprozess svchost.exe zugelassen wird.

Einschränkungen für veraltete Windows-Versionen

- In der Version Windows XP SP2 ist es nicht möglich, Remote-Geräte zu blockieren und die Einstellungen für die Liste der blockierten Netzwerksitzungen zu konfigurieren. In dieser Windows-Version ist das Kontrollkästchen **Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen** deaktiviert.

- Installation von Kaspersky Embedded Systems Security:

  - Auf Computern mit Windows XP SP2 Professional (32-Bit/64-Bit), Windows Server 2003 und Windows Server 2003 R2 gibt es zwei Möglichkeiten: Verwenden Sie entweder das Installationspaket aus dem Lieferumfang des Programms oder legen Sie die ausführbare Datei setup.exe aus dem Standard-Installationspaket „Kaspersky Security Center 10.5 Administrationsagent für Windows XP“ im Ordner des Programm-Installationspakets in Kaspersky Security Center ab.

  - Auf Computern mit den Betriebssystemen Windows XP SP3 Professional (32-Bit) und Windows XP Embedded SP3 (32-Bit) gibt es zwei Möglichkeiten: Verwenden Sie entweder das Installationspaket aus dem Lieferumfang des Programms oder legen Sie die ausführbare Datei setup.exe aus dem in Kaspersky Security Center Version 14 erstellten Programm-Installationspaket oder aus dem Standard-Installationspaket „Kaspersky Security Center 14 Administrationsagent für Windows XP“ im Ordner des Programm-Installationspakets in Kaspersky Security Center ab.

So extrahieren Sie die Datei setup.exe aus dem Standard-Installationspaket für Kaspersky Security Center

1. Wählen Sie in der Struktur der Kaspersky Security Center-Verwaltungskonsole den Punkt **Erweitert** → **Remote-Installation** → **Installationspakete** aus.

2. Klicken Sie im Arbeitsbereich auf **Zusätzliche Aktionen** und wählen Sie in der Dropdown-Liste **Aktuelle Versionen der Kaspersky-Programme anzeigen** aus.

3. Wählen Sie in der Liste das gewünschte Programm aus. Beispiel: Administrationsagent von Kaspersky Security Center 10.5 für Windows XP.

4. Klicken Sie auf **Herunterladen und Installationspaket erstellen**.

   Das erstellte Installationspaket erscheint in der Liste **Installationspakete**.

5. Öffnen Sie die Eigenschaften des erstellten Installationspakets.

6. Kopieren Sie im Abschnitt **Allgemein** den Pfad zum Ordner des Installationspakets.

7. Öffnen Sie den Ordner des Installationspakets.

8. Kopieren Sie die Datei setup.exe.

- So verwalten Sie Kaspersky Embedded Systems Security über Kaspersky Security Center:
  - Verwenden Sie auf einem Computer mit Windows XP SP2 Professional (32-Bit/64-Bit), Windows Server 2003 oder Windows Server 2003 R2 den Administrationsagenten von Kaspersky Security Center (klnagent) in Version 10.5.1781.
  - Verwenden Sie auf einem Computer mit Windows XP SP3 Professional (32-Bit) oder Windows XP Embedded SP3 (32-Bit) den Administrationsagenten für Kaspersky Security Center (klnagent) in Version 14.0.0.20023.
- Auf Computern mit Windows XP können Telemetriedaten nicht mithilfe des MQTT-Protokolls an eine Datendiode gesendet werden.

Integration in Kaspersky Security Center

- Wenn Update-Pakete empfangen werden, überprüft der Administrationsserver die Datenbanken-Updates, bevor die Updates an geschützte Geräte im Netzwerk gesendet werden. Der Kaspersky Security Center Administrationsserver sucht nicht nach Updates für die Programm-Module.
- Stellen Sie sicher, dass die erforderlichen Kontrollkästchen in den Einstellungen für die Interaktion mit dem Kaspersky Security Center Administrationsserver aktiviert sind, wenn Sie die Komponenten verwenden, die mithilfe von Netzwerklisten (Quarantäne, Backup) dynamische Daten an Kaspersky Security Center übermitteln.
- Der Administrationsagent 10.5 sendet keine Informationen über die installierten Komponenten an den Kaspersky Security Center Administrationsserver. Darum werden in der Kaspersky Security Center-Verwaltungskonsole und in der Kaspersky Security Center Web Console in den Einstellungen eines Geräts mit dem Administrationsagenten 10.5 die installierten Komponenten von Kaspersky Embedded Systems Security und deren Einstellungen nicht angezeigt.
- Wenn Kaspersky Security Center Administrationsagent 10.5 auf dem Gerät installiert ist, können Sie die Dateien aus dem Backup nicht über die Kaspersky Security Center Web Console herunterladen.
- Wenn Kaspersky Embedded Systems Security mit dem aktivierten ressourcenschonenden Modus für den Kaspersky Security Center Administrationsagenten installiert wird (Standard, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`) und anschließend Administrationsagent installiert wird, erstellt Kaspersky Embedded Systems Security in der Windows-Firewall keine Ausnahme für den Administrationsagenten, und die Windows-Firewall blockiert den Administrationsagenten.
- Wenn Kaspersky Embedded Systems Security mit dem aktivierten ressourcenschonenden Modus für den Kaspersky Security Center Administrationsagenten installiert wird (Standard, `SKIP_KLNAG_FLAG_TEST_VM_PERF=0`) werden Änderungen an Netzwerklisten mit einer Verzögerung von etwa zehn Minuten in der Kaspersky Security Center-Verwaltungskonsole angezeigt.
- 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 Embedded Systems 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.

Andere Einschränkungen

Untersuchung auf Befehl und Echtzeitschutz für Dateien

- Die Untersuchung von über das MTP-Protokoll angeschlossenen Geräten ist nicht verfügbar.
- Die Untersuchung von Archiven ist ohne die Untersuchung von SFX-Archiven nicht möglich: Wenn die Untersuchung von Archiven in den Schutzeinstellungen von Kaspersky Embedded Systems Security aktiviert ist, untersucht das Programm automatisch Objekte sowohl in Archiven als auch in SFX-Archiven. Die Untersuchung von SFX-Archiven ist auch ohne die Untersuchung von Archiven verfügbar.
- Wenn das Kontrollkästchen **Vertiefte Analyse des Starts von Prozessen (Prozess-Start wird während der Analyse blockiert)** und die Option **KSN-Nutzung** gleichzeitig aktiviert sind, wird jeder gestartete Prozess, der URL-Webadressen als Argument empfängt, selbst dann blockiert, wenn der „Informieren"-Modus ausgewählt ist. Um ein Blockieren des Prozesses zu vermeiden, wählen Sie eine der folgenden Optionen aus:
  - Deaktivieren Sie die **KSN-Nutzung**.
  - Deaktivieren Sie das Kontrollkästchen **Vertiefte Analyse des Starts von Prozessen (Prozess-Start wird während der Analyse blockiert)**.

  Empfohlene Option: Deaktivieren Sie das Kontrollkästchen **Vertiefte Analyse des Starts von Prozessen (Prozess-Start wird während der Analyse blockiert)**.

Lizenzverwaltung

- Sie können das Programm nicht mit einem Schlüssel über den Installationsassistenten aktivieren, wenn der Schlüssel mithilfe des Befehls SUBST erstellt wurde oder wenn für die Schlüsseldatei ein Netzwerkpfad angegeben ist.
- Wenn Sie einen Proxyserver von Kaspersky Security Center für die Aktivierung des Produkts auf einem Client-Gerät verwenden möchten, deaktivieren Sie die VDI-Optimierung auf diesem Gerät bei der Installation von Kaspersky Security Center Network Agent.

Update

- Bei der Installation und Deinstallation von Patches für Kaspersky Embedded Systems Security auf Geräten mit Windows XP kann aufgrund der Besonderheiten dieses Betriebssystems ein Neustart des Geräts erforderlich sein.
- Standardmäßig wird das Programmsymbol nach der Installation von Updates für kritische Module von Kaspersky Embedded Systems Security ausgeblendet.

- KLRAMDISK wird auf geschützten Geräten unter Windows XP oder Windows Server® 2003 nicht unterstützt.
- Wenn die Installation des Patches für Kaspersky Embedded Systems Security fehlschlägt, wird ein Rollback des Patches ausgeführt und Sie werden aufgefordert, das Betriebssystem neu zu starten.

Benutzeroberfläche

- Beachten Sie die Groß- und Kleinschreibung bei der Verwendung der Filterfunktion in der Programmkonsole für die Bereiche Quarantäne, Backup, Systemaudit-Protokoll oder Protokoll der Aufgabenausführung.
- Wenn Sie einen Schutz- oder Untersuchungsbereich in der Programmkonsole konfigurieren, können Sie nur eine Maske verwenden und sie nur am Pfadende platzieren. Hier finden Sie Beispiele für richtige Masken: `C:\Temp\Temp*`, `C:\Temp\Temp???.doc`, `C:\Temp\Temp*.doc`. Diese Einschränkung betrifft nicht die Konfiguration der vertrauenswürdigen Zone.
- Die Zeit, zu der die Ausführung der Aufgaben geplant ist, wird nicht in der Programmkonsole im **Telemetrie-Erfassungsserver** angezeigt. Die Spalte **Startzeit** ist leer.
- Pop-up-Benachrichtigungen für Textelemente der Benutzeroberfläche, die länger als 256 Zeichen sind, werden in der Kaspersky Security Center-Verwaltungskonsole oder in der Programmkonsole nicht angezeigt.
- 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.

Sicherheit

- Wenn die Benutzerkontensteuerung (User Account Control) des Betriebssystems aktiviert ist, muss das Benutzerkonto zur Gruppe "ESS Administrators" gehören, um die Programmkonsole mit einem Doppelklick auf das Programmsymbol im Infobereich der Taskleiste öffnen zu können. Ansonsten ist es erforderlich, sich als Benutzer mit der Berechtigung, das kompakte Diagnosefenster oder das Microsoft Management-Console-Snap-in zu öffnen, anzumelden.
- Wenn die Benutzerkontensteuerung aktiviert ist, können Sie das Programm nicht über das Microsoft Windows-Fenster "Apps und Features" deinstallieren.

Exploit-Prävention

- Die Exploit-Prävention ist nicht verfügbar, wenn die apphelp.dll-Bibliotheken in der aktuellen Umgebungskonfiguration nicht geladen sind.
- Die Komponente Exploit-Prävention ist auf geschützten Geräten, auf denen das Betriebssystem Microsoft Windows 10 ausgeführt wird, nicht mit dem Microsoft-Dienstprogramm EMET kompatibel. EMET wird durch Kaspersky Embedded Systems Security blockiert, wenn die Komponente Exploit-Prävention auf einem geschützten Gerät mit installiertem Dienstprogramm EMET installiert ist.
- Exploit-Prävention ist inkompatibel mit der SQL Server® 2012 Database Engine. Wenn Sie Kaspersky Embedded Systems Security auf einem Computer mit installiertem MS SQL Server 2012 installieren, müssen Sie die Bibliothek sqlos.dll des Datenbankservers in die Ausnahmeliste der Aufgabe Exploit-Prävention aufnehmen.

Detection and Response

- Wenn während der Reaktion auf Bedrohungen ein Fehler beim Zugriff auf einen freigegebenen Ordner auftritt, wird dieser Fehler nicht im Reaktionsverlauf für die Bedrohung angezeigt (Kaspersky Security Center Web Console → Eigenschaften des Hosts mit dem installierten Programm → **Detection and Response** – Abschnitt **Reaktionsverlauf**).

Konfiguration von Ereignissen

Einstellungen für das Ereignis *Dateivorgang im Kontrollbereich nicht kontrolliert*, das im Abschnitt **Konfiguration von Ereignissen** der Richtlinie für Kaspersky Security Center konfiguriert werden kann, werden auch auf die folgenden Ereignisse angewendet:

- *Erlaubter Dateivorgang im Kontrollbereich von einem vertrauenswürdigen Benutzer ausgeführt*.
- *Dateivorgang im Kontrollbereich verboten*.
- *Nur Statistik: Dateivorgang im Kontrollbereich verboten*.
- *Dateivorgang im Kontrollbereich nicht kontrolliert*.

Kompaktes Diagnosefenster

Auf Computern mit Windows XP muss der Terminaldienst ausgeführt werden, damit das kompakte Diagnosefenster funktioniert.

Im abgesicherten Modus von Windows arbeiten

Das Programm funktioniert nicht im Safe Mode von Windows.

Kompatibilität mit anderen Programmen

Kaspersky Endpoint Security ist inkompatibel mit Programmen, die Teil von Drittanbieter-EPP-Lösungen (Endpoint Protection Plattform) sind. Kaspersky Embedded Systems Security ist möglicherweise auch mit anderen Programmen und einigen Kaspersky-Programmen inkompatibel. Um die Kompatibilität zu ermitteln, verwendet Kaspersky Embedded Systems Security eine von Kaspersky erstellte Liste mit Programmen. Diese Liste ist in der Datei „incompatible.txt“ enthalten. Diese Datei ist im Lieferumfang enthalten.

Wenn ein Programm aus der Liste „incompatible.txt“ gefunden wird, bricht das Installationsprogramm die Installation von Kaspersky Embedded Systems Security ab. Dann müssen Sie das Drittanbieter-Antiviren-Programm entfernen. Möglicherweise löscht das Installationsprogramm einige Anwendung, die sich auf der Liste befinden.

Wenn die Windows-Firewall auf dem Computer installiert ist, wird sie vom Installationsprogramm deaktiviert, damit die Installation von Kaspersky Embedded Systems Security fortgesetzt werden kann.

Falls es erforderlich ist, Kaspersky Embedded Systems Security trotz der Risiken zusammen mit einem Programm aus der Liste „incompatible.txt“ zu installieren, können Sie die Überprüfung auf installierte Drittanbieter-Antiviren-Programmen überspringen. Geben Sie dazu im Installationsprogramm die folgenden Parameter an: `SKIPPRODUCTCHECK=1` und `SKIPPRODUCTUNINSTALL=1`.

Beispiel:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 SKIPPRODUCTCHECK=1 SKIPPRODUCTUNINSTALL=1
```

Programm installieren und deinstallieren

Dieser Abschnitt enthält schrittweise Anleitungen zur Installation und Deinstallation von Kaspersky Embedded Systems Security.

Installation planen

Dieser Abschnitt beschreibt das Paket von Administrations-Tools für Kaspersky Embedded Systems Security und besondere Aspekte bei der Installation und Deinstallation von Kaspersky Embedded Systems Security mithilfe eines Assistenten, mithilfe der Befehlszeile, über Kaspersky Security Center und mittels einer Active Directory-Gruppenrichtlinie.

Wenn Sie Kaspersky Embedded Systems Security installieren, nachdem Sie Kaspersky Industrial CyberSecurity for Nodes oder Kaspersky Endpoint Security für Windows entfernt haben, müssen Sie den Computer neu starten.

Planen Sie die Phasen der Installation, bevor Sie die Installation von Kaspersky Embedded Systems Security starten.

1. Bestimmen Sie die Administrations-Tools, die Sie zur Verwaltung und Konfiguration von Kaspersky Embedded Systems Security einsetzen möchten.
2. Legen Sie fest, welche Programmkomponenten für die Installation erforderlich sind.
3. Wählen Sie die Installationsmethode aus.

Administrations-Tools auswählen

Bestimmen Sie, welche Administrations-Tools Sie für die Konfiguration der Einstellungen von Kaspersky Embedded Systems Security und zur Verwaltung des Programms verwenden möchten. Als Administrations-Tools für Kaspersky Embedded Systems Security können die Programmkonsole, das Befehlszeilen-Tool sowie die Kaspersky Security Center Verwaltungskonsole dienen.

Konsole für Kaspersky Embedded Systems Security

Die Konsole für Kaspersky Embedded Systems Security ist ein eigenständiges Snap-in, das in die Microsoft Management Console eingefügt wird. Sie können Kaspersky Embedded Systems Security über die Programmkonsole verwalten, die auf dem geschützten Server Gerät oder auf einem anderen Gerät im Unternehmensnetzwerk installiert ist.

Einer Microsoft Management Console, die im Authoring-Modus geöffnet ist, können Sie mehrere Snap-ins von Kaspersky Embedded Systems Security hinzufügen, um mit ihr den Schutz mehrerer Geräte mit installiertem Kaspersky Embedded Systems Security zu verwalten.

Befehlszeilen-Utility

Sie können Kaspersky Embedded Systems Security aus der Befehlszeile eines geschützten Geräts verwalten.

Das Befehlszeilen-Tool gehört zum Paket der Programmkomponenten von Kaspersky Embedded Systems Security.

Kaspersky Security Center

Wenn Sie zur zentralisierten Verwaltung des Antiviren-Schutzes für die Geräte in Ihrem Unternehmen Kaspersky Security Center verwenden, können Sie Kaspersky Embedded Systems Security über die Kaspersky Security Center Verwaltungskonsole verwalten.

Die folgenden Programmkomponenten müssen installiert werden:

- **Modul für die Integration in den Kaspersky Security Center Administrationsagenten**. Diese Komponente gehört zum Paket der Programmkomponenten von Kaspersky Embedded Systems Security. Sie erlaubt Kaspersky Embedded Systems Security, mit dem Administrationsagenten zu kommunizieren. Installieren Sie das Modul zur Integration mit dem Kaspersky Security Center Administrationsagenten auf dem geschützten Gerät.

- **Kaspersky Security Center Administrationsagent**. Installieren Sie ihn auf jedem geschützten Gerät. Diese Komponente koordiniert die Interaktion zwischen dem auf dem geschützten Gerät installierten Programm Kaspersky Embedded Systems Security und der Kaspersky Security Center Verwaltungskonsole. Die Installationsdatei des Administrationsagenten gehört zum Lieferumfang von Kaspersky Security Center.

- **Verwaltungs-Plug-in für Kaspersky Embedded Systems Security**. Installieren Sie zusätzlich das Verwaltungs-Plug-in, um Kaspersky Embedded Systems Security über die Verwaltungskonsole auf dem geschützten Gerät zu verwalten, auf dem der Kaspersky Security Center Administrationsserver installiert ist. Dadurch wird eine Schnittstelle zur Programmverwaltung über Kaspersky Security Center bereitgestellt. Die Installationsdatei "\exec\klcfginst.exe" des Administrations-Plug-ins ist im Lieferumfang von Kaspersky Embedded Systems Security enthalten.

Installationstyp auswählen

Nachdem Sie die Softwarekomponenten für die Installation von Kaspersky Embedded Systems Security angegeben haben, müssen Sie die Installationsmethode des Programms auswählen.

Wählen Sie die entsprechende Installationsmethode je nach der Netzwerkarchitektur und den folgenden Bedingungen aus:

- Ob Sie spezielle Installationseinstellungen für Kaspersky Embedded Systems Security benötigen oder die empfohlenen Installationseinstellungen verwendet werden.

- Ob die Installationseinstellungen für alle Geräte einheitlich oder für jedes geschützte Gerät individuell sind.

Sie können Kaspersky Embedded Systems Security interaktiv mit dem Installationsassistenten oder im Silent-Modus ohne Benutzerbeteiligung installieren, sowie aufrufen, indem Sie die Datei aus dem Installationspaket mit den Installationseinstellungen aus der Befehlszeile ausführen. Sie können Kaspersky Embedded Systems Security zentral als Remote-Installation installieren, indem Sie Gruppenrichtlinien von Active Directory oder die Aufgabe zur Remote-Installation von Kaspersky Security Center verwenden.

Sie können Kaspersky Embedded Systems Security auf einem einzelnen geschützten Gerät installieren und konfigurieren und die Einstellungen in einer Konfigurationsdatei speichern, um später die angelegte Datei für die Installation von Kaspersky Embedded Systems Security auf anderen geschützten Geräten zu verwenden. Beachten Sie, dass diese Option bei der Installation über Gruppenrichtlinien des Active Directory nicht gilt.

Installationsassistent starten

Mit dem Installationsassistenten können Sie installieren:

- Komponenten von Kaspersky Embedded Systems Security auf dem geschützten Gerät durch Klicken auf den Link im Begrüßungsprogramm, das durch Öffnen der Datei "setupui.exe" oder direkt über die Datei "\exec\setup_ess.exe" im Lieferumfang gestartet werden kann.
- Konsole für Kaspersky Embedded Systems Security auf dem geschützten Gerät oder einem anderen Gerät im LAN durch Klicken auf den Link im Begrüßungsprogramm, das durch Öffnen der Datei "setupui.exe" oder direkt über die Datei "\console\setup_esstools.exe" im Lieferumfang gestartet werden kann.

Datei des Installationspaketes mit den erforderlichen Installationseinstellungen aus der Befehlszeile starten

Wenn Sie die Datei des Installationspaketes ohne Befehlszeilenoption aufrufen, installieren Sie Kaspersky Embedded Systems Security mit den Standardinstallationseinstellungen. Mit den Optionen von Kaspersky Embedded Systems Security können Sie die Installationseinstellungen ändern.

Die Programmkonsole kann auf dem geschützten Gerät und/oder auf dem Administrator-Arbeitsplatz installiert werden.

Sie können zur Installation von Kaspersky Embedded Systems Security und der Programmkonsole auch Beispiele für Befehle verwenden.

Zentrale Installation über Kaspersky Security Center

Wenn Sie Kaspersky Security Center zur Verwaltung des Antiviren-Schutzes der Netzwerkserver einsetzen, können Sie Kaspersky Embedded Systems Security mit der Aufgabe zur Remote-Installation auf mehreren Geräten installieren.

Die geschützten Geräte, auf denen Sie Kaspersky Embedded Systems Security mittels Kaspersky Security Center installieren möchten, können sich in derselben Domäne wie Kaspersky Security Center, in einer anderen Domäne oder in überhaupt keiner Domäne befinden.

Zentrale Installation über Gruppenrichtlinien des Active Directory

Mit den Gruppenrichtlinien von Active Directory können Sie Kaspersky Embedded Systems Security auf dem geschützten Gerät installieren. Sie können auch die Programmkonsole auf dem geschützten Gerät oder auf dem Administrator-Arbeitsplatz installieren.

Es ist möglich, Kaspersky Embedded Systems Security nur mit den empfohlenen Installationseinstellungen zu installieren.

Die geschützten Geräte, auf denen Kaspersky Embedded Systems Security mithilfe von Active Directory-Gruppenrichtlinien installiert wird, müssen sich in derselben Domäne und derselben Organisationseinheit befinden. Die Installation erfolgt beim Start des geschützten Geräts vor der Anmeldung bei Microsoft Windows.

Installation und Deinstallation des Programms mit dem Assistenten

Dieser Abschnitt beschreibt die Installation und Deinstallation von Kaspersky Embedded Systems Security und der Programmkonsole mithilfe des Installationsassistenten und beinhaltet Informationen über zusätzliche Konfiguration von Kaspersky Embedded Systems Security und Aktionen, die bei der Installation ausgeführt werden müssen.

Installation mit dem Installationsassistenten

Die folgenden Abschnitte enthalten Informationen über die Installation von Kaspersky Embedded Systems Security und der Programmkonsole.

Um Kaspersky Embedded Systems Security zu installieren und zu verwenden, gehen Sie wie folgt vor:

1. Installieren Sie Kaspersky Embedded Systems Security auf dem geschützten Gerät.
2. Installieren Sie die Programmkonsole auf den Geräten, von denen aus Sie Kaspersky Embedded Systems Security verwalten möchten.
3. Wenn die Programmkonsole auf einem anderen Gerät im Netzwerk als dem geschützten Gerät installiert wurde, führen Sie eine zusätzliche Konfiguration durch, damit Benutzer der Programmkonsole Kaspersky Embedded Systems Security remote verwalten können.
4. Führen Sie nach der Installation von Kaspersky Embedded Systems Security Aktionen durch.

Installation von Kaspersky Embedded Systems Security

Bevor Sie Kaspersky Embedded Systems Security installieren, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass auf dem geschützten Gerät keine anderen Antiviren-Anwendungen installiert sind. Sie müssen Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition entfernen. Sie müssen Kaspersky Security 10 für Windows Server nicht entfernen, um Kaspersky Embedded Systems Security zu installieren.
2. Vergewissern Sie sich, dass das Konto, mit dem Sie den Setup-Assistenten ausführen, zur Administratorengruppe auf dem geschützten Gerät gehört.

Kaspersky Embedded Systems Security enthält die folgenden vordefinierten Konfigurationen:

Computer mithilfe der Technologie „Alles standardmäßig verbieten“ schützen

Die Komponenten, die Updates ermöglichen, sind nicht in der Konfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** enthalten.

Wenn die Konfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** ausgewählt ist, sind standardmäßig die folgenden Komponenten enthalten:

- Exploit-Prävention
- Kontrolle des Programmstarts
- Systemfachsymbol

Wenn Sie die Programmkonfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** über eine Programmversion installieren, die Signaturanalyse- und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz von Programmkomponenten automatisch reduziert, indem die folgende Komponente entfernt wird:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Komponenten, die Updates ermöglichen

Diese Konfiguration wird zum Schutz von Geräten mit begrenzten Ressourcen empfohlen. In diesem Fall können Sie das Programm langfristig aktivieren, und die Komponente Kontrolle des Programmstarts sorgt für den Schutz des Computers.

Computer mit Antiviren-Datenbanken schützen

Wenn die Konfiguration **Computer mittels Antiviren-Datenbanken schützen** ausgewählt ist, sind standardmäßig alle Komponenten von Kaspersky Embedded Systems Security enthalten, unter Ausnahme der Komponenten Firewall und Leistungsindikatoren.

Wenn Sie die Programmkonfiguration **Computer mittels Antiviren-Datenbanken schützen** über eine Programmversion installieren, die keine Signaturanalyse und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz der Programmkomponenten automatisch erweitert. Dazu werden die folgenden Komponenten hinzugefügt:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Schutz vor Netzwerkbedrohungen

Erfahren Sie mehr über die Installations- bzw. Deinstallationseinstellungen.

So installieren Sie Kaspersky Embedded Systems Security mithilfe des Installationsassistenten:

1. Führen Sie auf dem geschützten Gerät die Datei "setupui.exe" aus.
2. Klicken Sie im angezeigten Fenster im Abschnitt **Installation** auf den Link **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** oder auf den Link **Computer mittels Antiviren-Datenbanken schützen**.
3. Klicken Sie im Begrüßungsfenster des Installationsassistenten von Kaspersky Embedded Systems Security auf die Schaltfläche **Weiter >**.

   Das Fenster **Endbenutzer-Lizenzvertrag** wird geöffnet.
4. Lesen Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
5. Wenn Sie den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie zustimmen, aktivieren Sie die Kontrollkästchen **Ich bestätige, dass ich die Bestimmungen und Bedingungen dieser Endbenutzer-Lizenzverträge vollständig gelesen habe und sie verstehe und akzeptiere** und **Mir ist bewusst, dass meine Daten wie in der Datenschutzrichtlinie beschrieben verarbeitet und (einschließlich in Drittländer) übertragen werden. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe**.

   Wenn Sie den Endbenutzer-Lizenzvertrag und/oder die Datenschutzrichtlinie nicht akzeptieren, wird die Installation abgebrochen.
6. Klicken Sie auf **Weiter >**.

   Das Fenster **Benutzerdefinierte Installation** wird geöffnet.

   Wählen Sie die Komponente, die Sie installieren wollen.

   Die Komponente Unterstützung des SNMP-Protokolls von Kaspersky Embedded Systems Security wird nur auf dem geschützten Server installiert, wenn auf dem geschützten Gerät der Dienst SNMP Microsoft Windows installiert ist.
7. Um alle Änderungen im Fenster **Benutzerdefinierte Installation** zu verwerfen, klicken Sie auf die Schaltfläche **Zurücksetzen**. Klicken Sie auf **Weiter >**.
8. Gehen Sie Fenster **Installationsordner wählen** wie folgt vor:

   - Geben Sie bei Bedarf einen Ordner an, in dem die Dateien von Kaspersky Embedded Systems Security gespeichert werden sollen.
   - Sehen Sie sich erforderlichenfalls die Informationen über den verfügbaren Speicherplatz auf den lokalen Festplatten an, indem Sie auf die Schaltfläche **Datenträger** klicken.

   Klicken Sie auf **Weiter >**.
9. Im Fenster **Anpassen** können Sie Objekte und Ordner aus dem Schutzbereich ausschließen und den Echtzeitschutz für Dateien konfigurieren.
10. Geben Sie im Fenster **Einstellungen aus Konfigurationsdatei importieren** einen Pfad zur Konfigurationsdatei an, wenn Sie die Einstellungen von Kaspersky Embedded Systems Security aus einer vorhandenen Konfigurationsdatei importieren möchten, die in einer früheren Programmversion erstellt wurde.

11. Führen Sie im Fenster **Programm aktivieren** eine der folgenden Aktionen aus:

    - Wenn Sie das Programm aktivieren möchten, geben Sie die Schlüsseldatei für Kaspersky Embedded Systems Security zur Aktivierung des Programms an.
    - Wenn Sie das Programm später aktivieren möchten, klicken Sie auf die Schaltfläche **Weiter >**.
    - Wenn zuvor eine Schlüsseldatei im Ordner \exec (der zum Lieferumfang gehört) gespeichert wurde, wird der Name dieser Datei im Feld **Schlüssel** angezeigt.
    - Um einen Schlüssel aus der Datei, die in einem anderen Ordner gespeichert ist, hinzuzufügen, geben Sie die Schlüsseldatei an.

      Der Installations-Assistent erlaubt es nicht, das Programm mit einem Aktivierungscode zu aktivieren. Wenn Sie das Programm mit einem Aktivierungscode aktivieren möchten, können Sie den Code nach der Installation des Programms angeben.

      Nach dem Hinzufügen der Schlüsseldatei werden im Fenster die Lizenzinformationen angezeigt. Kaspersky Embedded Systems Security zeigt das berechnete Ablaufdatum der Lizenz an. Die Gültigkeitsdauer der Lizenz wird ab dem Hinzufügen des Schlüssels gezählt, läuft jedoch spätestens nach dem Ablauf der Gültigkeitsdauer der Schlüsseldatei ab.

      Klicken Sie auf **Weiter >**, um die Schlüsseldatei zum Programm hinzuzufügen.

12. Im Abschnitt **Einstellungen für den Remote-Zugriff** können Sie bei Bedarf die TCP-Portnummern ändern, die die Programmkonsole für eine Remote-Verbindung mit dem Computer verwendet, auf dem das Programm installiert ist.

    Die Standardportnummer für die Verbindung mit Windows-Anmeldedaten ist 13032, und die Standardportnummer für die Verbindung mit Anmeldedaten manuell erstellter Benutzer ist 13031. Bereich der möglichen Portnummern: 1 bis 65535.

    Um eine Verbindung mit den Anmeldedaten manuell erstellter Benutzerkonten zu verhindern, deaktivieren Sie das Kontrollkästchen **Mittels Anmeldedaten von manuell erstellten Benutzern**.

13. Im Fenster **Programminstallation vorbereiten** können Sie bei Bedarf die Option **Installationsprozess schützen** deaktivieren. Der Installationsschutz enthält die folgenden Funktionen: Schutz vor dem Austausch eines Programmpakets durch schädliche Programme, Sperrung des Zugriffs auf den Installationsordner von Kaspersky Embedded Systems 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).

14. Falls erforderlich, können Sie den Dateipfad für kavshell.exe zur Systemvariablen %PATH% hinzufügen, um die Verwendung der Befehlszeilenschnittstelle zu vereinfachen.

15. Klicken Sie auf **Installieren**.

16. Sobald die Installation abgeschlossen wurde, öffnet sich das Fenster **Die Installation wurde abgeschlossen**.

17. Klicken Sie auf **Fertig**.

Der Installationsassistent wird geschlossen. Sobald die Installation abgeschlossen ist, ist Kaspersky Embedded Systems Security einsatzbereit, vorausgesetzt, dass Sie einen Aktivierungsschlüssel hinzugefügt haben.

Installation der Konsole für Kaspersky Embedded Systems Security

Folgen Sie den Anweisungen des Installationsassistenten und passen Sie die Installationseinstellungen für die Programmkonsole an. Sie können die Installation bei jedem Schritt des Assistenten abbrechen. Klicken Sie dazu im Fenster des Installationsassistenten auf die Schaltfläche **Abbrechen**.

So installieren Sie die Programmkonsole:

1. Vergewissern Sie sich, dass das Benutzerkonto, das Sie verwenden, um den Installationsassistenten starten, zur Administratorengruppe auf dem geschützten Gerät gehört.

2. Führen Sie auf dem geschützten Gerät die Datei "setupui.exe" aus.

   Das Fenster des Willkommen-Programms wird geöffnet.

3. Klicken Sie auf den Link **Konsole von Kaspersky Embedded Systems Security für Windows installieren**.

   Es öffnet sich das Begrüßungsfenster des Installationsassistenten. Klicken Sie auf **Weiter >**.

4. Wenn Sie den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie zustimmen, aktivieren Sie die Kontrollkästchen **Ich bestätige, dass ich die Bestimmungen und Bedingungen dieser Endbenutzer-Lizenzverträge vollständig gelesen habe und sie verstehe und akzeptiere** und **Mir ist bewusst, dass meine Daten wie in der Datenschutzrichtlinie beschrieben verarbeitet und (einschließlich in Drittländer) übertragen werden. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe**. Klicken Sie auf **Weiter >**.

5. Geben Sie im Fenster **Installationsordner wählen** einen Ordner an, in dem die zu installierenden Dateien gespeichert werden.

6. Klicken Sie auf **Weiter >**.

7. Klicken Sie im Fenster **Programminstallation vorbereiten** auf **Installieren**.

   Der Assistent installiert nun die ausgewählten Komponenten.

8. Klicken Sie auf **Fertig**.

Der Installationsassistent wird geschlossen. Die Programmkonsole wird auf dem geschützten Gerät installiert.

Wenn Sie die Programmkonsole nicht auf dem geschützten Gerät, sondern auf einem anderen Netzwerkgerät installiert haben, konfigurieren Sie die erweiterten Einstellungen.

Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Gerät

Wenn Sie die Programmkonsole nicht auf dem geschützten, sondern auf einem anderen Netzwerkgerät installiert haben, gehen Sie wie unten beschrieben vor, damit Kaspersky Embedded Systems Security von den Benutzern ferngesteuert verwaltet werden kann:

- Verwenden Sie in den Programmeinstellungen ein Benutzerkonto, das zum Herstellen einer Remote-Verbindung berechtigt ist. Standardmäßig verfügen alle Benutzer der Gruppen „Administratoren“ und „ESS-Administratoren“ über diese Berechtigung.

- Öffnen Sie auf dem Remote-Gerät in den Windows-Firewall-Einstellungen den Port TCP 13032 für Verbindungen über Windows-System-Benutzerkonten und TCP 13031 für Verbindungen über Benutzerkonten, die manuell in den Programmeinstellungen erstellt wurden. Erlauben Sie außerdem Netzwerkverbindungen für die ausführbare Datei des Fernverwaltungsprozesses von Kaspersky Embedded Systems Security (avp.exe). Sie können diese Einstellung über die Option `ADDWFEXCLUSION=1` verwalten, wenn Sie das Programm über die Befehlszeile installieren.

Wenn Sie Kaspersky Embedded Systems Security per Fernzugriff ausführen müssen, sind zusätzlich die folgenden Schritt erforderlich:

Das Benutzerkonto, mit dem das Programm aus der Ferne gestartet wird, muss zur Gruppe „Administratoren“ gehören.

- Aktivieren Sie auf dem Remote-Gerät in den Windows-Firewall-Einstellungen die Regel **Datei- und Druckerfreigabe (SMB-In)** (Port TCP 445). Außerdem wird empfohlen, den Port TCP 135 zu öffnen, um die Verbindung mit dem Gerät zu vereinfachen.

- Für Remote-Geräte mit Windows Vista oder höher, die nicht zu einer Domäne gehören oder die über ein lokales Benutzerkonto verwaltet werden, **deaktivieren Sie die Remote-Benutzerkontensteuerung (UAC).**

  1. Öffnen Sie den Registrierungseditor auf dem Computer.

  2. Öffnen Sie im Registrierungs-Editor den Schlüssel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

  3. Öffnen Sie den Wert LocalAccountTokenFilterPolicy.

     Wenn der Wert LocalAccountTokenFilterPolicy in diesem Schlüssel nicht vorhanden ist, erstellen Sie einen DWORD-Wert (32-Bit) mit diesem Namen (Details finden Sie auf der Website des Technischen Supports von Microsoft).

  4. Setzen Sie den Wert auf `1` und klicken Sie auf **OK**.

     Das Deaktivieren der Remote-Benutzerkontensteuerung hat keine Auswirkungen auf die lokale Benutzerkontensteuerung.

- Wenn auf dem Gerät, auf dem die Programmkonsole installiert ist, oder auf dem geschützten Gerät das Betriebssystem Windows 8.1 oder eine ältere Windows-Version ausgeführt wird, **aktivieren Sie die Unterstützung der SMB 1.0/CIFS-Dateifreigabe auf Geräten mit Windows 10 oder höher.**

  - Im Programm „Windows-Features“:

    1. Wählen Sie **Start** → **Systemsteuerung** → **Programme und Features** → **Windows-Features aktivieren oder deaktivieren**.
    2. Aktivieren Sie im Fenster **Windows-Features** das Kontrollkästchen **Unterstützung für die SMB 1.0/CIFS-Dateifreigabe**.
    3. Klicken Sie auf **OK**.

  - In Windows PowerShell:

    1. Führen Sie Windows PowerShell als Administrator aus.
    2. Führen Sie den folgenden Befehl aus:

    ```
    Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
    ```

Zur Konfiguration jeder anderen Software- oder Hardware-Firewall müssen dieselben Schritte ausgeführt werden.

Wenn die Programmkonsole geöffnet ist, während Sie die Verbindung zwischen dem geschützten Gerät und dem Gerät konfigurieren, auf dem die Programmkonsole installiert ist:

1. Schließen Sie die Programmkonsole.
2. Warten Sie, bis der Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security (avp.exe) abgeschlossen wird.
3. Starten Sie die Programmkonsole neu.

Die neuen Verbindungseinstellungen werden übernommen.

Anonymen Remote-Zugriff auf COM-Anwendungen erlauben

Die Bezeichnungen der Einstellungen können je nach installiertem Windows-Betriebssystem unterschiedlich sein.

So erlauben Sie anonymen Remote-Zugriff auf COM-Anwendungen:

1. Öffnen Sie auf dem Remote-Gerät, auf dem die Konsole für Kaspersky Embedded Systems Security installiert ist, die **Komponentendienste**-Konsole. Gehen Sie dazu wie folgt vor:

   a. Wählen Sie **Start → Ausführen**.

   b. Führen Sie den folgenden Befehl aus:

   ```
   dcomcnfg
   ```

   c. Die Konsole **Komponentendienste** wird geöffnet.

2. Öffnen Sie in der Konsole **Komponentendienste** des geschützten Geräts den Knoten **Computer**.

3. Öffnen Sie das Kontextmenü im Knoten **Arbeitsplatz**.

4. Wählen Sie den Menüpunkt **Eigenschaften**.

5. Klicken Sie auf der Registerkarte **COM-Sicherheit** im Fenster **Eigenschaften** auf die Schaltfläche **Beschränkungen ändern** in der Einstellungsgruppe **Zugriffsrechte**.

6. Vergewissern Sie sich im Fenster **Remote-Zugriff erlauben**, dass für den Benutzer ANONYMOUS LOGON das Kontrollkästchen **Remote-Zugriff erlauben** aktiviert ist.

7. Klicken Sie auf **OK**.

Netzwerkverbindungen für Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security erlauben

Die Bezeichnungen der Einstellungen können je nach installiertem Windows-Betriebssystem unterschiedlich sein.

Um den TCP-Port 135 in der Windows-Firewall freizugeben und Netzwerkverbindungen für den Prozess zur Remote-Verwaltung von Kaspersky Embedded Systems Security zu erlauben, gehen Sie wie folgt vor:

1. Schließen Sie die Konsole für Kaspersky Embedded Systems Security auf dem Remote-Gerät.

2. Führen Sie einen der folgenden Schritte aus:

   - In Microsoft Windows XP SP2 oder höher:

     a. Wählen Sie **Start → Windows Firewall** aus.

     b. Klicken Sie im Fenster **Windows-Firewall** (oder Einstellungen für Windows-Firewall) auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Port hinzufügen**.

     c. Geben Sie im Feld **Name** den Portnamen RPC (TCP/135) an, oder geben Sie einen anderen Namen an, z. B. DCOM für Kaspersky Embedded Systems Security. Geben Sie im Feld **Portnummer** die Nummer des Ports (135) an.

     d. Wählen Sie das Protokoll **TCP**.

e. Klicken Sie auf **OK**.

f. Klicken Sie auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Hinzufügen**.

- In Microsoft Windows 7 und höher:

  a. Wählen Sie **Start** → **Systemsteuerung** → **Windows Firewall**.

  b. Wählen Sie im Fenster **Windows-Firewall** den Punkt **Ein Programm oder Feature durch die Windows-Firewall zulassen**.

  c. Klicken Sie im Fenster **Verbindung von Programmen über Windows-Firewall erlauben** auf die Schaltfläche **Anderes Programm erlauben**.

3. Geben Sie im Fenster **Programm hinzufügen** die Datei kavfsrcn.exe an. Sie befindet sich im bei der Installation der Konsole für Kaspersky Embedded Systems Security mithilfe von Microsoft Management Console angegeben Zielordner.

4. Klicken Sie auf **OK**.

5. Klicken Sie auf die Schaltfläche **OK** im Fenster **Windows-Firewall (Einstellungen für Windows-Firewall)**.

Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen

Wenn Sie das Programm aktiviert haben, startet Kaspersky Embedded Systems Security die Aufgaben zum Schutz und zur Untersuchung sofort nach der Installation. Wenn das Kontrollkästchen **Echtzeitschutz für Dateien nach der App-Installation aktivieren (empfohlen)** während der Installation von Kaspersky Embedded Systems Security aktiviert ist, untersucht das Programm die Objekte des Gerätedateisystems, wenn darauf zugegriffen wird. Wenn die Komponente Skript-Überwachung im Rahmen einer benutzerdefinierten Installation installiert wurde, untersucht Kaspersky Embedded Systems Security den Quellcode aller Skripte, wenn diese gestartet werden. Kaspersky Embedded Systems Security führt die Aufgabe *Untersuchung wichtiger Bereiche* jeden Freitag um 20:00 Uhr aus.

Wir empfehlen Ihnen, nach der Installation von Kaspersky Embedded Systems Security die folgenden Schritte auszuführen:

- Starten Sie die Aufgabe zum Update der Programm-Datenbanken. Nach der Installation untersucht Kaspersky Embedded Systems Security Objekte anhand von Datenbanken, die im Lieferumfang des Programms enthalten sind.

  > Es wird empfohlen, sofort ein Update der Datenbanken von Kaspersky Embedded Systems Security durchzuführen, da die Datenbanken veraltet sein könnten.

  In der Folge führt das Programm gemäß dem in der Aufgabe standardmäßig festgelegten Zeitplan einmal pro Stunde ein Datenbanken-Update durch.

- Führen Sie eine Untersuchung wichtiger Bereiche des Geräts durch, wenn vor der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät kein Virenschutzprogramm mit aktivierter Funktion zum Echtzeitschutz für Dateien installiert war.

- Passen Sie Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security an.

Update-Aufgabe für Datenbanken und Programm-Module starten und konfigurieren

So aktualisieren Sie die Programm-Datenbank nach der Installation:

1. Konfigurieren Sie unter *Update* die Verbindung zur Update-Quelle.
2. Aufgabe *Update* starten.

Das Web Proxy Auto-Discovery Protocol (WPAD) ist in Ihrem Netzwerk möglicherweise nicht zum automatischen Erkennen von Proxyservereinstellungen im LAN konfiguriert. Dabei erfordert Ihr Netzwerk beim Zugriff auf den Proxyserver möglicherweise eine Authentifizierung.

So legen Sie die optionalen Proxyservereinstellungen und Authentifizierungseinstellungen für den Zugriff auf den Proxyserver fest:

1. Öffnen Sie in der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
2. Wählen Sie den Punkt **Eigenschaften des Programms**.
3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Netzwerkeinstellungen** aus.
4. Klicken Sie im Abschnitt **Proxyserver-Einstellungen** auf **Einstellungen** und aktivieren Sie im folgenden Fenster die das Kontrollkästchen **Angegebene Proxyserver-Einstellungen verwenden**.
5. Geben Sie die Proxyserver-Adresse in das Feld **Adresse** ein und geben Sie die Portnummer für den Proxyserver in das Feld **Port** ein.
6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Einen Proxyserver für lokale Adressen umgehen**. Wenn diese Funktionalität aktiviert ist, erfolgt der Zugriff auf Geräte direkt aus dem Netzwerk, zu dem das geschützte Gerät mit installiertem Kaspersky Embedded Systems Security gehört. Diese Option ist standardmäßig aktiviert.
7. Wählen Sie im Abschnitt **Einstellungen der Proxyserver-Authentifizierung** die erforderliche Authentifizierungsmethode aus der Dropdown-Liste:
   - **Keine Authentifizierung verwenden**.
   - **NTLM-Authentifizierung**. NTLM-Authentifizierung mit dem aktuellen Benutzerkonto (Standard).
   - **NTLM-Authentifizierung mit Benutzername und Kennwort**. NTLM-Authentifizierung mit manuell angegebenen Anmeldedaten.
   - **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.
- **Benutzername und Kennwort**. Authentifizierung mit manuell angegebenen Anmeldedaten.

Geben Sie bei Bedarf den Benutzernamen und das Kennwort an.

Wenn die Kerberos-Authentifizierung ausgewählt ist, kann Kaspersky Embedded Systems Security abhängig von den Proxyserver-Einstellungen die Authentifizierung anhand des Kerberos- oder NTLM-Protokolls durchführen.

8. Klicken Sie auf **OK**.

So starten Sie die Aufgabe Update:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Update**.
2. Wählen Sie im Kontextmenü des untergeordneten Knotens **Datenbanken-Update** den Punkt **Start**.

Die Aufgabe *Update* wird gestartet.

Sobald die Aufgabe erfolgreich abgeschlossen ist, können Sie das Veröffentlichungsdatum der zuletzt installierten Datenbanken-Updates im Ergebnisbereich des Knotens **Kaspersky Embedded Systems Security** anzeigen.

Untersuchung wichtiger Bereiche

Nachdem Sie die Datenbanken von Kaspersky Embedded Systems Security aktualisiert haben, untersuchen Sie das geschützte Gerät mit der Aufgabe *Untersuchung wichtiger Bereiche* auf Schadsoftware.

So starten Sie die Aufgabe Untersuchung wichtiger Bereiche:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie im Kontextmenü des untergeordneten Knotens **Untersuchung wichtiger Bereiche** den Befehl **Start**.

Die Aufgabe wird gestartet. Im Ergebnisfenster wird der Aufgabenstatus **Wird ausgeführt** angezeigt.

Um das Protokoll der Aufgabenausführung anzuzeigen, machen Sie Folgendes,

Klicken Sie im Ergebnisbereich des Knotens **Untersuchung wichtiger Bereiche** auf den Link **Aufgabenprotokoll öffnen**.

Ändern des Pakets von Programmkomponenten und Reparieren von Kaspersky Embedded Systems Security

Komponenten von Kaspersky Embedded Systems Security können hinzugefügt oder entfernt werden. Sie müssen die Aufgabe Echtzeitschutz für Dateien beenden, bevor Sie die Komponente Echtzeitschutz für Dateien entfernen. In den übrigen Fällen ist es nicht erforderlich, die Aufgabe Echtzeitschutz für Dateien oder Kaspersky Embedded Systems Security Service anzuhalten.

Wenn die Programmverwaltung kennwortgeschützt ist, verlangt Kaspersky Embedded Systems Security das Kennwort, wenn Sie versuchen im Installationsassistenten Programmkomponenten zu löschen oder ihre Zusammensetzung zu verändern.

Um die Programmkomponenten von Kaspersky Embedded Systems Security zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Programme und Features** aus. Das Fenster **Programm deinstallieren oder ändern** wird geöffnet.

2. Klicken Sie mit der rechten Maustaste auf **Kaspersky Embedded Systems Security** und wählen Sie **Ändern** aus.

   Dadurch wird der Setup-Assistent **App ändern, reparieren oder entfernen** geöffnet.

3. Wählen Sie den Punkt **Ändern**.

   Das Fenster **Benutzerdefinierte Installation** wird geöffnet. Wählen Sie **Vollständiger Funktionsumfang** aus und klicken Sie auf **Weiter >**.

4. Wählen Sie im Fenster **Benutzerdefinierte Installation** aus der Liste der verfügbaren Komponenten die Komponenten aus, die Sie hinzufügen oder aus Kaspersky Embedded Systems Security entfernen möchten. Gehen Sie hierzu wie folgt vor:

   - Um die Zusammenstellung von Komponenten zu verändern, klicken Sie auf die Schaltfläche neben dem Namen der ausgewählten Komponente. Wählen Sie dann im Kontextmenü:

     - **Die Komponente wird auf der lokalen Festplatte installiert**, wenn Sie eine einzelne Komponente installieren möchten.

     - **Die Komponente und ihre Teilkomponenten werden vollständig installiert**, wenn Sie die Gruppe von Komponenten installieren möchten;

   - Um zuvor installierte Komponenten zu entfernen, klicken Sie auf die Schaltfläche neben dem Namen der ausgewählten Komponente. Wählen Sie im Kontextmenü den Punkt **Die Komponente wird nicht verfügbar sein**.

   Klicken Sie auf **Weiter >**.

5. Bestätigen Sie im Fenster **Programminstallation vorbereiten** die Auswahl der Programmkomponenten durch Klick auf **Installieren**.

6. Klicken Sie im Fenster, das nach Abschluss der Installation geöffnet wird, auf **Fertig**.

Die Zusammensetzung der Komponenten von Kaspersky Embedded Systems Security wird gemäß den angegebenen Einstellungen geändert.

Wenn beim Betrieb von Kaspersky Embedded Systems Security Probleme auftreten (Kaspersky Embedded Systems Security stürzt ab; Aufgaben stürzen ab oder werden nicht gestartet), können Sie eine Reparatur für Kaspersky Embedded Systems Security durchführen. Wenn die Reparatur ausgeführt wird, können entweder die aktuellen Einstellungen von Kaspersky Embedded Systems Security beibehalten werden, oder alle Einstellungen von Kaspersky Embedded Systems Security können auf die Standardwerte zurückgesetzt werden.

So reparieren Sie Kaspersky Embedded Systems Security nach einer fehlerhaften Beendigung des Programms oder einer Aufgabe:

1. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Programme und Features** aus. Das Fenster **Programm deinstallieren oder ändern** wird geöffnet.

2. Klicken Sie mit der rechten Maustaste auf **Kaspersky Embedded Systems Security** und wählen Sie **Ändern** aus.

3. Dadurch wird der Setup-Assistent **App ändern, reparieren oder entfernen** geöffnet.

4. Wählen Sie die Option **Reparieren** aus.

   Das Fenster **Kaspersky Embedded Systems Security reparieren** wird geöffnet. Klicken Sie auf **Weiter >**.

5. Warten Sie, bis die Wiederherstellung abgeschlossen ist, und klicken Sie dann im folgenden Fenster auf **Fertig**.

Kaspersky Embedded Systems Security wird gemäß den angegebenen Einstellungen repariert.

Deinstallation mit dem Installationsassistenten

Dieser Abschnitt enthält Anleitungen zur Deinstallation von Kaspersky Embedded Systems Security und der Programmkonsole von einem geschützten Gerät mithilfe des Installationsassistenten bzw. Deinstallationsassistenten.

Deinstallation von Kaspersky Embedded Systems Security

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der während der Konfiguration des Schreibens von Dump- und Protokolldateien angegeben wurde.

Die Bezeichnungen der Einstellungen können je nach installiertem Windows-Betriebssystem unterschiedlich sein.

Sie können Kaspersky Embedded Systems Security mit dem Installations-/Deinstallationsassistenten vom geschützten Gerät deinstallieren.

Nach der Deinstallation von Kaspersky Embedded Systems Security von einem geschützten Gerät ist möglicherweise ein Neustart erforderlich. Der Neustart kann auf später verschoben werden.

Die Deinstallation, Reparatur oder Installation des Programms ist über die Windows-Systemsteuerung nicht verfügbar.

Wenn der Benutzer im Installationsassistenten versucht, Komponenten zu entfernen oder die Komponentenauswahl zu ändern, fragt Kaspersky Embedded Systems Security die Anmeldedaten des Benutzerkontos ab. Sie müssen die Anmeldedaten eines Benutzers mit ausreichenden Rechten eingeben. Wenn für das Benutzerkonto, unter dem die Deinstallation ausgeführt wird, ein leeres Windows-Kennwort festgelegt ist, deaktivieren Sie die Funktion **Kennwort zur Bestätigung kritischer Aktionen abfragen**, bevor Sie mit der Deinstallation beginnen.

So deinstallieren Sie Kaspersky Embedded Systems Security:

1. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Programme und Features** aus. Das Fenster **Programm deinstallieren oder ändern** wird geöffnet.
2. Klicken Sie mit der rechten Maustaste auf **Kaspersky Embedded Systems Security** und wählen Sie **Ändern** aus.
3. Dadurch wird der Setup-Assistent **App ändern, reparieren oder entfernen** geöffnet.
4. Wählen Sie den Punkt **Entfernen**.

   Das Fenster **Objekte speichern** wird geöffnet.
5. Gehen Sie bei Bedarf im Fenster **Objekte speichern** wie folgt vor:

   Geben Sie unter **Objekte speichern** an, welche Objekte oder Einstellungen Sie beibehalten möchten. Die Kontrollkästchen sind standardmäßig deaktiviert.

   - Aktivieren Sie das Kontrollkästchen **Aktivierungsdaten**.
   - Aktivieren Sie das Kontrollkästchen **Backup-Dateien**.
   - Aktivieren Sie das Kontrollkästchen **Programmeinstellungen**.

   Geben Sie unter **Objekte exportieren** an, welche Objekte Sie exportieren möchten. Die Kontrollkästchen sind standardmäßig deaktiviert.

   - Aktivieren Sie das Kontrollkästchen **Quarantäne-Objekte exportieren**, damit Kaspersky Embedded Systems Security die Quarantäneobjekte exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Aktivieren Sie das Kontrollkästchen **Backup-Objekte exportieren**, damit Kaspersky Embedded Systems Security Objekte aus dem Backup exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Klicken Sie auf die Schaltfläche **Speichern** und geben Sie den Ordner an, in den Sie die Objekte exportieren möchten. Standardmäßig erfolgt der Export von Objekten in den Ordner: %ProgramData%\Kaspersky Lab\KESS.4.1\QB.

     Klicken Sie auf **Weiter**.

6. Bestätigen Sie im Fenster **Deinstallation des Programms bestätigen** die Deinstallation durch Klick auf **Entfernen**.

7. Klicken Sie im Fenster, das nach Abschluss der Deinstallation geöffnet wird, auf **Fertig**.

Kaspersky Embedded Systems Security wird vom geschützten Gerät deinstalliert.

Deinstallation der Konsole für Kaspersky Embedded Systems Security

Die Bezeichnungen der Einstellungen können je nach installiertem Windows-Betriebssystem unterschiedlich sein.

Sie können die Programmkonsole mit Hilfe des Installations-/Deinstallationsassistenten vom geschützten Gerät deinstallieren.

Nach der Deinstallation der Programmkonsole ist kein Neustart des geschützten Geräts erforderlich.

Um die Programmkonsole zu deinstallieren:

1. Wählen Sie im Fenster **Systemsteuerung** den Punkt **Programme und Features** aus. Das Fenster **Programm deinstallieren oder ändern** wird geöffnet.

2. Klicken Sie mit der rechten Maustaste auf **Konsole für Kaspersky Embedded Systems Security** und wählen Sie **Ändern** aus.

   Dadurch wird das Fenster des Assistenten **App ändern, reparieren oder entfernen** geöffnet.

3. Wählen Sie den Punkt **Entfernen**.

   Das Fenster **Deinstallation des Programms bestätigen** wird geöffnet. Klicken Sie auf **Deinstallieren**.

4. Klicken Sie im Fenster, das nach Abschluss der Deinstallation geöffnet wird, auf **OK**.

Die Deinstallation ist nun abgeschlossen, und der Installationsassistent wird geschlossen.

Installation und Deinstallation des Programms aus der Befehlszeile

Dieser Abschnitt enthält eine Beschreibung der Besonderheiten, die für die Installation und Deinstallation von Kaspersky Embedded Systems Security aus der Befehlszeile gelten. Außerdem finden Sie hier Beispiele für Befehle, mit denen Kaspersky Embedded Systems Security aus der Befehlszeile installiert und deinstalliert werden kann, sowie Beispiele für Befehle, mit denen Komponenten von Kaspersky Embedded Systems Security aus der Befehlszeile hinzugefügt oder entfernt werden können.

Über die Installation und Deinstallation von Kaspersky Embedded Systems Security aus der Befehlszeile

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der während der Konfiguration des Schreibens von Dump- und Protokolldateien angegeben wurde.

Sie können Kaspersky Embedded Systems Security installieren oder deinstallieren und seine Komponenten hinzufügen oder entfernen, indem Sie die Installationspaketdatei \exec\ess_win.msi über die Befehlszeile ausführen, nachdem Sie die Installationseinstellungen mit Hilfe der Befehlszeilenoptionen festgelegt haben.

Sie können die Konsole für Kaspersky Embedded Systems Security auf dem geschützten Gerät oder auf einem anderen Gerät im Netzwerk installieren, um das Programm lokal oder im Remote-Betrieb zu verwenden. Dazu können Sie das Installationspaket \client\esstools.msi verwenden.

Führen Sie die Installation mit dem Benutzerkonto durch, das zur Administratorengruppe auf dem geschützten Gerät gehört, auf dem das Programm installiert ist.

Wenn die Datei \exec\ess_win.msi auf dem geschützten Gerät ohne zusätzliche Befehlszeilenoptionen ausgeführt wird, wird Kaspersky Embedded Systems Security mit den Standardinstallationseinstellungen installiert.

Sie können die Auswahl der zu installierenden Komponenten mit dem Schlüssel ADDLOCAL festlegen und als Werte die Codes der ausgewählten Komponenten oder Komponentensätze verwenden.

Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer

Die Datei \product_long_term\ess_win.msi dient zur Installation von Kaspersky Embedded Systems Security in der Konfiguration **Computer mittels Default Deny-Technologie schützen**. Die Datei \exec\ess_win.msi dient zur Installation von Kaspersky Embedded Systems Security in der Konfiguration **Computer mittels Antiviren-Datenbanken schützen**.

Wenn die Konfiguration **Computer mittels Antiviren-Datenbanken schützen** ausgewählt ist, sind standardmäßig alle Komponenten von Kaspersky Embedded Systems Security enthalten, unter Ausnahme der Komponenten Firewall und Leistungsindikatoren.

Wenn Sie die Programmkonfiguration **Computer mittels Antiviren-Datenbanken schützen** über eine Programmversion installieren, die keine Signaturanalyse und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz der Programmkomponenten automatisch erweitert. Dazu werden die folgenden Komponenten hinzugefügt:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Schutz vor Netzwerkbedrohungen

Die Komponenten, die Updates ermöglichen, sind nicht in der Konfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** enthalten.

Wenn die Konfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** ausgewählt ist, sind standardmäßig die folgenden Komponenten enthalten:

- Exploit-Prävention
- Kontrolle des Programmstarts
- Systemfachsymbol

Wenn Sie die Programmkonfiguration **Computer durch die Technologie „Standardmäßig ablehnen“ schützen** über eine Programmversion installieren, die Signaturanalyse- und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz von Programmkomponenten automatisch reduziert, indem die folgende Komponente entfernt wird:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Komponenten, die Updates ermöglichen

Diese Konfiguration wird zum Schutz von Geräten mit begrenzten Ressourcen empfohlen. In diesem Fall können Sie das Programm langfristig aktivieren, und die Komponente Kontrolle des Programmstarts sorgt für den Schutz des Computers.

Die Datei \console\esstools.msi dient zur Installation der Konsole von Kaspersky Embedded Systems Security.

Die folgenden Tabellen enthalten Kennzeichnungen und Beschreibungen der Programmkomponenten von Kaspersky Embedded Systems Security.

Beschreibung der Programmkomponenten von Kaspersky Embedded Systems Security

Komponente	Code	Funktionen der Komponente
Echtzeitschutz für Dateien	`FileThreatProtection`	Diese Komponente führt auf dem geschützten Gerät eine Untersuchung von Dateien auf Viren durch, sobald auf diese Dateien zugegriffen wird.
AMSI-Untersuchung	`AMSI`	Diese Komponente dient der Unterstützung der Microsoft-Schnittstelle „Antimalware Scan Interface“. Mithilfe Schnittstelle für Antimalware Scan Interface (AMSI) können Dritthersteller-Anwendungen, die AMSI unterstützen, Objekte (z. B. PowerShell-Skripte) für eine zusätzliche Untersuchung an Kaspersky Embedded Systems Security senden und Untersuchungsergebnisse für diese Objekte erhalten.
Verhaltensanalyse	`BehaviorDetection`	Diese Komponente trägt die Namen von Remote-Geräten, die schädliche Aktivitäten zeigen, in die Liste der blockierten Hosts ein.

Komponente	Code	Funktionen der Komponente
Exploit-Prävention	`ExploitPrevention`	Diese Komponente ermöglicht die Verwaltung der Einstellungen zum Schutz des Prozess-Speichers im Speicher des Geräts.
Rollback von schädlichen Aktionen	`RemediationEngine`	Mithilfe dieser Komponente kann Kaspersky Embedded Systems Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.
Firewall	`Firewall`	Diese Komponente ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Embedded Systems Security zu verwalten.
Schutz vor Netzwerkbedrohungen	`NetworkThreatProtection`	Diese Komponente untersucht eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind. Wird ein versuchter Netzwerkangriff erkannt, der auf den Computer abzielt, blockiert Kaspersky Embedded Systems Security die Netzwerkaktivitäten vom angreifenden Computer.
Kontrolle des Programmstarts	`ApplicationControl`	Diese Komponente überwacht die Versuche von Benutzern, Programme zu starten, und erlaubt oder verbietet den Programmstart in Übereinstimmung mit den angegebenen Regeln für die Kontrolle des Programmstarts.
Gerätekontrolle	`DeviceControl`	Diese Komponente überwacht die Verbindungsversuche von externen Geräten auf einem geschützten Gerät und verbietet oder erlaubt deren Verwendung entsprechend den festgelegten Regeln für die Gerätekontrolle.
Modul für die Integration in den Kaspersky Security Center Administrationsagenten	`AdminKitConnector`	Koordination der Verbindung zwischen dem Server von Kaspersky Embedded Systems Security und dem Netzwerkagenten von Kaspersky Security Center. Sie können diese Komponente auf dem geschützten Gerät installieren, wenn Sie vorhaben, das Programm über Kaspersky Security Center zu verwalten.
Protokollanalyse	`LogInspector`	Diese Komponente führt eine Integritätsprüfung des geschützten Mittwochs auf Grundlage der Ergebnisse der Protokollanalyse von Windows-Ereignissen aus.
Überwachung der Systemintegrität	`SystemIntegrityMonitor`	Diese Komponente enthält alle Funktionen der Überwachung der Datei-Integrität und ermöglicht zusätzlich die Überwachung von Registrierungsänderungen und angeschlossenen Geräten.
Schutz vor BadUSB-Angriffen	`BadUSBAttackPrevention`	Die Komponente verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden.
Managed Detection and Response	`MDR`	Diese Komponente vereinfacht die Interaktion mit der Kaspersky Managed Detection and Response-Lösung.

Installations- und Wiederherstellungseinstellungen und Befehlszeilenoptionen für Windows Installer

In diesem Abschnitt werden die Installations- und Wiederherstellungseinstellungen für Kaspersky Embedded Systems Security beschrieben. Der Abschnitt enthält auch die Schlüssel zum Ändern der Installationseinstellungen sowie mögliche Schlüsselwerte. Sie können diese Schlüssel gemeinsam mit den Standardschlüsseln für den Befehl `msiexec` des Dienstes Windows Installer verwenden, wenn Sie Kaspersky Embedded Systems Security aus der Befehlszeile installieren.

Installationseinstellungen und Befehlszeilenoptionen für Windows-Installer

- Akzeptieren der Bedingungen des Endbenutzer-Lizenzvertrags.

  `EULA=<value>` kann folgende Werte annehmen.

  - `0` – Sie lehnen die Bedingungen des Endbenutzer-Lizenzvertrags ab (Standardwert).
  - `1` – Sie akzeptieren die Bedingungen des Endbenutzer-Lizenzvertrags.

- Akzeptieren der Bedingungen der Datenschutzrichtlinie

  `PRIVACYPOLICY=<value>` kann folgende Werte annehmen.

  - `0` – Sie lehnen die Bedingungen der Datenschutzrichtlinie ab (Standardwert).
  - `1` – Sie akzeptieren die Bedingungen der Datenschutzrichtlinie.

- Zielordner, in dem die Dateien für Kaspersky Embedded Systems Security während der Installation gespeichert werden. Sie können einen anderen Ordner angeben.

  Die Standardwerte für die Befehlszeilenoption `INSTALLDIR=<full path to the folder>` lauten wie folgt:

  - Für die 32-Bit-Version von Microsoft Windows:
    - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0
    - Konsole für Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Console 4.1.0
  - Für die 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%, der Rest der Pfade entspricht jenen für die 32-Bit-Versionen von Microsoft Windows.

- Die Aufgabe *Echtzeitschutz für Dateien* wird sofort nach dem Start von Kaspersky Embedded Systems Security gestartet.

  `RUNRTP=<value>` kann folgende Werte annehmen.

  - `1` – starten (Standardwert)
  - `0` – nicht starten

- Pfad der Schlüsseldatei (`LICENSEKEYPATH`). Standardmäßig versucht das Windows-Installationsprogramm, die Datei mit der Erweiterung .key im Ordner \exec des Distributionskits zu finden. Wenn der Ordner \exec mehrere Schlüsseldateien enthält, wählt Windows Installer die Schlüsseldatei aus, deren Ablaufdatum am weitesten in der Zukunft liegt. Eine Schlüsseldatei kann zuvor im Ordner \exec oder in einem anderen Pfad gespeichert werden, den Sie im Parameter `LICENSEKEYPATH` angeben können.

  `LICENSEKEYPATH` kann folgende Werte annehmen.

  - Vollständiger Pfad zur Schlüsseldatei, einschließlich des Namens.
  - Pfad zum Ordner, in dem die Schlüsseldateien gespeichert sind.

  Sie können nach der Installation von Kaspersky Embedded Systems Security einen Schlüssel mithilfe der von Ihnen gewählten Administrations-Tools hinzufügen, zum Beispiel mit der Programmkonsole. Wenn Sie während der Programminstallation keinen Programmschlüssel hinzufügen, funktioniert Kaspersky Embedded Systems Security nicht.

- Pfad der Konfigurationsdatei. Kaspersky Embedded Systems Security importiert die Einstellungen aus der angegebenen, im Programm erstellten Konfigurationsdatei. Kennwörter, wie z.B. Kennwörter von Konten für den Start von Aufgaben oder Kennwörter für die Verbindung mit einem Proxyserver, werden von Kaspersky Embedded Systems Security nicht aus der Konfigurationsdatei importiert. Nach dem Import der Parameter müssen alle Kennwörter manuell eingegeben werden. Wenn Sie die Konfigurationsdatei nicht angeben, beginnt das Programm nach der Installation mit den Standardparametern zu arbeiten.

  Der Standardwert für `CONFIGPATH=<configuration file name>` ist nicht festgelegt.

- Modus für *Untersuchung beim Start des Betriebssystems* (`SCANSTARTUP_BLOCKING`). Wenn Kaspersky Embedded Systems Security ohne den Schlüssel `SCANSTARTUP_BLOCKING` installiert wurde, wird der Parameter **Untersuchungsbereich** in der Aufgabe *Untersuchung beim Start des Betriebssystems* wie folgt festgelegt:

  - Aktion für infizierte und andere Objekte: **Informieren**.
  - Aktion für möglicherweise infizierte Objekte: **Informieren**.

  Wenn Kaspersky Embedded Systems Security mit dem Schlüssel `SCANSTARTUP_BLOCKING` installiert wurde, wird der Parameter **Untersuchungsbereich** in der Aufgabe *Untersuchung beim Start des Betriebssystems* wie folgt festgelegt:

  - Aktion für infizierte und andere Objekte: **Perform recommended action**.
  - Aktion für möglicherweise infizierte Objekte: **Perform recommended action**.

  Die Aufgabe *Untersuchung beim Start des Betriebssystems* wird automatisch erstellt. Der Modus **Informieren** wird standardmäßig verwendet. In diesem Fall können Sie nach der Bereitstellung von Kaspersky Embedded Systems Security auf den Geräten die Aufgabe *Untersuchung beim Start des Betriebssystems* aktivieren, vorausgesetzt, bei der Untersuchung wurden keine Probleme mit Systemdiensten festgestellt. Wenn das Programm kritische Systemdienste als infiziert oder möglicherweise infizierte Objekte erkennt, können Sie im Modus **Informieren** den Grund ermitteln und das Problem beheben. Wenn das Programm den Modus **Perform recommended action** verwendet, wird die Aktion **Disinfect. Delete if disinfection fails** ausgeführt. Die Desinfektion oder Entfernung von Systemdateien kann zu kritischen Problemen beim Starten des Betriebssystems führen.

- Überprüfung auf nicht kompatible Software deaktivieren. Verwenden Sie diese Einstellung, um die Überprüfung auf inkompatible Software während der Hintergrund-Installation des Programms auf dem geschützten Gerät zu aktivieren oder zu deaktivieren. Unabhängig vom Wert dieser Einstellung warnt das Programm bei der Installation von Kaspersky Embedded Systems Security immer vor anderen Versionen des Programms, die auf dem geschützten Gerät installiert sind.

  Für die Befehlszeilenoption `SKIPPRODUCTCHECK=<value>` sind folgende Werte möglich (Sie können auch `SKIPINCOMPATIBLESW=<value>` verwenden):

  - `0` – Die Überprüfung auf nicht kompatible Software wird ausgeführt (Standardwert)
  - `1` – Die Überprüfung auf nicht kompatible Software wird nicht ausgeführt

- Automatisches Entfernen von gefundener inkompatibler Software deaktivieren.

  Wenn die Option `SKIPPRODUCTUNINSTALL=1` angegeben wird, entfernt Kaspersky Embedded Systems Security inkompatible Software nicht. Wenn diese Option nicht angegeben wird, versucht Kaspersky Embedded Systems Security automatisch, inkompatible Software zu entfernen.

  > Wenn Kaspersky Embedded Systems Security mithilfe des Installationsprogramms msiexec installiert wurde, wird inkompatible Software nicht entfernt. Wenn Sie Programme, die Kompatibilitätsprobleme verursachen können, automatisch entfernen möchten, verwenden Sie die Datei „setup_ess.exe“.

- Deaktivieren der Suche nach dem Betriebssystem-Update KB5007186.

Nach der Installation des Updates KB5007186 funktioniert das Programm normal weiter. Die Systemsicherheit wird nicht beeinträchtigt, aber kleinere Programmversions-Updates sind nicht mehr möglich. Bevor das Programm wird installiert, überprüft das Installationsprogramm die installierten Betriebssystem-Updates. Wenn das Update KB5007186 gefunden wird, bricht das Installationsprogramm die Installation ab. Sie können den Schlüssel `SKIPKB5007186CHECK` in der Befehlszeile verwenden, um die Suche nach dem Betriebssystem-Update KB5007186 zu aktivieren oder zu deaktivieren.

`SKIPKB5007186CHECK=<value>` kann folgende Werte annehmen.

- `0` – Das Installationsprogramm überprüft, ob das Betriebssystem-Update KB5007186 installiert ist.
- `1` – Das Installationsprogramm überprüft nicht, ob das Betriebssystem-Update KB5007186 installiert ist.

Standardmäßig ist der Schlüssel nicht festgelegt, was dem Wert 0 entspricht.

- Konfigurieren der Funktionalität zum Schutz von Betriebssystemdiensten.

  Wenn diese Funktion aktiviert ist, können Drittanbieter-Programme die Prozesse des Betriebssystems nicht beeinflussen. `PROTECTOSSERVICES=<value>` kann folgende Werte annehmen.

  - `1` bedeutet, dass der Schutz für Betriebssystemdienste aktiviert ist (Standardeinstellung).
  - `0` bedeutet, dass der Schutz für Betriebssystemdienste deaktiviert ist.

- Konfiguration der Ports, die für die Remote-Verbindung der Programmkonsole mit einem Computer verwendet wird, auf dem das Programm installiert ist:

  Den Port für die Verbindung mit Windows-Anmeldedaten können Sie mithilfe des Parameters `UIPORT=<port number>` konfigurieren. Bereich der möglichen Portnummern: 1 bis 65535. Wenn die Nummer außerhalb des angegebenen Bereichs liegt, wird die standardmäßige Portnummer verwendet. Der Standardwert ist 13032.

  Bei Bedarf können Sie den Port für die Verbindung mit Anmeldedaten manuell erstellter Benutzer mithilfe des Parameters `ENABLEUIKLPORT=<value>` schließen:

  - `1` öffnet den Port (Standardeinstellung).
  - `0` schließt den Port.

  Der Standardwert für diesen Port ist 13031. Sie können die Portnummer ändern, indem Sie den Parameter `UIKLPORT=<value>` angeben. Bereich der möglichen Portnummern: 1 bis 65535.

- Einstellung für die Aktivierung von Netzwerkverbindungen für die Fernverwaltung von Kaspersky Embedded Systems Security mithilfe der Anwendungskonsole, die auf einem anderen Computer installiert ist.

  `ADDWFEXCLUSION=<value>` kann folgende Werte annehmen.

  - `1` Wenn dieser Wert angegeben ist, werden in der Windows-Firewall die TCP-Ports geöffnet, die für die Remote-Verbindung der Programmkonsole mit einem Computer, auf dem das Programm installiert ist, konfiguriert wurden (Parameter `UIPORT=<value>` und `UIKLPORT=<value>`), und für die ausführbare Datei des Remote-Verwaltungsprozesses von Kaspersky Embedded Systems Security (avp.exe) werden Netzwerkverbindungen zugelassen.

    Lesen Sie auch die Informationen über die zusätzliche Konfiguration bei der Installation des Programms auf einem anderen Gerät.

  - `0` Wenn dieser Wert angegeben ist, erfolgt keine Aktion.

- Überspringen der Installation des Stammzertifikats DigiCert Assured ID Root CA in den Betriebssystemspeicher für vertrauenswürdige Zertifikate.

  Wenn die Option `SKIPINSTALLROOTCACERTIFICATES` bei der Programminstallation angegeben wird, wird das Stammzertifikat DigiCert Assured ID Root CA nicht installiert. Standardmäßig wird das Zertifikat automatisch aus dem Programminstallationspaket installiert.

Wiederherstellungseinstellungen und Befehlszeilenoptionen für Windows Installer

- Wiederherstellung von Objekten aus der Quarantäne

  `RESTOREQTN=<value>` kann folgende Werte annehmen.

  - `0` – in Quarantäne verschobenen Inhalt entfernen (Standardwert)
  - `1` – Inhalt der Quarantäne im Unterordner \QB im Ordner wiederherstellen, der mit der Einstellung RESTOREPATH vorgegeben ist

- Wiederherstellen des Backup-Inhalts

  `RESTOREBCK=<value>` kann folgende Werte annehmen.

  - `0` – ins Backup verschobenen Inhalt entfernen (Standardwert)
  - `1` – Inhalt des Backups in dem Unterordner \QB im Ordner wiederherstellen, der mit der Einstellung RESTOREPATH vorgegeben ist

- Eingabe des aktuellen Kennworts, um die Deinstallation zu bestätigen (wenn der Kennwortschutz aktiviert ist).

  Der Standardwert für `UNLOCK_PASSWORD=<specified password>` ist nicht festgelegt.

- Ordner für wiederhergestellte Objekte Wiederhergestellte Objekte werden im angegebenen Ordner gespeichert.

  Der Standardwert für die Befehlszeilenoption `RESTOREPATH=<full path to the folder>` lautet %ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KESS.4.1.0\QB\Restored

Beispiele von Befehlen für die Installation von Kaspersky Embedded Systems Security

Dieser Abschnitt bietet Beispiele für Befehle zur Installation von Kaspersky Embedded Systems Security.

Führen Sie auf dem geschützten Gerät die Datei ess_win.msi aus dem Lieferumfang aus.

Detaillierte Informationen über die Verwendung von Standardbefehlen und Schlüsseln des Dienstes Windows Installer finden Sie in der Dokumentation der Firma Microsoft.

Beispiele für die Installation von Kaspersky Embedded Systems Security aus der Datei setup_ess.exe

Um Kaspersky Embedded Systems Security mit den empfohlenen Installationseinstellungen und ohne Benutzerbeteiligung zu installieren:

```
\exec\setup_ess.exe EULA=1 PRIVACYPOLICY=1
```

Zur Installation von Komponenten, z. B. Gerätekontrolle:

```
\exec\setup_ess.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0
```

Bei der Installation von Kaspersky Embedded Systems Security auf Computern mit Netzwerkgeräten und SCSI-Geräten, die nach der Installation einen Systemabsturz verursachen, können Sie die folgenden zusätzlichen Optionen mit diesem Befehl verwenden:

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

Aktiviert (`1`) oder deaktiviert (`0`) das Abfangen von Verbindungen von Netzwerkadaptern.

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

Aktiviert (`1`) oder deaktiviert (`0`) das Abfangen von Verbindungen von SCSI-Adaptern.

Um Kaspersky Embedded Systems Security zu installieren und mithilfe der Schlüsseldatei zu aktivieren:

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

So ändern Sie den Port, der für die Remote-Verbindung der Programmkonsole mit einem Computer verwendet wird, auf dem das Programm mit Windows-Anmeldedaten installiert wurde:

```
setup_ess.exe /pUIPORT=<port number>
```

Bereich der möglichen Portnummern: 1 bis 65535. Der Standardwert ist 13032.

Liste der Installationsbefehle: Starten einer msi-Datei

Um Kaspersky Embedded Systems Security mit den empfohlenen Installationseinstellungen und ohne Benutzerbeteiligung zu installieren:

```
msiexec /i ess_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security mit den empfohlenen Installationseinstellungen zu installieren und die Installationsoberfläche anzuzeigen:

```
msiexec /i ess_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

Führen Sie den folgenden Befehl aus, um Kaspersky Embedded Systems Security mit den empfohlenen Installationseinstellungen zu installieren und die Rotation der Ablaufverfolgungsdateien zu aktivieren, wenn die Anzahl der Ablaufverfolgungsdateien die festgelegte maximale Anzahl erreicht hat:

```
msiexec /i ess_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1 PRIVACYPOLICY=1
```

Der Parameter `TRACE_FOLDER` ist erforderlich.

Für den Parameter `TRACE_MAX_ROLL_COUNT` gelten die folgenden Regeln:

- Wenn dieser Parameter angegeben ist, wird die Rotation der Ablaufverfolgungsdateien aktiviert, wenn die Anzahl der Ablaufverfolgungsdateien die im Parameter angegebene maximale Anzahl erreicht hat. Verfügbarer Wertebereich der Parameter: von 1 bis 999.

- Wenn als maximale Anzahl von Ablaufverfolgungsdateien 0 angegeben ist, ist die Rotation der Ablaufverfolgungsdateien deaktiviert.

- Wenn ein Parameterwert angegeben wird, aber ungültig ist oder außerhalb des Bereichs der verfügbaren Werte (von 1 bis 999) liegt, wird die Rotation der Ablaufverfolgungsdateien aktiviert und die standardmäßige maximale Anzahl von Ablaufverfolgungsdateien auf 5 festgelegt.

- Wenn der Parameter nicht angegeben ist:

  - Wenn die Rotation der Ablaufverfolgungsdateien bereits auf dem Gerät konfiguriert ist, werden ihre Einstellungen nicht geändert. Das Programm ignoriert die eingegebenen Parameter.

  - Wenn die Rotation der Ablaufverfolgungsdateien auf dem Gerät nicht konfiguriert ist, wird die Rotationsoption aktiviert und die maximale Anzahl von Ablaufverfolgungsdateien standardmäßig auf 5 festgelegt.

Um Kaspersky Embedded Systems Security zu installieren und mithilfe der Schlüsseldatei C:\0000000A.key zu aktivieren:

```
msiexec /i ess_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

Führen Sie den folgenden Befehl aus, um Kaspersky Embedded Systems Security mit einer vorherigen Untersuchung der aktiven Prozesse und Bootsektoren der lokalen Computerlaufwerke zu installieren:

```
msiexec /i ess_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security in dem Installationsordner C:\KESS zu installieren:

```
msiexec /i ess_win.msi INSTALLDIR=C:\KESS/qn EULA=1 PRIVACYPOLICY=1
```

Führen Sie den folgenden Befehl aus, um Kaspersky Embedded Systems Security zu installieren und eine Installationsprotokolldatei mit dem Namen "ess.log" im Ordner zu speichern, in dem die msi-Datei von Kaspersky Embedded Systems Security gespeichert ist:

```
msiexec /i ess_win.msi/l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

So installieren Sie die Konsole für Kaspersky Embedded Systems Security:

```
msiexec /i esstools.msi /qn EULA=1
```

Führen Sie den folgenden Befehl aus, um Kaspersky Embedded Systems Security zu installieren und mithilfe der Schlüsseldatei "C:\0000000A.key" zu aktivieren und um Kaspersky Embedded Systems Security gemäß den Einstellungen in der Konfigurationsdatei "C:\settings.xml" anzupassen:

```
msiexec /i ess_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

Führen Sie den folgenden Befehl aus, um einen Programmpatch zu installieren, wenn Kaspersky Embedded Systems Security kennwortgeschützt ist:

```
msiexec /p "<MSP file path>" UNLOCK_PASSWORD=<password>
```

Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen

Wenn Sie das Programm aktiviert haben, startet Kaspersky Embedded Systems Security die Aufgaben zum Schutz und zur Untersuchung sofort nach der Installation. Wenn das Kontrollkästchen **Echtzeitschutz für Dateien nach der App-Installation aktivieren (empfohlen)** während der Installation von Kaspersky Embedded Systems Security aktiviert ist, untersucht das Programm die Objekte des Gerätedateisystems, wenn darauf zugegriffen wird. Wenn die Komponente Skript-Überwachung im Rahmen einer benutzerdefinierten Installation installiert wurde, untersucht Kaspersky Embedded Systems Security den Quellcode aller Skripte, wenn diese gestartet werden. Kaspersky Embedded Systems Security führt die Aufgabe *Untersuchung wichtiger Bereiche* jeden Freitag um 20:00 Uhr aus.

Wir empfehlen Ihnen, nach der Installation von Kaspersky Embedded Systems Security die folgenden Schritte auszuführen:

- Starten Sie die Update-Aufgabe für Kaspersky Embedded Systems Security. Nach der Installation untersucht Kaspersky Embedded Systems Security Objekte anhand von Datenbanken, die im Lieferumfang enthalten sind. Wir empfehlen Ihnen, die Datenbank von Kaspersky Embedded Systems Security sofort zu aktualisieren. Starten Sie dazu die Aufgabe *Update*. Danach wird das Update nach dem standardmäßigen Zeitplan jede Stunde ausgeführt.

  Mit dem folgenden Befehl können Sie beispielsweise die Aufgabe *Update* starten:

  ```
  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
  ```

  Dabei werden die Datenbanken-Updates für Kaspersky Embedded Systems Security von den Kaspersky-Update-Servern heruntergeladen.

- Starten Sie die Aufgabe *Untersuchung wichtiger Bereiche*, wenn vor der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät kein Virenschutzprogramm mit Echtzeitschutz für Dateien installiert war.

  Die Aufgabe *Untersuchung wichtiger Bereiche* können Sie über die Befehlszeile mit dem folgenden Befehl starten:

  ```
  KAVSHELL SCANCRITICAL /W:scancritical.log
  ```

  Dieser Befehl speichert das Protokoll der Aufgabenausführung in der Datei scancritical.log im aktuellen Ordner.

- Passen Sie Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security an.

Komponenten hinzufügen und entfernen. Beispiele für Befehle

Um die Komponente Untersuchung auf Befehl zu installieren, führen Sie den folgenden Befehl aus:

```
msiexec /i ess_win.msi ADDLOCAL=Oas,Ods /qn
```

oder

```
\exec\setup_ess.exe /s /p ADDLOCAL=Oas,Ods
```

Wenn Sie die Komponenten zur Liste hinzugefügt haben, installiert Kaspersky Embedded Systems Security die bestehenden Komponenten neu und zusätzlich die angegebenen Komponenten.

Um installierte Komponenten zu löschen, führen Sie den folgenden Befehl aus:

```
msiexec /i ess_win.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

Um neue Komponenten zu installieren, führen Sie den folgenden Befehl aus:

```
msiexec /i ess_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas,Ods,SnmpSupport,TrayApp,IDS,
EULA=1 PRIVACYPOLICY=1 /qn
```

Wenn Sie die Komponenten, die Sie installieren oder entfernen möchten aufgelistet haben, installiert oder entfernt Kaspersky Embedded Systems Security die Komponenten entsprechend.

Deinstallation von Kaspersky Embedded Systems Security. Beispiele für Befehle

Um Kaspersky Embedded Systems Security im unbeaufsichtigten Modus von dem geschützten Gerät zu deinstallieren, führen Sie den folgenden Befehl aus:

```
msiexec /x ess_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

oder

```
msiexec /x {6202AB29-4AC2-4A92-AF8E-977AADD4B27F} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

oder

```
setup_ess.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

wobei `<user name>` für den Namen und Benutzernamen eines Benutzers steht, der über ausreichende Rechte für die Deinstallation verfügt.

Wenn für das Benutzerkonto, unter dem die Deinstallation ausgeführt wird, ein leeres Windows-Kennwort festgelegt ist, deaktivieren Sie die Funktion **Kennwort zur Bestätigung kritischer Aktionen abfragen**, bevor Sie mit der Deinstallation beginnen.

Um die Konsole für Kaspersky Embedded Systems Security im unbeaufsichtigten Modus zu deinstallieren, führen Sie den folgenden Befehl aus:

```
msiexec /x esstools.msi /qn
```

oder

```
msiexec /x {E827CBBA-974C-4386-B50E-8F202D41E428} /qn
```

Rückgabecodes

Das Installationsprogramm des Programms kann die in diesem Artikel beschriebenen Rückgabecodes zurückgeben.

In der nachfolgenden Tabelle werden die Feedback-Codes der Befehlszeile beschrieben.

Rückgabecodes

Code	Beschreibung
27100	Auf dem Computer wurden Laufwerke gefunden, auf denen ein Authentifizierungsagent im Testmodus installiert ist.
27101	Auf dem Computer wurden Laufwerke gefunden, auf denen ein Authentifizierungsagent im Testmodus installiert ist.

Code	Beschreibung
27102	Verschlüsselte Datenträger konnten nicht gefunden werden.
27200	Die Anwendung kann nicht aus dem Arbeitsspeicher entladen werden.
27201	Fehler beim Start des Prozesses AVP.exe. Ihr Computer ist möglicherweise infiziert.
27204	Zwischenspeicherung des Verteilungspakets ist fehlgeschlagen.
27205	Lizenzinformationen konnten nicht migriert werden.
27206	Lizenzinformationen konnten nicht entfernt werden.
27207	Inkompatible Software konnte nicht entfernt werden.
27208	Inkompatible Software konnte nicht überprüft werden.
27209	Dateien aus CAB-Datei konnten nicht extrahiert werden.
27210	Fehler beim Konfigurieren des „Selbstschutzes“.
27211	Fehler beim Aktivieren des „Selbstschutzes“.
27212	Informationen zur Betriebssystemversion konnten nicht abgerufen werden.
27213	Startverzeichnis konnte nicht abgerufen werden.
27214	Installationsverzeichnis konnte nicht überprüft werden.
27215	Fehler beim Konfigurieren des Dienstes.
27216	Fehler beim Konfigurieren von klcp.
27217	Fehler beim Upgrade von klcp.
27218	kl1-Treiberparameter konnten nicht konfiguriert werden.
27219	klelam-Treiberparameter konnten nicht konfiguriert werden.
27220	klwfp-Treiberparameter konnten nicht konfiguriert werden.
27221	Treiberkompatibilitätsmodus konnte nicht konfiguriert werden.
27222	Registrierungsschlüssel konnte nicht entfernt werden.
27223	Fehler beim Neustart des Betriebssystems.
27224	Treiber konnte nicht installiert werden.
27225	Treiber-Einstellungen konnten nicht migriert werden.
27226	Treiber konnte nicht angehalten werden.
27227	Der Start des Treibers konnte nicht blockiert werden.
27228	Die Signatur der Datei konnte nicht überprüft werden.
27230	Vorbereitung der kldl-Treiber-Einstellungen ist fehlgeschlagen.
27231	kldl-Treiber-Einstellungen konnten nicht konfiguriert werden.
27300	Fehler beim Installieren des Treibers.
27301	Fehler beim Entfernen des Treibers.
27302	Fehler bei der Installation der Netzwerkkomponenten.
27303	Die Registrierungsinformationen für den Treiber sind inkonsistent oder unvollständig. Bitte starten Sie das Betriebssystem neu und versuchen Sie es erneut.
27305	Fehler beim Deaktivieren des Treibers.
27310	Digital signierte Katalogdatei konnte nicht installiert werden.
27311	Digital signierte Katalogdatei konnte nicht deinstalliert werden.
27312	Installation von Zertifikaten fehlgeschlagen.
27313	Entfernen von Zertifikaten fehlgeschlagen.
27320	Fehler beim Konfigurieren des Dienstes.

Code	Beschreibung
27321	Fehler beim Deaktivieren des Schutzes für Dienst.
27350	Patch <Patch-Name> ist nicht für diese Sprachversion der Anwendung <Anwendungsname> vorgesehen.
27352	Ein Patch für die vollständige Festplattenverschlüsselung kann nicht entfernt werden.
27353	Patch <Name von Patch 1> kann nur zusammen mit Patch <Patch-Name von Patch 2> installiert werden.
27354	Bevor das Programm geändert oder repariert wird, muss der Computer neu gestartet werden, um Patches zu übernehmen.
27355	Die Verwaltung der vollständigen Festplattenverschlüsselung konnte nicht gesperrt werden. Die Verwaltung der vollständigen Festplattenverschlüsselung konnte nicht gesperrt werden. Sie müssen die Verschlüsselung zuerst abschließen, um ein Update für die vollständige Festplattenverschlüsselung zu installieren.
27356	Patch kann nicht installiert werden.
27357	Das Installationspaket enthält gesperrte Patches. Die Installation wird abgebrochen.
27360	Patch kann nicht registriert werden.
27361	Patch-Installationsparameter konnten nicht festgelegt werden.
27363	Patch enthält Verschlüsselungsbibliotheken, die inkompatibel sind mit den installierten Verschlüsselungsbibliotheken.
27370	Fehler beim Initialisieren des Entpackens von .NET 8.0.
27371	Fehler beim Entpacken von .NET 8.0.
27372	Registrierungsinformationen zur vorherigen App-Version wurden gelöscht. Bitte starten Sie die Installation neu.
27373	Registrierungsinformationen zur vorherigen Anwendungsversion konnten nicht gelöscht werden.
27374	Das Programm wird aktualisiert. Bitte versuchen Sie es später erneut.
27375	Das Kennwort oder der Benutzername zum Löschen der Anwendung wurde nicht festgelegt oder ist ungültig.
27376	Kaspersky Endpoint Agent konnte nicht deinstalliert werden. Bitte deinstallieren Sie das Programm manuell oder deaktivieren Sie den Kennwortschutz in den Einstellungen. Starten Sie anschließend erneut die Installation des Programms.
27377	Kaspersky Security für Windows Server konnte nicht deinstalliert werden. Bitte deinstallieren Sie das Programm manuell oder deaktivieren Sie den Kennwortschutz in den Einstellungen. Starten Sie anschließend erneut die Installation des Programms.
27378	Zu wenig Platz auf dem Laufwerk.
27379	Die App-Installation ist fehlgeschlagen, da inkompatible Komponenten ausgewählt wurden. Bitte ändern Sie die Komponentenauswahl und starten Sie die Installation erneut.
27380	Die ausgewählte Konfigurationsdatei ist ungültig.
27381	Die ausgewählte Lizenzdatei ist ungültig.
27382	Die Anwendungsadministrationsgruppe konnte nicht erstellt werden.
27383	Sie haben einen ungültigen Ordner ausgewählt. Der Name des Installationsordners für das Programm darf höchstens 160 Zeichen lang sein.
27384	Der gewählte Ordner oder das Laufwerk ist ungültig. Das Programm muss auf einer lokalen Festplatte installiert werden.
27385	Sie haben einen ungültigen Ordner ausgewählt. Das Programm kann nicht in einem Stammordner installiert werden.
27386	Sie haben einen ungültigen Ordner ausgewählt. Das Programm kann nicht im „Windows“-Ordner oder dessen Unterordnern installiert werden.
27387	Sie haben einen ungültigen Ordner ausgewählt. Das Programm kann nicht im Ordner installiert werden, in dem sich der „Temp“-Ordner befindet.
27388	Sie haben einen ungültigen Ordner ausgewählt. Das Programm kann nicht direkt im Ordner „Programme“ installiert werden.
27389	Sie haben einen ungültigen Ordner ausgewählt. Das Programm kann nicht auf einem virtuellen Laufwerk installiert werden.
27390	Der gewählte Ordner oder das Laufwerk ist ungültig. Das Programm kann nicht in einem Ordner installiert werden, in den die vorherige Programmversion installiert wurde.
27391	Der gewählte Ordner oder das Laufwerk enthält bereits Dateien. Das Programm kann nicht in einem Ordner installiert werden, der bereits Dateien enthält. Andernfalls können nach Aktivierung der Funktion zum Selbstschutz Probleme beim Zugriff auf diese Dateien auftreten.
27392	Das Programm kann nicht in einem Ordner installiert werden, der Analysepunkte (Reparse Points) enthält. Wählen Sie bitte einen anderen Installationsordner.
27393	Dieses Programm kann nicht in einen Ordner installiert werden, in dessen Namen ';' verwendet wird. Wählen Sie bitte einen anderen Installationsordner.

Code	Beschreibung
27394	Sie haben einen ungültigen Ordner ausgewählt. Sie haben einen ungültigen Ordner ausgewählt.
27395	Sie haben einen ungültigen Ordner ausgewählt. Der Ordner „Windows“ oder dessen Unterordner können nicht angegeben werden.
27396	Sie haben einen ungültigen Ordner ausgewählt. Der Ordner „Programme“ kann nicht direkt angegeben werden.
27397	Sie haben einen ungültigen Ordner ausgewählt. Ein Ordner, der einen „Temp“-Unterordner enthält, kann nicht angegeben werden.
27400	Fehler beim Initialisieren von Datei-Updates.
27450	CAB-Datei konnte nicht installiert werden.
27451	Fehler beim Entfernen.
27452	Fehler beim Entfernen von Dateien.
27453	Fehler beim Verschieben von Dateien.
27454	Registrierungsdateien konnten nicht erstellt werden.
27455	Informationen zur Betriebssystemversion konnten nicht abgerufen werden.
27456	Rollback von Registrierungswerten konnte nicht geplant werden.
27457	Bekannte Sicherheits-IDs (SIDs) konnten nicht abgerufen werden.
27460	Fehler beim Erstellen der Sicherheitsdeskriptoren.
27461	Fehler beim Wiederherstellen von Sicherheitsdeskriptoren.
27462	Regeln für Microsoft Windows-Firewall konnten nicht erstellt werden.
27463	Regeln für Microsoft Windows-Firewall konnten nicht gelöscht werden.

Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center

Dieser Abschnitt enthält Informationen über die Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center, eine Beschreibung der Vorgehensweise für die Installation und Deinstallation von Kaspersky Embedded Systems Security über Kaspersky Security Center und eine Beschreibung der Aktionen, die nach der Installation von Kaspersky Embedded Systems Security Kaspersky Embedded Systems Security sind für Windows ist installiert.

Allgemeine Informationen zur Installation über Kaspersky Security Center

Sie können Kaspersky Embedded Systems Security mithilfe einer Remote-Installationsaufgabe über Kaspersky Security Center installieren.

Nach Abschluss der Remote-Installationsaufgabe ist Kaspersky Embedded Systems Security auf mehreren geschützten Geräten mit einheitlichen Einstellungen installiert.

Alle geschützten Geräte können in eine einzige Administrationsgruppe zusammengeführt werden und Sie können eine Gruppenaufgabe zur Installation von Kaspersky Embedded Systems Security auf den geschützten Geräten dieser Gruppe erstellen.

Sie können eine Remote-Installationsaufgabe für Kaspersky Embedded Systems Security erstellen, die sich auf eine Auswahl von geschützten Geräten bezieht, die nicht zur gleichen Administrationsgruppe gehören. Wenn Sie diese Aufgabe erstellen, müssen Sie die Liste der einzelnen geschützten Geräte anlegen, auf denen Kaspersky Embedded Systems Security installiert werden soll.

Ausführliche Informationen über die Aufgabe zur Remote-Installation finden Sie im Hilfesystem von Kaspersky Security Center.

Rechte zur Installation bzw. Deinstallation von Kaspersky Embedded Systems Security

Das Benutzerkonto, das Sie in der Aufgabe zur Remote-Installation (Deinstallation) angeben, muss auf jedem der geschützten Geräte zur Administratorengruppe gehören. Dies gilt in allen Fällen unter Ausnahme der folgenden:

- Auf den geschützten Geräten, auf denen Sie Kaspersky Embedded Systems Security installieren möchten, ist bereits der Kaspersky Security Center Administrationsagent installiert (unabhängig davon, in welcher Domäne sich die geschützten Geräte befinden und ob sie zu einer Domäne gehören).

  Wenn der Administrationsagent noch nicht auf den geschützten Geräten installiert ist, können Sie ihn im Rahmen der Remote-Installationsaufgabe zusammen mit Kaspersky Embedded Systems Security installieren. Bevor Sie den Administrationsagenten installieren, vergewissern Sie sich, dass das Benutzerkonto, das Sie in der Aufgabe angeben, auf allen geschützten Geräten zur Gruppe der lokalen Administratoren gehört.

- Alle geschützten Geräte, auf denen Sie Kaspersky Embedded Systems Security installieren möchten, gehören zur gleichen Domäne wie der Administrationsserver, und der Administrationsserver ist als das Benutzerkonto **Domain-Administrator** (Domain Admin) registriert (wenn dieses Benutzerkonto über die Rechte eines Administrators auf den geschützten Geräten der Domäne verfügt).

Die Aufgabe zur Remote-Installation mit der **Push-Installation** Methode wird standardmäßig mit dem Benutzerkonto, unter dem der Administrationsserver läuft, ausgeführt.

In Gruppenaufgaben und in den Aufgaben für die Gerätesätze, die Push-Installationsmethode (Deinstallationsmethode) nützen, muss das Benutzerkonto auf dem geschützten Gerät über die folgende Rechte verfügen:

- Recht zur Remote-Ausführung von Apps
- Rechte für die **Admin$**-Freigabe
- Recht zur **Anmeldung als Dienst**

Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center

Zur Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center gehören die folgenden Schritte:

1. **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.

   So erstellen Sie ein Installationspaket (in der Kaspersky Security Center Verwaltungskonsole)

   1. Wählen Sie in der Struktur der Kaspersky Security Center Verwaltungskonsole den Ordner **Erweitert** → **Remote-Installation** → **Installationspakete** aus.
   2. Klicken Sie im Ergebnisbereich auf die Schaltfläche **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 Embedded Systems Security*).

Schritt 3. Programmpaket für die Installation auswählen

Geben Sie die Datei ess_win.kud aus dem Lieferumfang von Kaspersky Embedded Systems Security als Installationspaketdatei an.

Wenn Sie beabsichtigen, das Programm mit der Konfiguration **Computer mittels Antiviren-Datenbanken schützen** über die Programmkonfiguration zu installieren, die zum Schutz des Computers keine Signaturanalyse und Antiviren-Datenbanken verwendet, oder umgekehrt, müssen Sie zuerst den Benutzernamen und das Kennwort des Benutzerkontos mit den Berechtigungen zur Programminstallation in der Datei ess_win.kud angeben. Öffnen Sie dazu die Datei ess_win.kud in einem Texteditor und fügen Sie der Zeile `Params` die folgenden Parameter hinzu: `/pKLLOGIN=<login>` und `/pKLPASSWD=<password>`.

Aktivieren Sie bei Bedarf das Kontrollkästchen **Updates aus der Datenverwaltung ins Installationspaket kopieren**, um die Antiviren-Datenbanken im Installationspaket zu aktualisieren.

Schritt 4. Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie

Wenn Sie den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie zustimmen, aktivieren Sie die Kontrollkästchen **Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe, und sie verstehe und akzeptiere** und **Ich bin mir bewusst und damit einverstanden, dass meine Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe**.

Sie müssen den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie akzeptieren, um fortzufahren.

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

So ändern Sie den Umfang der zu installierenden Komponenten von Kaspersky Embedded Systems Security und die standardmäßigen Installationseinstellungen im erstellten Installationspaket:

1. Öffnen Sie in der Kaspersky Security Center-Verwaltungskonsole den Knoten **Remote-Installation**.
2. Öffnen Sie im Ergebnisbereich des untergeordneten Knotens **Installationspakete** das Kontextmenü für das erstellte Installationspaket von Kaspersky Embedded Systems Security und wählen Sie **Eigenschaften** aus.
3. Öffnen Sie im Fenster **Eigenschaften: <Name des Installationspakets>** den Abschnitt **Einstellungen**.
4. Konfigurieren Sie die vertrauenswürdige Zone. Klicken Sie dazu auf **Konfigurieren**.
5. Aktivieren Sie im Block **Komponentenauswahl** die Kontrollkästchen neben den Namen der Komponenten von Kaspersky Embedded Systems Security, die Sie installieren möchten.
6. Aktivieren Sie im Block **Modus „Echtzeitschutz für Dateien“** das Kontrollkästchen **Echtzeitschutz für Dateien nach der App-Installation aktivieren (empfohlen)** und wählen Sie den Funktionsmodus der Komponente aus.
7. Ändern Sie gegebenenfalls die TCP-Portnummern, die die Programmkonsole für die Remote-Verbindung mit dem Computer verwendet, auf dem das Programm installiert ist.

   Die Standardportnummer für die Verbindung mit Windows-Anmeldedaten ist 13032, und die Standardportnummer für die Verbindung mit Anmeldedaten manuell erstellter Benutzer ist 13031. Bereich der möglichen Portnummern: 1 bis 65535.

   Um eine Verbindung mit den Anmeldedaten manuell erstellter Benutzerkonten zu verhindern, deaktivieren Sie das Kontrollkästchen **Mittels Anmeldedaten von manuell erstellten Benutzern**.
8. Um einen Installationsordner anzugeben, der nicht dem standardmäßigen Ordner entspricht, geben Sie im Block **Installationspfade des Programms konfigurieren** den Namen und Pfad des Ordners an. Klicken Sie dazu auf die Schaltfläche **Einstellungen**.
9. Um das Programm mit vordefinierten Einstellungen zu installieren, laden Sie die Konfigurationsdatei hoch.
10. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie ein Installationspaket (in der Web Console)

1. Führen Sie einen der folgenden Schritte aus:

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

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.

Außerdem können Sie ein Installationspaket aus einer Datei erstellen.

Schritt 2. Installationspakete

Wählen Sie das Installationspaket für Kaspersky Embedded Systems 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.

Sie müssen den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie akzeptieren, um fortzufahren.

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

So ändern Sie den Umfang der zu installierenden Komponenten von Kaspersky Embedded Systems Security und die standardmäßigen Installationseinstellungen im erstellten Installationspaket:

1. Klicken Sie im Fenster **Installationspakete** auf den Namen des erstellten Installationspakets für Kaspersky Embedded Systems Security.
2. Wählen Sie im folgenden Fenster die Registerkarte **Einstellungen** aus.
3. Wählen Sie den Abschnitt **Schutzkomponenten** aus.
4. Konfigurieren Sie die vertrauenswürdige Zone. Klicken Sie dazu auf **Anpassen**.

5. Aktivieren Sie im Abschnitt **Zu installierende Komponenten auswählen** die Kontrollkästchen neben den Namen der Komponenten von Kaspersky Embedded Systems Security, die Sie installieren möchten.

6. Aktivieren Sie im Block **Modus für den Echtzeitschutz für Dateien** das Kontrollkästchen **Echtzeitschutz für Dateien nach der App-Installation aktivieren (empfohlen)** und wählen Sie den Funktionsmodus der Komponente aus.

7. Ändern Sie gegebenenfalls die TCP-Portnummern, die die Programmkonsole für die Remote-Verbindung mit dem Computer verwendet, auf dem das Programm installiert ist.

   Die Standardportnummer für die Verbindung mit Windows-Anmeldedaten ist 13032, und die Standardportnummer für die Verbindung mit Anmeldedaten manuell erstellter Benutzer ist 13031. Bereich der möglichen Portnummern: 1 bis 65535.

   Um eine Verbindung mit den Anmeldedaten manuell erstellter Benutzerkonten zu verhindern, deaktivieren Sie das Kontrollkästchen **Port für Remote-Verbindung mittels Anmeldedaten von manuell erstellten Benutzern**.

8. Wählen Sie den Abschnitt **Installationseinstellungen** aus.

9. Konfigurieren Sie im Abschnitt **Erweiterte Einstellungen** die folgenden Einstellungen:

   - **Pfad des Programms zur Umgebungsvariablen „%PATH%“ hinzufügen**. Sie können den Installationspfad zur Variablen %PATH% hinzufügen, um das Programm bequem über die Befehlszeile zu verwalten.

   - **Symbol im Infobereich der Taskleiste anzeigen**. Wenn das Kontrollkästchen aktiviert ist, wird das Programmsymbol nach der Installation von Kaspersky Embedded Systems Security im Infobereich der Microsoft Windows-Taskleiste angezeigt.

10. Deaktivieren Sie bei Bedarf die Funktionalität **Installationsprozess schützen**.

11. Ändern Sie bei Bedarf die Standardordner, die während der Programminstallation auf dem geschützten Gerät erstellt werden.

12. Um das Programm mit vordefinierten Einstellungen zu installieren, klicken Sie auf den Link **Konfigurationsdatei hinzufügen** und laden Sie die Konfigurationsdatei hoch.

    Wenn Sie mit Installationspaketen in der Kaspersky Security Center Web Console arbeiten, ist die Größe hochgeladener Konfigurationsdateien auf 4 MB beschränkt. Wenn Sie mit Installationspaketen in der Kaspersky Security Center Verwaltungskonsole arbeiten, gilt diese Beschränkung nicht.

13. Speichern Sie die vorgenommenen Änderungen.

2 Erstellung einer Aufgabe zur Remote-Installation

Die Aufgabe *Remote-Installation einer Anwendung* ermöglicht eine Remote-Installation von Kaspersky Embedded Systems Security. Mit der Aufgabe *Remote-Installation einer Anwendung* kann das Installationspaket des Programms auf allen Computern des Unternehmens bereitgestellt werden.

So erstellen Sie eine Aufgabe zur Remote-Installation (in der Kaspersky Security Center Verwaltungskonsole)

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 das Installationspaket für Kaspersky Embedded Systems Security aus. Wenn das Installationspaket für Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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. Anschließend wird Kaspersky Embedded Systems Security mithilfe 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 Embedded Systems 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 Embedded Systems 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 Kaspersky Embedded Systems Security installiert wird. 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 Embedded Systems 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 Embedded Systems Security für Windows 4.1 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.

So erstellen Sie eine Aufgabe zur Remote-Installation (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 **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 Security Center**.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Remote-Installation einer Anwendung**.
3. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein (z. B. *Installation von Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security für Windows (4.1) aus.
2. Wählen Sie ein Installationspaket für den Administrationsagenten aus.

   Die ausgewählte Version des Administrationsagenten wird zusammen mit Kaspersky Embedded Systems 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 Embedded Systems 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. Anschließend wird Kaspersky Embedded Systems Security mithilfe 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 **Behavior for devices managed through other Administration Servers** eine Installationsmethode für Kaspersky Embedded Systems 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 Embedded Systems 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.

Wie Sie ein Installationspaket und eine Aufgabe zur Remote-Installation erstellen, erfahren Sie in der Hilfe zu Kaspersky Security Center.

Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen

Nach der Installation von Kaspersky Embedded Systems Security wird empfohlen, die Datenbanken von Kaspersky Embedded Systems Security auf den Geräten zu aktualisieren. Sollte vor der Installation von Kaspersky Embedded Systems Security auf den Geräten kein Virenschutzprogramm mit aktiviertem Echtzeitschutz installiert gewesen sein, wird außerdem empfohlen, eine Untersuchung wichtiger Bereiche der Geräte durchzuführen.

Wenn geschützte Geräte, auf denen Kaspersky Embedded Systems Security installiert wurde, im Kaspersky Security Center Teil einer Administrationsgruppe sind, können Sie diese Aufgaben auf folgende Arten ausführen:

1. Erstellen Sie die Aufgabe *Update* für die Gruppe der geschützten Geräte, auf denen Kaspersky Embedded Systems Security installiert ist. Geben Sie den Kaspersky Security Center Administrationsserver als Update-Quelle an.

2. Erstellen Sie eine Gruppenaufgabe zur Untersuchung auf Befehl mit dem Status *Untersuchung wichtiger Bereiche*. Kaspersky Security Center bewertet den Sicherheitszustand aller geschützten Geräte aus dieser Gruppe aufgrund der Ergebnisse dieser Aufgabe, nicht nach den Ergebnissen der Aufgabe *Untersuchung wichtiger Bereiche*.

3. Erstellen Sie eine neue Richtlinie für die Gruppe der geschützten Geräte. Deaktivieren Sie in den Richtlinieneinstellungen im Abschnitt **Programmeinstellungen** den geplanten Start von lokalen Systemaufgaben zur Untersuchung auf Befehl und die *Update*-Aufgaben auf den geschützten Geräten der Administrationsgruppe mithilfe der Einstellungen des Unterabschnitts **Lokale Systemaufgaben ausführen**.

Sie können auch die Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security anpassen.

Installation der Programmkonsole über das Kaspersky Security Center

Wie Sie ein Installationspaket und eine Aufgabe zur Remote-Installation erstellen, erfahren Sie in der Hilfe zu Kaspersky Security Center.

Gehen Sie folgendermaßen vor, um die Programmkonsole mithilfe einer Aufgabe zur Remote-Installation zu installieren:

1. Öffnen Sie in der Kaspersky Security Center Verwaltungskonsole den Knoten **Erweitert**.

2. Erweitern Sie den untergeordneten Knoten **Remote-Installation**.

3. Erstellen Sie ein Installationspaket:

   a. Klicken Sie im Ergebnisfenster des untergeordneten Knotens **Installationspakete** auf die Schaltfläche **Installationspaket erstellen**.

   b. Wählen Sie im Fenster **Assistent für neues Paket** als Pakettyp **Installationspaket für angegebene ausführbare Datei erstellen** aus.

   c. Geben Sie den Namen des neuen Installationspakets ein.

   d. Wählen Sie die Datei \client\setup_esstool.exe in dem Ordner des Lieferumfangs von Kaspersky Embedded Systems Security aus und aktivieren Sie das Kontrollkästchen **Ganzen Ordner in das Installationspaket kopieren**.

e. Geben Sie im Feld **Einstellungen für den Start der ausführbaren Datei (optional)** die Parameterwerte EULA=1 und PRIVACYPOLICY=1:

```
/s /p "EULA=1 PRIVACYPOLICY=1"
```

an

Andernfalls können keine Komponenten installiert werden.

f. Falls erforderlich, können Sie im Feld **Einstellungen für den Start der ausführbaren Datei (optional)** die Befehlszeilenoption ADDLOCAL angeben, um die Menge der zu installierenden Komponenten zu ändern, und die Befehlszeilenoption INSTALLDIR, um einen anderen Zielordner als den Standardordner anzugeben. Mit der folgenden Befehlszeilenoption können Sie beispielsweise eine autonome Installation der Programmkonsole im Ordner C:\KasperskyConsole durchführen:

```
/s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
```

4. Erstellen Sie im untergeordneten Knoten **Installationspakete** eine Aufgabe zur Remote-Installation der Programmkonsole auf den ausgewählten geschützten Geräten (Administrationsgruppe).

5. Passen Sie die Aufgabeneinstellungen an.

6. Starten Sie die Aufgabe zur Remote-Installation.

Die Programmkonsole wird auf den in der Aufgabe angegebenen geschützten Geräten installiert.

Deinstallation von Kaspersky Embedded Systems Security über Kaspersky Security Center

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der während der Konfiguration des Schreibens von Dump- und Protokolldateien angegeben wurde.

Wenn die Verwaltung von Kaspersky Embedded Systems Security auf Netzwerkgeräten kennwortgeschützt ist, geben Sie das Kennwort ein, wenn Sie eine Aufgabe zur Deinstallation mehrerer Programme erstellen. Wenn der Kennwortschutz nicht zentralisiert mit einer Richtlinie von Kaspersky Security Center verwaltet wird, wird Kaspersky Embedded Systems Security erfolgreich von den Geräten deinstalliert, auf denen das eingegebene Kennwort mit dem festgelegten Wert übereinstimmt. Kaspersky Embedded Systems Security wird nicht von anderen geschützten Geräten deinstalliert.

So deinstallieren Sie Kaspersky Embedded Systems Security:

1. Erstellen und starten Sie in der Kaspersky Security Center Verwaltungskonsole eine Aufgabe zur Deinstallation von Programmen.

2. Wählen Sie in der Aufgabe die Deinstallationsmethode (auf die gleiche Weise, wie die Installationsmethode gewählt wurde; siehe vorhergehender Abschnitt) und geben Sie das Benutzerkonto an, unter dem der Administrationsserver auf die geschützten Geräte zugreifen soll. Sie können Kaspersky Embedded Systems Security nur mit den Standardinstallationseinstellungen deinstallieren.

Änderung der Auswahl der Programmkomponenten mithilfe von Kaspersky Security Center

Wenn Sie die Auswahl der Komponenten von Kaspersky Embedded Systems Security nach der Programminstallation ändern möchten, können Sie die Aufgabe *Auswahl der Programmkomponenten ändern* verwenden.

So ändern Sie die Auswahl der Programmkomponenten (in der Kaspersky Security Center-Verwaltungskonsole)

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 Embedded Systems Security für Windows (4.1)** → **Auswahl der Programmkomponenten ändern**.

Schritt 2. Einstellungen für die Aufgabe zum Ändern der Programmkomponenten

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

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 Namen für die Aufgaben ein, z. B. *Komponente „Programmkontrolle" hinzufügen*.

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 ändern Sie die Auswahl der Programmkomponenten (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 **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 Embedded Systems Security 4.1.0**.
2. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Komponenten für Kaspersky Embedded Systems Security 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

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

2. Wählen Sie in den Eigenschaften der Aufgabe die Registerkarte **Anwendungseinstellungen** aus.

3. 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 Embedded Systems Security im unbeaufsichtigten Modus geändert.

Erweiterte Aufgabeneinstellungen

Einstellung	Beschreibung
Vertrauenswürdige Zone	Für die Aufgabe *Auswahl der Programmkomponenten ändern* können Sie der vertrauenswürdigen Zone nur Untersuchungsausnahmen und vertrauenswürdige Programme hinzufügen.
Kennwort für das Ändern der Programmkomponentenauswahl verwenden	Gewöhnlich aktivieren Administratoren den Kennwortschutz, um den Zugriff auf Kaspersky Embedded Systems 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 KLAdmin-Konto verwenden.
Auf inkompatible Drittherstellerprogramme überprüfen	Kaspersky Embedded Systems Security überprüft standardmäßig die Kompatibilität der installierten Programme. Eine Liste der inkompatiblen Software befindet sich in der Datei incompatible.txt, die zum Lieferumfang gehört. Wenn die Überprüfung auf inkompatible Software aktiviert ist, hält Kaspersky Embedded Systems Security die Aufgabe an, sobald ein Programm aus der Liste gefunden wird. Wenn in der Herstellerdokumentation der Drittanbieter-Software angegeben ist, dass diese mit Endpoint Protection Platform (EPP) kompatibel ist, können Sie die Untersuchung von installierten Programmen deaktivieren.
Inkompatible Programme von Drittherstellern entfernen	Automatisches Entfernen von Programme, die auf der Liste incompatible.txt stehen, bevor die Auswahl der Komponenten geändert wird. Wenn diese Funktionalität aktiviert ist, versucht Kaspersky Embedded Systems Security, die inkompatiblen Programme zu entfernen, damit die Aufgabe fortgesetzt werden kann. Diese Option ist standardmäßig aktiviert.

Installation und Deinstallation des Programms über Active Directory-Gruppenrichtlinien

Dieser Abschnitt beschreibt die Installation und Deinstallation von Kaspersky Embedded Systems Security mithilfe von Active Directory-Gruppenrichtlinien sowie Informationen über die Aktionen, die nach der Installation von Kaspersky Embedded Systems Security mithilfe von Gruppenrichtlinien ausgeführt werden müssen.

Installation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory

Sie können Kaspersky Embedded Systems Security auf mehreren geschützten Geräten über die Gruppenrichtlinie von Active Directory installieren. Auf die gleiche Weise kann auch die Programmkonsole installiert werden.

Die geschützten Geräte, auf denen Sie Kaspersky Embedded Systems Security oder die Programmkonsole installieren möchten, müssen sich in derselben Domäne und einer einzelnen Organisationseinheit befinden.

Die Betriebssysteme auf den geschützten Geräten, auf denen Sie Kaspersky Embedded Systems Security mithilfe der Richtlinie installieren wollen, müssen die gleiche Bit-Version (32-Bit oder 64-Bit) aufweisen.

Sie müssen über Administratorrechte auf der Domain verfügen.

Verwenden Sie zur Installation von Kaspersky Embedded Systems Security das Installationspaket ess_win.msi. Um die Programmkonsole zu installieren, verwenden Sie das Installationspaket esstools.msi.

Detaillierte Informationen über die Verwendung von Gruppenrichtlinien für Active Directory finden Sie in der Dokumentation, die von der Firma Microsoft zur Verfügung gestellt wird.

Um Kaspersky Embedded Systems Security oder die Programmkonsole zu installieren, gehen Sie wie folgt vor:

1. Speichern Sie ess_win.msi in einem freigegebenen Ordner am dem Domänencontroller.
2. Speichern Sie die Schlüsseldatei im selben öffentlichen Verzeichnis auf dem Domain-Controller.
3. Erstellen Sie im selben freigegebenen Ordner auf dem Domänencontroller die Datei install_props.json, die die folgenden Zeilen enthält. Dies bedeutet, dass Sie den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie zustimmen.

   ```
   {
   "EULA": "1",
   "PRIVACYPOLICY": "1"
   }
   ```

4. Erstellen Sie auf dem Domain-Controller eine neue Richtlinie für die Gruppe, zu der die geschützten Geräte gehören.
5. Legen Sie mit dem **Gruppenrichtlinienobjekteditor** ein neues Installationspaket im Knoten **Computer-Konfiguration** an. Geben Sie den Pfad zur msi-Datei für Kaspersky Embedded Systems Security (oder die Programmkonsole) im UNC-Format (Universal Naming Convention) ein.
6. Aktivieren Sie das Kontrollkästchen **Immer mit erhöhten Rechten installieren** für den Dienst Windows Installer, und zwar sowohl im Knoten **Computer-Konfiguration**, als auch im Knoten **Benutzer-Konfiguration** der ausgewählten Gruppe.
7. Übernehmen Sie die Änderungen mithilfe des Befehls `gpupdate / force`.

Kaspersky Embedded Systems Security wird auf den geschützten Geräten der Gruppe nach deren Neustart installiert.

Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen

Nach der Installation von Kaspersky Embedded Systems Security auf den geschützten Geräten wird empfohlen, sofort die Programm-Datenbanken zu aktualisieren und eine Untersuchung wichtiger Bereiche durchzuführen. Sie können diese Aktionen aus der Programmkonsole ausführen.

Sie können auch die Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security anpassen.

Deinstallation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der während der Konfiguration des Schreibens von Dump- und Protokolldateien angegeben wurde.

Wenn Sie eine Active Directory-Gruppenrichtlinie verwendet haben, um Kaspersky Embedded Systems Security (oder die Programmkonsole) auf der Gruppe von geschützten Geräten zu installieren, können Sie diese Richtlinie verwenden, um Kaspersky Embedded Systems Security (oder die Programmkonsole) zu deinstallieren.

Sie können das Programm nur mit den Standarddeinstallationseinstellungen deinstallieren.

Detaillierte Informationen über die Verwendung von Gruppenrichtlinien für Active Directory finden Sie in der Dokumentation, die von der Firma Microsoft zur Verfügung gestellt wird.

Wenn die Programmverwaltung kennwortgeschützt ist, können Sie Kaspersky Embedded Systems Security nicht mithilfe von Active Directory-Gruppenrichtlinien deinstallieren.

Um Kaspersky Embedded Systems Security (oder die Programmkonsole) zu deinstallieren, gehen Sie wie folgt vor:

1. Wählen Sie im Domänencontroller die Organisationseinheit aus, von deren geschützten Geräten Sie Kaspersky Embedded Systems Security oder die Programmkonsole deinstallieren möchten.
2. Wählen Sie eine Richtlinie aus, die für die Installation von Kaspersky Embedded Systems Security erstellt wurde, öffnen Sie im **Editor für Gruppenrichtlinien** im Knoten **Software-Installation** (**Computerkonfiguration** > **Software-Einstellungen** > **Software-Installation**) das Kontextmenü des Installationspakets für Kaspersky Embedded Systems Security (die Programmkonsole) und wählen Sie den Befehl **Alle Aufgaben** > **Löschen**.
3. Wählen Sie die Deinstallationsmethode **Sofortige Deinstallation der Software von Benutzern und Computern**.
4. Übernehmen Sie die Änderungen mithilfe des Befehls `gpupdate /force`.

Kaspersky Embedded Systems Security wird von den geschützten Geräten nach deren Neustart und vor der Anmeldung bei Microsoft Windows deinstalliert.

Installations- und Deinstallationsprotokolle für Kaspersky Embedded Systems Security

Wenn Sie Kaspersky Embedded Systems Security mithilfe des Installations-Assistenten (Deinstallations-Assistenten) installieren (deinstallieren), erstellt der Windows-Installationsdienst ein Protokoll über die Installation (Deinstallation). Eine Protokolldatei mit dem Namen kl-install-<uid>.log (wobei <uid> ein eindeutiger 8-stelliger Protokollbezeichner ist) wird im Ordner %temp% für den Benutzer gespeichert, dessen Konto zum Starten der Datei setup_ess.exe oder setup_esstool.exe verwendet wurde.

Wenn Sie die Installation oder Deinstallation von Kaspersky Embedded Systems Security aus der Befehlszeile ausführen, wird in der Grundeinstellung keine Log-Datei erstellt.

Um Kaspersky Embedded Systems Security zu installieren und eine Protokolldatei auf Laufwerk C:\ zu erstellen, führen Sie den folgenden Befehl aus:

```
msiexec /i ess_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

Systemänderungen nach der Installation von Kaspersky Embedded Systems Security

Wenn Kaspersky Embedded Systems Security und die Konsole für Kaspersky Embedded Systems Security gleichzeitig installiert werden, nimmt der Windows-Installer-Dienst auf dem geschützten Gerät folgende Veränderungen vor:

- Auf dem geschützten Gerät sowie auf dem Gerät, auf dem die Programmkonsole installiert ist, werden Ordner für Kaspersky Embedded Systems Security erstellt.
- Die Dienste von Kaspersky Embedded Systems Security werden registriert.
- Die Benutzergruppe für Kaspersky Embedded Systems Security wird erstellt.
- Die Schlüssel für Kaspersky Embedded Systems Security werden in der Systemregistrierung registriert.
- Es wird die Kaspersky Embedded Systems Security-Systemaufgabe zum erkennen eines Betriebssystem-Updates erstellt und in der Windows Aufgabenplanung angezeigt.

Diese Änderungen sind nachfolgend beschrieben.

Ordner für Kaspersky Embedded Systems Security auf einem geschützten Gerät

Wenn Kaspersky Embedded Systems Security installiert wird, werden auf einem geschützten Gerät die folgenden Ordner erstellt:

- Standardmäßiger Installationsordner von Kaspersky Embedded Systems Security, der die ausführbaren Dateien von Kaspersky Embedded Systems Security enthält. Standardmäßig wird der folgende Installationsordner verwendet:

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0

- Dateien für die Management Information Base (MIB) mit einer Beschreibung der Indikatoren und Traps, die von Kaspersky Embedded Systems Security mit dem SNMP-Protokoll veröffentlicht werden.

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0\mibs

- Dienstdateien für Kaspersky Embedded Systems Security:
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Data
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Settings
  - %ProgramData%\Kaspersky Lab\KESS.4.1\Dskm
- Dateien mit Einstellungen für Update-Quellen:

  %ProgramData%\Kaspersky Lab\KESS.4.1\Data
- Datenbanken-Updates und Updates der Programm-Module, die mithilfe der *Update*-Aufgabe heruntergeladen wurden (der Ordner wird erstellt, wenn erstmals Updates mithilfe der *Update*-Aufgabe heruntergeladen werden).

  %ProgramData%\Kaspersky Lab\KESS.4.1\Update distribution
- Berichte über Aufgabenausführung und Systemaudit-Bericht:

  %ProgramData%\Kaspersky Lab\KESS.4.1\Reports
- Derzeit verwendetes Datenbankpaket:

  %ProgramData%\Kaspersky Lab\KESS.4.1\Bases
- Backup-Kopien der Datenbanken; werden bei jedem Datenbanken-Update überschrieben:

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB
- Temporäre Dateien, die beim Ausführen der Update-Aufgabe angelegt werden:

  %ProgramData%\Kaspersky Lab\KESS.4.1\Data\temp\temporaryFolder
- Objekte in der Quarantäne (standardmäßiger Ordner):

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB
- Objekte im Backup (standardmäßiger Ordner):

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB
- Objekte, die aus Backup oder Quarantäne wiederhergestellt wurden (standardmäßiger Ordner für die Wiederherstellung von Objekten):

  %ProgramData%\Kaspersky Lab\KESS.4.1\QB\Restored

Ordner, der bei der Installation der Programmkonsole erstellt wird

Der Standardinstallationsordner für die Programmkonsole ist vom Bit-Satz des Betriebssystems abhängig. Standardmäßig wird der folgende Installationsordner verwendet:

%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Console 4.1.0

Dienste von Kaspersky Embedded Systems Security

Die folgenden Dienste von Kaspersky Embedded Systems Security werden unter dem SYSTEM-Konto ausgeführt:

- Kaspersky Embedded Systems Security Service (AVP.KESS.4.1). Basis-Systemdienst von Kaspersky Embedded Systems Security, der Geräte vor Viren und anderen Bedrohungen schützt
- Kaspersky Embedded Systems Security Side-by-Side Service (AVP.KESS.4.1.SbS). Systemdienst, der Geräte schützt, während Kaspersky Embedded Systems Security aktualisiert oder wiederhergestellt wird oder Komponenten geändert werden
- Kaspersky Seamless Update Service (avpsus.KESS.4.1). Systemdienst, der wichtige und genehmigte Updates für die Programm-Module installiert und zurücksetzt
- Remote-Steuerungsdienst für Kaspersky Embedded Systems Security (avpcos.KESS.4.1). Systemdienst, mit dem Kaspersky Embedded Systems Security Service aus der Anwendungskonsole per Fernsteuerung neu gestartet oder beendet wird

Gruppe in Kaspersky Embedded Systems Security

ESS-Administratoren ist eine Gruppe auf dem geschützten Gerät, deren Mitglieder vollen Zugriff auf alle Funktionen von Kaspersky Embedded Systems Security haben.

Schlüssel der Systemregistrierung

Wenn Kaspersky Embedded Systems Security installiert wird, werden die folgenden Systemregistrierungsschlüssel erstellt:

- Einstellungen für Kaspersky Embedded Systems Security:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.ESS.4.1]
- Einstellungen des Ereignisprotokolls von Kaspersky Embedded Systems Security (Kaspersky-Ereignisprotokoll):
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Embedded Systems Security]
- Einstellungen für Protokolldateien:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.1\Trace]
- Einstellungen für die Aufgaben und Funktionen des Programms:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.1\environment]

Kaspersky Embedded Systems Security-Systemaufgabe zum Erkennen eines Betriebssystem-Updates

Der Dienst des Windows Installer erstellt während der Programminstallation eine Aufgabe zur Kaspersky Embedded Systems Security OS Upgrade Detect. Die Aufgabe gestartet, sobald sie erstellt ist, und wenn das Betriebssystem zukünftig neu gestartet wird. Die Aufgabe überprüft die Version der vom Programm verwendeten Treiber: Wenn eine Version des Betriebssystems aktualisiert wird, aktualisiert das Programm die Treiber für die entsprechende Version des Betriebssystems.

Die Aufgabe hat keine Auswirkungen auf das Programm und kann gelöscht werden. Es wird empfohlen, das Szenario für Betriebssystem-Updates im Hinterkopf zu behalten.

Windows-Firewall-Regeln

Abhängig von den angegebenen Installationseinstellungen können auf dem geschützten Gerät die in der folgenden Tabelle beschriebenen Windows-Firewall-Zulassungsregeln für eingehende Verbindungen erstellt werden.

Windows-Firewall-Regeln

Regelname	Regelbeschreibung	Bedingung für die Regelerstellung
AVP.KESS.4.1	Zulassungsregel für die ausführbare Datei avp.exe.	Wird immer erstellt.
AVP.KESS.4.1 Remote UI Connection	Zulassungsregel für TCP-Port 13032.	Installation des Programms mit dem Parameter `ADDWFEXCLUSION=1`.
AVP.KESS.4.1 Remote UI Connection	Zulassungsregel für TCP-Port 13031. Diese Portnummer wird standardmäßig verwendet. Sie können die Portnummer ändern, indem Sie den Parameter `UIKLPORT=<port>` angeben. In diesem Fall erstellt das Programm eine Regel für die angegebene Portnummer.	Installation des Programms mit den Parametern `ADDWFEXCLUSION=1` und `UIKLPORT=13031`. Die Regel wird nicht erstellt, wenn der Parameter `ENABLEUIKLPORT=0` übergeben wird

Prozesse von Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security startet die in der folgenden Tabelle beschriebenen Prozesse.

Prozesse von Kaspersky Embedded Systems Security

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

Überprüfung der Funktionen von Kaspersky Embedded Systems Security Verwendung des EICAR-Testvirus

Dieser Abschnitt beschreibt den EICAR-Testvirus und wie der EICAR-Testvirus verwendet wird, um den Echtzeitschutz für Dateien und die Funktionen der Untersuchung auf Befehl von Kaspersky Embedded Systems Security zu überprüfen.

EICAR-Testvirus

Der Testvirus eignet sich dazu, die Funktionen von Antiviren-Anwendungen zu überprüfen. Er ist vom The European Institute for Computer Antivirus Research (EICAR) entwickelt worden.

Der Testvirus ist kein schädliches Objekt und enthält keinen ausführbaren Code, der Ihr Gerät beschädigen könnte, er wird jedoch von den meisten Antiviren-Programmen der Antiviren-Hersteller als Bedrohung erkannt.

Die Datei, die den Testvirus enthält, heißt eicar.com. Sie können sie von der EICAR-Website herunterladen.

Vergewissern Sie sich vor dem Speichern der Datei in einem Ordner auf der Festplatte des Geräts, dass der Echtzeitschutz für Dateien in diesem Ordner deaktiviert ist.

Die Datei eicar.com enthält eine Textzeile. Beim Untersuchen der Datei erkennt Kaspersky Embedded Systems Security in dieser Textzeile eine Testbedrohung, weist der Datei den Status **Infiziert** zu und löscht sie. Die Daten über die erkannte Bedrohung in der Datei werden in der Programmkonsole und im Protokoll der Aufgabenausführung angezeigt.

Sie können die Datei eicar.com verwenden, um zu prüfen, wie Kaspersky Embedded Systems Security infizierte Objekte desinfiziert und wie möglicherweise infizierte Objekte erkannt werden. Öffnen Sie dazu die Datei mit einem Texteditor, fügen Sie eines der in der folgenden Tabelle aufgeführten Präfixe am Anfang der Textzeile in der Datei ein und speichern Sie die Datei unter einem neuen Namen, z. B. eicar_cure.com.

Damit Kaspersky Embedded Systems Security die Datei eicar.com mit einem Präfix verarbeiten kann, aktivieren Sie im Abschnitt der Sicherheitseinstellungen **Schutz von Objekten** die Option **Alle Objekte** für die Aufgaben zum Echtzeit-Computerschutz und die Aufgaben zur Untersuchung auf Befehl von Kaspersky Embedded Systems Security.

Präfixe in EICAR-Dateien

Präfix	Dateistatus nach Untersuchung und Aktion von Kaspersky Embedded Systems Security
Ohne Präfix	**Kaspersky Embedded Systems Security weist dem Objekt den Status Infiziert zu und löscht es.**
SUSP–	Kaspersky Embedded Systems Security weist dem mit heuristischer Analysemethode erkannten Objekt den Status **Möglicherweise infiziert** zu und löscht es, da möglicherweise infizierte Objekte nicht desinfiziert werden.
WARN–	Kaspersky Embedded Systems Security weist dem Objekt den Status **Möglicherweise infiziert** (Code des Objektes stimmt partiell mit einem bekannten schädlichen Code überein) zu und löscht es, da möglicherweise infizierte Objekte nicht desinfiziert werden.
CURE–	Kaspersky Embedded Systems Security weist dem Objekt den Status **Infiziert** zu und desinfiziert es. Wenn die Desinfektion gelingt, wird der gesamte Text in der Datei durch das Wort "CURE" ersetzt.

Echtzeitschutz für Dateien und Funktionen der Untersuchung auf Befehl testen

Nach der Installation von Kaspersky Embedded Systems Security können Sie bestätigen, dass Kaspersky Embedded Systems Security Objekte erkennt, die schädlichen Code enthalten. Verwenden Sie dazu den Testvirus EICAR.

So prüfen Sie die Aufgabe zum Echtzeitschutz für Dateien:

1. Laden Sie die Datei eicar.com von der EICAR-Website herunter. Speichern Sie sie in einem gemeinsamen Ordner auf dem lokalen Laufwerk eines beliebigen Geräts im Netzwerk.

   Vergewissern Sie sich vor dem Speichern der Datei in einem Ordner, dass der Echtzeitschutz für Dateien für diesen Ordner deaktiviert ist.

2. Wenn Sie prüfen möchten, ob die Benachrichtigungen für die Benutzer des Netzwerks funktionieren, vergewissern Sie sich, dass sowohl auf dem geschützten Gerät als auch auf dem Gerät, auf dem Sie die Datei eicar.com gespeichert haben, der Windows Messenger Dienst aktiviert ist.

3. Öffnen Sie die Programmkonsole auf dem geschützten Gerät.

4. Kopieren Sie auf folgende Weise die gespeicherte Datei eicar.com auf den lokalen Datenträger des geschützten Geräts:

   - Um die Funktion Benachrichtigung über ein Fenster für Terminaldienste zu überprüfen, kopieren Sie die Datei eicar.com auf ein Gerät, das mithilfe des Programms "Remote Desktop Connection" an den Server angeschlossen ist.

   - Um die Funktion Benachrichtigung über den Windows Messenger Dienst zu überprüfen, kopieren Sie die Datei eicar.com von dem Gerät, auf dem Sie sie gespeichert haben, über die Netzwerkumgebung dieses Geräts.

Die Echtzeitschutz für Dateien funktioniert auf vorgeschriebene Weise, wenn folgende Bedingungen erfüllt werden:

- Die Datei eicar.com wird vom geschützten Gerät gelöscht.

- Das Aufgabenprotokoll erhält in der Anwendungskonsole den Status *Kritisch*. Das Protokoll enthält eine neue Zeile mit Informationen über eine Bedrohung in der Datei eicar.com.

- Auf dem Gerät, von dem aus Sie die Datei kopiert haben, wird die folgende Meldung des Windows Messenger Dienstes mit folgendem Inhalt angezeigt: Kaspersky Embedded Systems Security hat den Zugriff auf <Pfad der Datei eicar.com auf dem Gerät>\eicar.com für den Computer <Netzwerkname des Geräts> um <Uhrzeit für Ereigniseintritt> gesperrt. Grund: Bedrohung erkannt. Virus: EICAR-Test-File. Name des Objektbenutzers: <Benutzername>. Computername: <Netzwerkname des Geräts, von dem die Datei kopiert wurde>.

  Vergewissern Sie sich, dass der Windows Messenger Dienst auf dem Gerät funktioniert, von dem Sie die Datei eicar.com kopiert haben.

Um die Funktion "Untersuchung auf Befehl" zu prüfen, gehen Sie wie folgt vor:

1. Laden Sie die Datei eicar.com von der EICAR-Website herunter. Speichern Sie sie in einem gemeinsamen Ordner auf dem lokalen Laufwerk eines beliebigen Geräts im Netzwerk.

   Vergewissern Sie sich vor dem Speichern der Datei in einem Ordner, dass der Echtzeitschutz für Dateien für diesen Ordner deaktiviert ist.

2. Öffnen Sie die Programmkonsole und erweitern Sie den Knoten **Untersuchung auf Befehl** in der Programmkonsolenstruktur.

3. Wählen Sie den untergeordneten Knoten **Untersuchung wichtiger Bereiche** aus.

4. Fügen Sie **Alle Netzlaufwerke** zum Bereich der Aufgabe Untersuchung auf Befehl hinzu.

5. Führen Sie die Aufgabe Untersuchung wichtiger Bereiche aus.

Die Untersuchung auf Befehl funktioniert auf vorgeschriebene Weise, wenn folgende Bedingungen erfüllt werden:

- Die Datei eicar.com wird von der Festplatte des Geräts gelöscht.
- Das Aufgabenprotokoll erhält in der Anwendungskonsole den Status *Kritisch*. Das Protokoll der Aufgabe „Untersuchung auf Befehl“ enthält eine neue Zeile mit Informationen über eine Bedrohung in der Datei „eicar.com“.

Upgrade älterer Versionen von Kaspersky Embedded Systems Security auf Version 4.1

Für das Upgrade einer älteren Version von Kaspersky Embedded Systems Security auf Version 4.1 haben wir folgende Empfehlungen für Sie:

- Planen Sie voraus und erstellen Sie einen Zeitplan für das Upgrade. Wählen Sie einen Zeitpunkt aus, zu dem die Server am wenigsten ausgelastet sind, z. B. am Wochenende.
- Aktivieren Sie nach dem Upgrade eine Programmkomponente nach der anderen. Aktivieren Sie beispielsweise zuerst nur die Komponente „Echtzeitschutz für Dateien“, aktivieren Sie dann weitere Schutzkomponenten, aktivieren Sie anschließend die Kontrollkomponenten und so weiter. Unser Tipp: Testen Sie das Programm bei jedem dieser Schritte.
- Führen Sie das Upgrade Schritt für Schritt durch. Aktualisieren Sie zuerst einen einzelnen Computer, dann mehrere Computer und anschließend alle Computer des Unternehmens.

Schritte für das Upgrade

Halten Sie beim Upgrade von Kaspersky Embedded Systems Security auf Version 4.1 die folgende Reihenfolge ein:

1. **Upgrade von Kaspersky Security Center**

   Upgraden Sie alle Komponenten von Kaspersky Security Center auf Version 14.2 oder höher, einschließlich des Administrationsagenten auf den Benutzercomputern und in Kaspersky Security Center Web Console.

2. **Upgrade des Web-Plug-ins von Kaspersky Embedded Systems Security**

   Upgraden Sie in der Kaspersky Security Center Web Console das Kaspersky Embedded Systems Security-Web-Plug-in auf Version 4.1.

3. **Migration der Aufgaben und Richtlinien von Kaspersky Embedded Systems Security**

   Nach der Migration von Richtlinien und Aufgaben müssen Sie die Einstellungen konfigurieren. Hier geht es um die Einstellungen, die der Migrations-Assistent nicht migrieren kann und die in älteren Programmversionen nicht vorhanden waren. Außerdem sollten Sie unbedingt überprüfen, ob der Migrations-Assistent alle Einstellungen korrekt migriert hat.

4. **Installation von Kaspersky Embedded Systems Security 4.1**

   Kaspersky Embedded Systems Security Version 4.1 verwendet das HTTPS-Protokoll anstelle des DCOM-Protokolls. Bevor Sie die neue Version von Kaspersky Embedded Systems Security installieren, müssen Sie das Gerät konfigurieren, auf dem das Programm aktualisiert wird. Dadurch wird der Remote-Start des KESS-Dienstes ermöglicht. Wenn das Gerät nicht entsprechend konfiguriert wird, ist der Remote-Start des Dienstes nicht verfügbar.

   Sie können Kaspersky Embedded Systems Security 4.1 installieren, nachdem Sie eine ältere Version des Programms entfernt haben oder wenn eine andere Version vorhanden ist.

   Bei der Installation über eine ältere Programmversion werden die gleichen Programmkomponenten installiert. Dabei werden die neuen Namen und Inhalte einiger Komponenten berücksichtigt.

Bei einer Remote-Installation installiert das Installationsprogramm die Komponenten, die Sie in den Eigenschaften des Installationspakets auswählen.

5. **Aktivieren Sie Kaspersky Embedded Systems Security 4.1, falls dies erforderlich ist.**

   Wenn Kaspersky Embedded Systems Security 4.1 über eine ältere Programmversion installiert wird, wird die aktuelle Lizenz automatisch für das Programm verwendet und die neuen Programmkomponenten und Aufgaben sind vollständig verfügbar. Die Gültigkeitsdauer der Lizenz bleibt dabei unverändert.

6. **Korrekte Funktion des Programms sicherstellen**

   Stellen Sie nach dem Upgrade von Kaspersky Embedded Systems Security sicher, dass das Programm ordnungsgemäß funktioniert. Stellen Sie sicher, dass im Programm keine Fehler vorliegen. Überprüfen Sie außerdem den Zeitpunkt der letzten Verbindung zum Administrationsserver, den Zeitpunkt des letzten Updates und den Status des Computerschutzes.

   Achten Sie auf migrierte Ausnahmelisten, vertrauenswürdige Programme, Regeln der Gerätekontrolle und Regeln der Kontrolle des Programmstarts.

Kaspersky Embedded Systems Security aktualisieren

Das Upgrade auf Kaspersky Embedded Systems Security 4.1 wird für die Versionen 2.3, 3.1 oder höher unterstützt. Um das Upgrade von früheren Versionen aus durchzuführen, müssen Sie die installierte Version entfernen und anschließend Version 4.1 installieren.

Das Update wird ausgeführt, indem die neue Version des Programms über die bereits verwendete ältere Version installiert wird, und erfordert keinen Neustart des Computers.

Standardmäßig erstellt das Programm dazu basierend auf dem Pfad des vorhandenen Programminstallationsordners einen neuen Installationsordner mit dem Namen der neuen Programmversion. Sie können manuell einen neuen Pfad für den Installationsordner des Programms angeben.

Beim Upgrade von Kaspersky Embedded Systems Security auf Version 4.1 wird die zuvor installierte Version des Programms automatisch gelöscht.

Wenn Sie eine kennwortgeschützte Installation von Kaspersky Embedded Systems Security aktualisieren möchten, können Sie das Kennwort auf eine folgende Arten an das Installationsprogramm übertragen:

- Geben Sie bei einer lokalen Installation über die Benutzeroberfläche des Installationsassistenten oder im interaktiven CLI-Modus das Kennwort an, wenn Sie dazu aufgefordert werden.
- Geben Sie bei einer lokalen Installation im nicht interaktiven CLI-Modus das Kennwort im Schlüssel `UNLOCK_PASSWORD` an.
- Wenn Sie bei der Installation Active Directory-Gruppenrichtlinien verwenden, geben Sie den Wert des Schlüssels `UNLOCK_PASSWORD` in der Konfigurationsdatei install_props.json an.

Wenn das Programm per Fernzugriff über Kaspersky Security Center upgraden und das Programm durch ein Kennwort geschützt ist, müssen Sie den Kennwortschutz zunächst mithilfe einer Kaspersky Security Center-Richtlinie deaktivieren.

Beim Update des Programms wird die aktuelle Lizenz automatisch für Kaspersky Embedded Systems Security Version 4.1 angewendet und die neuen Programmkomponenten und Aufgaben können im vollen Umfang verwendet werden. Die Gültigkeitsdauer der Lizenz bleibt dabei unverändert.

Wenn ein Programm mit einer abgelaufenen Lizenz aktualisiert wird, wird die neue Version des Programms nach der Installation nur im eingeschränkten Funktionsmodus ausgeführt (z. B. sind für die Programmdatenbanken keine Updates verfügbar).

Administrations-Tools von Kaspersky Embedded Systems Security aktualisieren

Sie können das Verwaltungs-Plug-in für die Verwaltung des Programms mithilfe von Kaspersky Security Center von den Versionen 2.3, 3.1, 3.2, 3.3, 3.4 oder höher auf Version 4.1 aktualisieren. Um ältere Versionen des Verwaltungs-Plug-ins und der Anwendungskonsole zu aktualisieren, müssen Sie die installierte Version entfernen und anschließend Version 4.1 installieren.

Während des Updates wird eine neue Version des Verwaltungs-Plug-ins über die bereits vorhandene Version installiert. Ein Neustart des Computers ist nicht erforderlich.

Informationen über die Migration der Einstellungen des Verwaltungs-Plug-ins finden Sie in diesem Artikel.

Migration von Richtlinien und Aufgaben

Sie können Richtlinien- und Aufgabeneinstellungen von älteren Programmversionen wie folgt in Version 4.1 migrieren:

- Mithilfe des Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben (nur in der Kaspersky Security Center-Verwaltungskonsole verfügbar).
- Mit dem Migrations-Assistenten für Richtlinien und Aufgaben von Kaspersky Embedded Systems Security 4.1 (nur in der Kaspersky Security Center Web Console verfügbar).

Wir empfehlen folgendes Vorgehen: Migrieren Sie die Richtlinien und Aufgaben von Kaspersky Embedded Systems Security zunächst auf einem einzelnen Computer, dann auf einer Gruppe von Computern und schließlich auf allen Computern des Unternehmens.

So verwenden Sie den Assistenten für das Massenkonvertieren von Richtlinien und Aufgaben, um Einstellungen für Richtlinien und Aufgaben zu migrieren

1. Wählen Sie in der Kaspersky Security Center 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.

Dadurch wird der Assistent für das Massenkonvertieren von Richtlinien und Aufgaben gestartet. Folgen Sie den Anweisungen.

Schritt 1. Auswahl des Programms, für das Sie Richtlinien und Aufgaben konvertieren müssen

Wählen Sie Kaspersky Embedded Systems Security 4.1 aus. Weiter zum nächsten Schritt

Schritt 2. Konvertieren von Richtlinien

Wählen Sie die Richtlinien der zu aktualisierenden Programmversion aus, die Sie für Kaspersky Embedded Systems Security 4.1 erstellen möchten. Weiter zum nächsten Schritt

Schritt 3. Konvertieren von Aufgaben

Wählen Sie die Aufgaben der zu aktualisierenden Programmversion aus, die Sie für Kaspersky Embedded Systems Security 4.1 erstellen möchten.

Nicht gruppenbezogene Aufgaben (Aufgaben, die bestimmten Geräten zugewiesen sind) werden bei diesem Schritt nicht angezeigt.

So konvertieren Sie nicht gruppenbezogene Aufgaben aus Ihrer Programmversion in die Version Kaspersky Embedded Systems Security 4.1:

1. Klicken Sie auf **Weiter**.

   Das Fenster **Zusätzlich Zeitpläne und nicht gruppenbezogene Aufgaben migrieren** wird geöffnet.

2. Aktivieren Sie das Kontrollkästchen **Nicht-Gruppenaufgaben migrieren**.

3. Geben Sie die Verbindungseinstellungen für den Kaspersky Security Center Administrationsserver an.

4. Klicken Sie auf **OK**.

Schritt 4. Assistent abschließen

Schließen Sie den Assistenten ab. Als Ergebnis geht der Assistent wie folgt vor:

- Es werden neue Richtlinien für Kaspersky Embedded Systems Security 4.1 erstellt.

  Neue Richtlinien enthalten Einstellungen aus den ausgewählten Richtlinien von Kaspersky Embedded Systems Security sowie neue Einstellungen, die in Kaspersky Embedded Systems Security 4.1 eingeführt wurden. Die Namen der neuen Richtlinien entsprechen den Namen der Richtlinien von Kaspersky Embedded Systems Security, bevor diese konvertiert wurden, und haben den Zusatz „(konvertiert)“. Neue Richtlinien haben den Status *Inaktive Richtlinie*.

- Es werden neue Aufgaben für Kaspersky Embedded Systems Security 4.1 erstellt.

  Neue Aufgaben enthalten Einstellungen aus den ausgewählten Aufgaben von Kaspersky Embedded Systems Security sowie neue Einstellungen, die in Kaspersky Embedded Systems Security 4.1 eingeführt wurden. Die Namen der neuen Aufgaben entsprechen den Namen der Aufgaben von Kaspersky Embedded Systems Security, bevor diese konvertiert wurden, und haben den Zusatz „(konvertiert)“.

- Richtlinien und Aufgaben, die zur Konvertierung ausgewählt wurden, bleiben unverändert.

So verwenden Sie den Migrations-Assistenten, um Einstellungen für Richtlinien und Aufgaben zu migrieren

Wählen Sie im „Web Console“-Hauptfenster den Punkt **Vorgänge** → **Migration auf KESS 4.1.0** aus.

Dadurch wird der Migrations-Assistent für Richtlinien und Aufgaben ausgeführt. Folgen Sie den Anweisungen.

Schritt 1. Migration der Richtlinien

Wählen Sie die Richtlinien von Kaspersky Embedded Systems Security aus, die Sie für Kaspersky Embedded Systems Security 4.1 erstellen möchten. Weiter zum nächsten Schritt

Schritt 2. Aufgabenmigration

Wählen Sie in der Aufgabenliste die Aufgaben von Kaspersky Embedded Systems Security aus, die Sie für Kaspersky Embedded Systems Security 4.1 erstellen möchten. Weiter zum nächsten Schritt

Schritt 3. Assistent abschließen

Schließen Sie den Assistenten ab. Als Ergebnis geht der Assistent wie folgt vor:

- Es werden neue Richtlinien für Kaspersky Embedded Systems Security 4.1 erstellt.

  Neue Richtlinien enthalten Einstellungen aus migrierten Richtlinien von Kaspersky Embedded Systems Security sowie neue Einstellungen, die in Kaspersky Embedded Systems Security 4.1 eingeführt wurden. Die Namen der neuen Richtlinien entsprechen den Namen der Richtlinien von Kaspersky Embedded Systems Security, bevor diese zusammengeführt wurden, und haben den Zusatz „aus KESS kopiert“. Neue Richtlinien haben den Status *Inaktive Richtlinie*.

- Es werden neue Aufgaben für Kaspersky Embedded Systems Security 4.1 erstellt.

  Neue Aufgaben enthalten Einstellungen aus migrierten Aufgaben von Kaspersky Embedded Systems Security sowie neue Einstellungen, die in Kaspersky Embedded Systems Security 4.1 eingeführt wurden. Die Namen der neuen Aufgaben entsprechen den Namen der Aufgaben von Kaspersky Embedded Systems Security, bevor diese migriert wurden, und haben den Zusatz „aus KESS kopiert“.

Migration von Einstellungen der zu aktualisierenden Programmversion

Die folgenden Elemente werden nach dem Upgrade des Programms und der Verwaltungs-Plug-ins auf Version 4.1 unverändert migriert:

- Einstellungen von Komponenten und Aufgaben, mit Ausnahme derjenigen, die auf die Standardeinstellungen zurückgesetzt werden und die unter „Einschränkungen bei der Migration von Einstellungen und Komponenten“ genannt werden
- Aufgabenprotokolle und Systemaudit-Protokolle sowie Einträge im Windows-Ereignisprotokoll
- Benachrichtigungseinstellungen für Aufgaben
- Benutzerkonten, unter denen Aufgaben gestartet werden
- Benutzerrechte für die Programmverwaltung
- Kennwort für die Verbindung zum Proxyserver
- Status des Attributs

Die folgenden Einstellungen werden nach dem Upgrade des Programms und der Plug-ins auf Version 4.1 entweder zurückgesetzt oder auf die Standardwerte für die neue Programmversion festgelegt:

- Alle Zähler, einschließlich der Statuswerte der Antiviren-Datenbanken
- Daten über installierte Updates von Programm-Modulen und Antiviren-Datenbanken
- Statuswerte von Aufgaben
- Benutzerzugriffsberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security Service
- Programm- und Aufgabeneinstellungen, die über die Registry konfiguriert werden
- Programm- und Aufgabeneinstellungen, die während der Installation kritischer Fixes geändert wurden
- Konfiguration von Ereignissen
- Einstellungen für die Datenübertragung an den Kaspersky Security Center Administrationsserver: Standardmäßig ist die Übertragung aller Daten aktiviert
- Einstellungen für die Ablaufverfolgung und für Dumps
- Einstellungen der lokalen Programmaufgaben, die sich auf der Registerkarte **Meldungen** befinden

Einstellungen, die in der zu aktualisierenden Programmversion nicht vorhanden waren, erhalten Standardwerte.

Einschränkungen bei der Migration von Einstellungen und Komponenten

- Der Inhalt der Quarantäne der zu aktualisierenden Version wird in das Backup von Version 4.1 verschoben. Gleichzeitig wird die maximale Backup-Größe auf 400 MB erhöht und der Schwellenwert für den verfügbaren Speicherplatz wird auf 100 MB erhöht.

- Die folgenden Einstellungen von Kaspersky Embedded Systems Security Version 3.4 sind in Kaspersky Embedded Systems Security Version 4.0 und höher nicht vorhanden und werden daher nicht migriert: **Quarantäne-Ordner**, **Backup-Ordner** und **Ordner für die Wiederherstellung von Objekten**. Andere Einstellungen, die in der alten Version vorhanden sind und in der neuen Version fehlen, werden ebenfalls nicht migriert.

- Die Liste der blockierten Netzwerksitzungen von Client-Computern wird nicht migriert. Die Einstellungen für das automatische Entsperren des Zugriffs auf blockierte Dateiressourcen im Netzwerk bleiben nach dem Programm-Upgrade unverändert.

- Die Einstellungen für den Kennwortschutz werden nicht migriert. Der Kennwortschutz in Kaspersky Embedded Systems Security 4.0 unterscheidet erheblich von früheren Versionen. Aktivieren Sie bei Bedarf den Kennwortschutz und legen Sie ein Kennwort fest.

- Vertrauenswürdige Zone:

  - Die Methode zur Auswahl von Objekten der vertrauenswürdigen Zone wurde in Kaspersky Embedded Systems Security 4.1 geändert. Ausnahmen, die als einzelne Dateien oder als Datei- oder Ordnerpfade definiert sind, können migriert werden. Ausnahmen, die als vordefinierter Bereich (z. B. Festplatten) oder als Skript-URL definiert sind, werden nicht migriert. Solche Ausnahmen müssen Sie nach der Migration manuell hinzufügen.

  - Der vertrauenswürdigen Zone wurden vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme hinzugefügt, die eine Einrichtung des Programms auf Servern vereinfachen.

- Die Komponenten Kontrolle des Programmstarts und Gerätekontrolle wurden grundlegend überarbeitet. Die Komponenteneinstellungen der zu aktualisierenden Version werden migriert. Dabei wird die neue Struktur der Einstellungen in Kaspersky Embedded Systems Security 4.1 berücksichtigt. Dies bedeutet, dass Sie möglicherweise mehr Speicherplatz auf dem Administrationsserver benötigen, um die Programmeinstellungen zu speichern.

- Die Einstellungen der Komponenten „Überwachung der Datei-Integrität“ und „Überwachung des Registrierungszugriffs“ der zu aktualisierenden Programmversion werden in die Einstellungen der Komponente „Überwachung der Systemintegrität“ migriert.

- Die Komponente Firewall-Verwaltung wurde zur Komponente Firewall überarbeitet, die neben ihrer Funktion als Schnittstelle zur Windows-Firewall jetzt auch als Firewall fungiert. Nach Abschluss der Migration müssen Sie den Modus dieser Komponente komplett neu konfigurieren.

- Um KSN zu verwenden, müssen Sie die KSN-Erklärung erneut lesen und akzeptieren.

- Die Versionen 4.0 und höhere Versionen des Programms unterstützen die Zeitplanung für einzelne Komponenten nicht. Aktivierte Komponenten werden weiterhin ausgeführt, während das Programm ausgeführt wird.

- Bei der Migration von Aufgaben kann sich die geplante Startzeit für die Aufgabe ändern. Dabei wird die Zeitzone berücksichtigt, die in den Betriebssystemeinstellungen des Computers festgelegt ist, auf dem die Migration ausgeführt wird. Angenommen, die Startzeit der Aufgabe in der älteren Programmversion ist 7:00 Uhr und die für das Betriebssystem konfigurierte Zeitzone ist UTC +3:00. Dann ändert sich die Startzeit nach der Migration der Aufgabe auf 10:00 Uhr.

- Der Abschnitt zur Auswahl von Aktionen für möglicherweise infizierte Objekte wurde aus den Einstellungen der Komponente „Echtzeitschutz für Dateien“ und der Aufgaben „Untersuchung auf Befehl“ entfernt. Diese Einstellungen werden nicht in die neuere Programmversion migriert.

- Kaspersky Security Center Web Console oder die Administrationskonsole können nicht verwendet werden, um Backup-Objekte zur Analyse an Kaspersky zu senden, falls sie nach einem Upgrade von Programmversion 3.4 oder früher auf Version 4.0 oder höher migriert wurden.

- Bei der Migration von Aufgaben zur Untersuchung auf Befehl ändert sich die standardmäßige Sicherheitsstufe für vordefinierte Untersuchungsbereiche von *Informieren* in *Benutzerdefiniert*.

- Wenn eine Komponente, die zuvor in der Installation enthalten war, während eines lokalen Upgrades von Kaspersky Embedded Systems Security nicht installiert wird, werden die Einstellungen dieser Komponente nicht gespeichert. Wenn Sie diese Komponente später installieren, werden dafür die Standardeinstellungen übernommen.

Vergleich der Komponenten und Aufgaben in Kaspersky Embedded Systems Security Version 3.4 und 4.1

Beim Upgrade von Kaspersky Embedded Systems Security 3.4 auf Version 4.1 werden die Komponenten und Aufgaben nur migriert, wenn das Programm lokal installiert ist.

Vergleich der Komponenten in Kaspersky Embedded Systems Security Version 3.4 und 4.1

Komponente von Kaspersky Embedded Systems Security 3.4	Komponente von Kaspersky Embedded Systems Security 4.1
Vertrauenswürdige Zone	Vertrauenswürdige Zone
Echtzeitschutz für Dateien	Echtzeitschutz für Dateien
Verwendung von KSN	KSN-Nutzung
Exploit-Prävention	Exploit-Prävention
AMSI-Untersuchung	AMSI-Scanner
Kontrolle des Programmstarts	Kontrolle des Programmstarts
Gerätekontrolle	Gerätekontrolle
Firewall-Verwaltung	Firewall Die Windows-Firewall fungiert als Firewall von Kaspersky Embedded Systems Security 3.4. Dabei wird die Windows-Firewall vom Programm verwaltet. In Kaspersky Embedded Systems Security 4.1 ist eine separate Komponente für die Firewall-Funktionalität verantwortlich.
Schutz vor Netzwerkbedrohungen	Schutz vor Netzwerkbedrohungen
Überwachung der Datei-Integrität	Überwachung der Systemintegrität Die Funktionalität der Komponenten Überwachung der Datei-Integrität und Überwachung des Registrierungszugriffs wurde mit der Komponente „Überwachung der Systemintegrität“ zusammengeführt.
Protokollanalyse	Protokollanalyse

Komponente von Kaspersky Embedded Systems Security 3.4	Komponente von Kaspersky Embedded Systems Security 4.1
Überwachung des Registrierungszugriffs	Überwachung der Systemintegrität Die Funktionalität der Komponenten Überwachung der Datei-Integrität und Überwachung des Registrierungszugriffs wurde mit der Komponente „Überwachung der Systemintegrität“ zusammengeführt.
(nicht vorhanden)	Verhaltensanalyse
(nicht vorhanden)	Rollback von schädlichen Aktionen
Aufgabe von Kaspersky Embedded Systems Security 3.4	**Aufgabe von Kaspersky Embedded Systems Security 4.1**
Programm aktivieren	Aktivierung des Programms
Update-Verteilung	Update Die Funktionalität der Aufgabe „Update-Verteilung“ wurde mit der Aufgabe „Update“ zusammengeführt.
Überwachung der Baseline-Integrität	Baseline-Überwachung der Systemintegrität
Update der Programm-Datenbanken	Update Die Funktionalität der Aufgabe „Datenbanken-Update“ wurde mit der Aufgabe „Update“ zusammengeführt.
Update der Programm-Module	Update Die Funktionalität der Aufgabe „Update der Programm-Module“ wurde mit der Aufgabe „Update“ zusammengeführt.
Rollback des Updates der Programm-Datenbanken	Update-Rollback
Untersuchung auf Befehl	Untersuchung auf Befehl
Integritätsprüfung für Programme	Kontrolle der Anwendungsintegrität
Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts	Erstellen von Regeln für die Kontrolle des Programmstarts
Erstellen von Regeln für die Gerätekontrolle	Erstellen von Regeln für die Gerätekontrolle
(nicht vorhanden)	Schutz der Verbindung zum Administrationsserver
(nicht vorhanden)	Komponenten für Kaspersky Embedded Systems Security ändern
(nicht vorhanden)	Status der Systemintegrität zurücksetzen

Programmoberfläche

Sie können Kaspersky Embedded Systems Security mit den folgenden Benutzeroberflächen verwalten:

- Anwendungskonsole.
- Kaspersky Security Center-Verwaltungskonsole.
- Kaspersky Security Center Web Console.

Kaspersky Security Center-Verwaltungskonsole

Mit Kaspersky Security Center können Sie Kaspersky Embedded Systems Security remote installieren und deinstallieren, starten und beenden, dessen Programm-Einstellungen anpassen, den Satz der verfügbaren Programmkomponenten ändern, Schlüssel hinzufügen, sowie Aufgaben starten und beenden.

Das Programm kann über Kaspersky Security Center mit dem Kaspersky Embedded Systems Security Administrations-Plug-in verwaltet werden. Ausführliche Informationen über die Benutzeroberfläche von Kaspersky Security Center finden Sie in der Hilfe von Kaspersky Security Center.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (im Folgenden auch als Web Console bezeichnet) ist ein Web-Programm, das für die zentrale Durchführung der Hauptaufgaben zur Verwaltung und Wartung des Sicherheitssystems eines Unternehmensnetzwerks ausgerichtet ist. Kaspersky Security Center Web Console ist eine Komponente von Kaspersky Security Center, das eine Benutzeroberfläche zur Verfügung stellt. Ausführliche Informationen zu „Kaspersky Security Center Web Console“ finden Sie in der Hilfe zu Kaspersky Security Center.

Die folgenden Aktionen sind für die Web Console verfügbar:

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

Arbeiten mit dem Verwaltungs-Plug-in

Dieser Abschnitt bietet Informationen über das Verwaltungs-Plug-in von Kaspersky Embedded Systems Security und beschreibt, wie das auf einem geschützten Gerät oder einer Gruppe von Geräten installierte Programm verwaltet wird.

Verwaltung von Kaspersky Embedded Systems Security über Kaspersky Security Center

Sie können mehrere geschützte Geräte, auf denen Kaspersky Embedded Systems Security installiert ist und die derselben Administrationsgruppe angehören, über das Kaspersky Embedded Systems Security Administration Plug-in zentral verwalten. Mit Kaspersky Security Center können Sie auch die Einstellungen für jedes geschützte Gerät in der Administrationsgruppe separat konfigurieren.

Eine Administrationsgruppe wird manuell über Kaspersky Security Center erstellt. Eine Gruppe beinhaltet mehrere Geräte, auf denen Kaspersky Embedded Systems Security installiert ist und für die Sie einheitliche Verwaltungs- und Schutzeinstellungen festlegen möchten. Ausführliche Informationen über die Verwendung von Administrationsgruppen finden Sie im Hilfesystem von Kaspersky Security Center.

Die Programmeinstellungen für ein einzelnes geschütztes Gerät sind nicht verfügbar, wenn die Arbeit von Kaspersky Embedded Systems Security auf dem geschützten Gerät durch die aktive Richtlinie von Kaspersky Security Center kontrolliert wird.

In Kaspersky Security Center sind für den Start des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security keine weiteren Aktionen erforderlich. Nachdem das Verwaltungs-Plug-in auf dem geschützten Gerät des Administrators installiert ist, wird es zusammen mit einem beliebigen Typ der Kaspersky Security Center-Verwaltungskonsole gestartet.

Sie können Kaspersky Embedded Systems Security auf folgende Arten durch Kaspersky Security Center verwalten:

- **Mithilfe der Richtlinien von Kaspersky Security Center**. Die Richtlinien von Kaspersky Security Center ermöglichen es, einheitliche Schutzeinstellungen für Gerätegruppen per Fernzugriff zu konfigurieren. Die in der aktiven Richtlinie festgelegten Aufgabeneinstellungen haben Priorität vor den Aufgabeneinstellungen, die lokal in der Programmkonsole oder per Remote-Zugriff im Fenster **Eigenschaften: <Name des geschützten Geräts>** von Kaspersky Security Center konfiguriert wurden.

  Mithilfe von Richtlinien lassen sich allgemeine Programmeinstellungen, Einstellungen für Aufgaben zum Echtzeit-Computerschutz, Aufgaben zur Aktivitätskontrolle auf Geräten, Einstellungen für den Schutz von Netzwerkspeichern und Einstellungen für den Start lokaler Systemaufgaben nach einem Zeitplan konfigurieren.

- **Mit Hilfe der Gruppenaufgaben von Kaspersky Security Center**. Die Gruppenaufgaben von Kaspersky Security Center ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit einer begrenzten Ausführungsdauer für Gerätegruppen per Fernzugriff.

  Mithilfe von Gruppenaufgaben können Sie das Programm aktivieren sowie die Einstellungen der Aufgaben „Untersuchung auf Befehl“, der Update-Aufgabe und der Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts konfigurieren.

- **Mithilfe von Aufgaben für eine Auswahl von Geräten**. Aufgaben für eine Auswahl von Geräten ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit begrenzter Ausführungsdauer und für geschützten Geräte, die keiner Administrationsgruppe zugeordnet sind, per Fernzugriff.

- **Mithilfe des Konfigurationsfensters für ein einzelnes Gerät**. Im Fenster **Eigenschaften: <Name des geschützten Geräts>** können Sie die Aufgabeneinstellungen für ein einzelnes geschütztes Gerät, das einer Administrationsgruppe zugeordnet ist, per Fernzugriff konfigurieren. Sie können außerdem sowohl allgemeine Programmeinstellungen als auch Einstellungen für alle Aufgaben von Kaspersky Embedded Systems Security anpassen, wenn das ausgewählte geschützte Gerät sich nicht unter der Verwaltung der aktiven Richtlinie von Kaspersky Security Center befindet.

Programmeinstellungen verwalten

Dieser Abschnitt enthält Informationen über die Konfiguration der allgemeinen Einstellungen von Kaspersky Embedded Systems Security in der Kaspersky Security Center-Verwaltungskonsole.

Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center

Sie können die allgemeinen Einstellungen von Kaspersky Embedded Systems Security für Gruppen von geschützten Geräten und für ein einzelnes geschütztes Gerät über Kaspersky Security Center konfigurieren.

Einstellungen der Benutzeroberfläche und Untersuchungseinstellungen in Kaspersky Security Center konfigurieren

Um die Skalierbarkeitseinstellungen und die Programmoberfläche zu konfigurieren, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole.

2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.

3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:

   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.

   - Um die Einstellungen einer Aufgabe oder eines Programms für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und wechseln Sie zu den lokalen Aufgabeneinstellungen oder den Programmeinstellungen.

4. Klicken Sie im Abschnitt **Programmeinstellungen** im Unterabschnitt **Einstellungen der Benutzeroberfläche** auf die Schaltfläche **Einstellungen**.

5. Konfigurieren Sie im Fenster **Einstellungen der Benutzeroberfläche** auf der Registerkarte **Allgemein** die folgenden Einstellungen:

   - Legen Sie im Abschnitt **Interaktion mit dem Benutzer** fest, ob das Taskleistensymbol nach jedem Start des Programms in der Taskleiste angezeigt werden soll.

     - **Benutzeroberfläche anzeigen**. Auf dem Client-Computer wird ein Symbol in der Windows-Taskleiste angezeigt. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Embedded Systems Security ausführen. Kaspersky Embedded Systems Security zeigt Benachrichtigungen über dem Programmsymbol an. Über das Kontextmenü des Symbols in der Windows-Taskleiste können Sie das kompakte Diagnosefenster öffnen. Wenn Sie im kompakten Diagnosefenster auf einen Link klicken, wird die Anwendungskonsole geöffnet.

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

   - Im Abschnitt **Statusvarianten** können Sie festlegen, welche Warnungen im Taskleistensymbol von Kaspersky Embedded Systems Security angezeigt werden sollen.

6. Klicken Sie auf **OK**.

Die vorgenommenen Programmeinstellungen werden gespeichert.

Sicherheitseinstellungen in Kaspersky Security Center anpassen

Um die Sicherheitseinstellungen manuell anpassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole.

2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.

3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:

   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.

   - Um die Einstellungen einer Aufgabe oder eines Programms für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und wechseln Sie zu den lokalen Aufgabeneinstellungen oder den Programmeinstellungen.

4. Klicken Sie im Abschnitt **Programmeinstellungen** im Unterabschnitt **Sicherheit und Zuverlässigkeit** auf die Schaltfläche **Einstellungen**.

5. Konfigurieren Sie im Fenster **Sicherheitseinstellungen** auf der Registerkarte **Sicherheit** die folgenden Einstellungen:

   - Wir empfehlen Ihnen, im Abschnitt **Allgemein** die Option **Programm beim Hochfahren des Computers starten (empfohlen)** aktiviert zu lassen (Standardeinstellung).

   - Aktivieren oder deaktivieren Sie im Abschnitt **Selbstschutz** die Funktionalität Programmprozesse vor externen Bedrohungen schützen.

- Legen Sie im Abschnitt **Aktionen beim Wechsel auf USV-Stromversorgung** die von Kaspersky Embedded Systems Security beim Wechsel auf eine USV-Quelle erzeugte Belastungsbeschränkung auf den geschützten Geräten fest:

  - **Geplante Untersuchungsaufgaben nicht starten**
  - **Laufende Untersuchungsaufgaben abbrechen**

- Konfigurieren im Abschnitt **Computerstatus beim Anwenden von Einstellungen** die Anzeige des Status der Client-Computer, auf denen das Programm installiert ist, falls beim Anwenden einer Richtlinie oder bei der Aufgabenausführung Fehler auftreten.

- Konfigurieren Sie im Abschnitt **Kompatibilitätseinstellungen** die Einstellung **Kompatibilität mit Fernverwaltungsanwendungen**.

6. Konfigurieren Sie auf der Registerkarte **Untersuchungseinstellungen** die folgenden Einstellungen:

   - **CPU-Auslastung für Untersuchungsaufgaben begrenzen**. Während auf einem geschützten Gerät eine Untersuchung auf Befehl durchgeführt wird, begrenzt Kaspersky Embedded Systems Security die CPU-Nutzung auf dem Gerät mit dem im Feld **Obergrenze** angegeben Wert. Das Aktivieren dieser Einstellung kann sich negativ auf die Leistung von Kaspersky Embedded Systems Security auswirken.

   - **Ressourcen für andere Programme freigeben**. Während der Computer untersucht wird, beansprucht Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security mehr Zeit benötigt, um den Computer zu untersuchen. Der Modus zur Freigabe von Ressourcen für andere Programme ist standardmäßig aktiviert.

7. Klicken Sie auf **OK**.

Die konfigurierten Sicherheitseinstellungen werden gespeichert.

Verbindungseinstellungen über Kaspersky Security Center anpassen

Die angepassten Verbindungseinstellungen werden verwendet: für die Verbindungsaufnahme von Kaspersky Embedded Systems Security mit den Update- und Aktivierungsservern sowie bei der Integration des Programms in die Dienste von Kaspersky Security Network.

Zum Einrichten der Verbindungseinstellungen gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole.

2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.

3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:

   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.

   - Um die Einstellungen einer Aufgabe oder eines Programms für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und wechseln Sie zu den lokalen Aufgabeneinstellungen oder den Programmeinstellungen.

4. Klicken Sie im Abschnitt **Programmeinstellungen** im Unterabschnitt **Verbindungseinstellungen** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Verbindungseinstellungen** wird geöffnet.

5. Klicken Sie im Abschnitt **Proxyserver** auf **Einstellungen**.

6. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster im Abschnitt **Proxyserver-Einstellungen** aus, wie die Proxyserver-Einstellungen verwaltet werden sollen:

   - **Keinen Proxyserver verwenden**. Wenn diese Option ausgewählt ist, verwendet Kaspersky Embedded Systems Security keinen Proxyserver.

   - **Proxyserver-Einstellungen automatisch ermitteln.** Wenn diese Option ausgewählt ist, verwendet Kaspersky Embedded Systems Security die Proxyserver-Einstellungen des Betriebssystems.

   - **Angegebene Proxyserver-Einstellungen verwenden**. Wenn diese Option ausgewählt ist, verwendet Kaspersky Embedded Systems Security die manuell angegebenen Proxyserver-Einstellungen. Geben Sie die IP-Adresse oder den symbolischen Namen des Proxyservers sowie die Portnummer ein.

     Deaktivieren Sie bei Bedarf das Kontrollkästchen **Einen Proxyserver für lokale Adressen umgehen**. Wenn diese Funktionalität aktiviert ist, erfolgt der Zugriff auf Geräte direkt aus dem Netzwerk, zu dem das geschützte Gerät mit installiertem Kaspersky Embedded Systems Security gehört. Diese Option ist standardmäßig aktiviert.

7. Wählen Sie im Abschnitt **Einstellungen der Proxyserver-Authentifizierung** in der Dropdown-Liste die Methode für die Authentifizierung beim Proxyserver aus:

   a. Wenn Sie **Proxyserver-Einstellungen automatisch ermitteln** ausgewählt haben:

      - **Keine Authentifizierung verwenden**.

      - **NTLM-Authentifizierung**. NTLM-Authentifizierung mit dem aktuellen Benutzerkonto (Standard).

      - **Kerberos-Authentifizierung**. Kerberos-Authentifizierung mit dem aktuellen Benutzerkonto.

   b. Wenn Sie **Angegebene Proxyserver-Einstellungen verwenden** ausgewählt haben:

      - **Keine Authentifizierung verwenden**.

      - **NTLM-Authentifizierung**. NTLM-Authentifizierung mit dem aktuellen Benutzerkonto (Standard).

      - **NTLM-Authentifizierung mit Benutzername und Kennwort**. NTLM-Authentifizierung mit manuell angegebenen Anmeldedaten.

- **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.

- **Benutzername und Kennwort**. Authentifizierung mit manuell angegebenen Anmeldedaten.

Geben Sie bei Bedarf einen Benutzernamen und ein Kennwort ein.

Wenn die Kerberos-Authentifizierung ausgewählt ist, kann Kaspersky Embedded Systems Security abhängig von den Proxyserver-Einstellungen die Authentifizierung anhand des Kerberos- oder NTLM-Protokolls durchführen.

8. Aktivieren oder deaktivieren Sie im Abschnitt **Lizenzverwaltung** das Kontrollkästchen **Kaspersky Security Center als Proxyserver für die Programmaktivierung verwenden**.

9. Klicken Sie auf **OK**.

10. Geben Sie im Abschnitt **Überwachte Ports** eine Option für Netzwerkports an:

    - **Alle Netzwerkports überwachen**. In diesem Modus zur Überwachung von Netzwerkports überwachen die Schutzkomponenten die Datenströme, die über beliebige offene Netzwerkports des Computers übertragen werden.

    - **Nur ausgewählte Netzwerkports überwachen**. In diesem Überwachungsmodus für Netzwerkports kontrollieren die Schutzkomponenten die ausgewählten Ports des Computers und die Netzwerkaktivität der ausgewählten Programme. Eine Liste der Netzwerkports, über die E-Mail-Nachrichten und Netzwerkverkehr gewöhnlich übertragen werden, ist gemäß der Empfehlungen der Kaspersky-Experten vorgegeben. Bei Bedarf können Sie die Liste der Netzwerkports bearbeiten.

11. Klicken Sie auf die Schaltfläche **Einstellungen** und bearbeiten Sie die folgenden Einstellungen:

    - **Alle Ports für Programme überwachen, die auf der von Kaspersky empfohlenen Liste stehen**. Kaspersky Embedded Systems Security überwacht die Netzwerkports von Programmen aus der vordefinierten Liste. Diese Liste enthält z. B. Google Chrome, Adobe Reader, Java und andere Programme.

    - **Alle Ports für die angegebenen Programme überwachen**. Kaspersky Embedded Systems Security überwacht die Netzwerkports von Programmen, die zur Liste hinzugefügt wurden.

12. Klicken Sie auf **OK**.

Die vorgenommenen Verbindungseinstellungen werden gespeichert.

Konfigurieren des Ausführungsmodus für lokale Aufgaben

Sie können Richtlinien verwenden, um den Start von lokalen Systemaufgaben zur Untersuchung auf Befehl und zum Update zuzulassen oder zu blockieren. Dies erfolgt gemäß des Zeitplans, der lokal auf jedem geschützten Gerät in der Administrationsgruppe konfiguriert wurde:

- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie verboten ist, werden solche Aufgaben nicht auf dem geschützten Gerät gemäß Zeitplan ausgeführt. Sie können lokale Systemaufgaben manuell starten.

- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie erlaubt ist, werden solche Aufgaben gemäß den lokal für diese Aufgabe angepassten Zeitplan-Einstellungen ausgeführt.

Standardmäßig ist der Start von lokalen Systemaufgaben durch eine Richtlinie verboten.

Es wird empfohlen, den Start lokaler Systemaufgaben nicht zu erlauben, wenn die Updates oder die Untersuchungen auf Befehl anhand von Gruppenaufgaben von Kaspersky Security Center gesteuert werden.

Wenn Sie keine Gruppenaufgaben für Updates oder Untersuchungen auf Befehl verwenden, erlauben Sie den Start lokaler Systemaufgaben in einer Richtlinie: Kaspersky Embedded Systems Security wird Updates der Datenbanken und Programm-Module ausführen und alle lokalen Systemaufgaben zur Untersuchung auf Befehl gemäß den standardmäßigen Zeitplan-Einstellungen starten.

Mithilfe von Richtlinien können Sie den Start folgender lokaler Systemaufgaben nach Zeitplan erlauben oder verbieten:

- Aufgaben zur Untersuchung auf Befehl: *Untersuchung wichtiger Bereiche*, *Untersuchung beim Start des Betriebssystems*, *Kontrolle der Anwendungsintegrität*, *Baseline-Überwachung der Systemintegrität*.

- Update-Aufgaben: *Update der Datenbanken und Programm-Module*, *Programm-Update*.

Wenn Sie ein geschütztes Gerät aus der Administrationsgruppe ausschließen, wird der Zeitplan der lokalen Systemaufgaben automatisch aktiviert.

So erlauben oder verbieten Sie die Verwaltung des Startzeitplans für die lokalen Aufgaben des Programms (in einer Richtlinie):

1. Erweitern Sie in der Struktur der Kaspersky Security Center-Verwaltungskonsole den Knoten **Verwaltete Geräte**, erweitern Sie die entsprechende Gruppe und wählen Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.

2. Auf der Registerkarte **Richtlinien** im Kontextmenü der Richtlinie, für die Sie den Start von lokalen Systemaufgaben für Kaspersky Embedded Systems Security auf der Gruppe der geschützten Geräte planen möchten, wählen Sie **Eigenschaften**.

3. Wählen Sie im Eigenschaftenfenster der Richtlinie den Abschnitt **Programmeinstellungen** aus.

4. Klicken Sie im Unterabschnitt **Lokale Systemaufgaben ausführen** auf **Einstellungen**.

5. Aktivieren Sie das Kontrollkästchen **Verwendung lokaler Aufgaben erlauben**.

6. Verwenden Sie das Kontrollkästchen **Verwaltung von Zeitplänen erlauben**, um die Verwaltung des Startzeitplans für die lokalen Aufgaben des Programms zu erlauben oder zu verbieten.

Backup-Einstellungen in Kaspersky Security Center konfigurieren

Um die Backup-Einstellungen in Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole.

2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.

3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:

   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.

   - Um die Einstellungen einer Aufgabe oder eines Programms für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und wechseln Sie zu den lokalen Aufgabeneinstellungen oder den Programmeinstellungen.

4. Wechseln Sie zum Abschnitt **Zusätzlich**.

5. Klicken Sie im Unterabschnitt **Speicher** auf die Schaltfläche **Einstellungen**.

6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Speichereinstellungen

Einstellung	Beschreibung
Nehmen Sie auf der Registerkarte **Berichte** die folgenden Berichtseinstellungen vor:	
Berichte speichern für maximal	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 Embedded Systems Security automatisch die ältesten Einträge aus der Berichtsdatei.
Maximale Größe der Berichtsdatei	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 Embedded Systems Security automatisch die ältesten Einträge aus der Berichtsdatei. Dadurch ist gewährleistet, dass die maximale Berichtsdateigröße nicht überschritten wird.
Nehmen Sie auf der Registerkarte **Backup** die folgenden Backup-Einstellungen vor:	
Objekte speichern für maximal	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 Embedded Systems Security die ältesten Dateien aus dem Backup.
Maximale Größe des Backups	Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 400 MB. Nach Erreichen der maximalen Backup-Größe löscht Kaspersky Embedded Systems Security automatisch die ältesten Dateien. Dadurch ist gewährleistet, dass die maximale Backup-Größe nicht überschritten wird.
Grenzwert für verfügbaren Speicherplatz	Das Kontrollkästchen aktiviert oder deaktiviert die Verfolgung der minimalen Größe des freien Speicherplatzes im Backup (standardmäßig 100 MB). Ist der Umfang des freien Speicherplatzes kleiner als der vorgegebene Grenzwert, protokolliert Kaspersky Embedded Systems Security das Ereignis *Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* und benachrichtigt gemäß den Benachrichtigungseinstellungen über Ereignisse dieses Typs. Wenn dieses Kontrollkästchen aktiviert ist, verfolgt Kaspersky Embedded Systems Security die Größe des freien Speicherplatzes im Backup. Das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz** ist aktiv, wenn das Kontrollkästchen **Maximale Größe des Backups** aktiviert ist.

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt bietet Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Embedded Systems Security auf mehreren geschützten Geräten.

Sie können in Kaspersky Security Center einheitliche Richtlinien erstellen, um den Schutz auf mehreren Geräten zu verwalten, auf denen Kaspersky Embedded Systems Security installiert ist.

Eine Richtlinie erzwingt die Einstellungen, Funktionen und Aufgaben von Kaspersky Embedded Systems Security auf allen geschützten Geräten einer Administrationsgruppe.

Sie können mehrere Richtlinien für eine Administrationsgruppe erstellen und sie temporär übernehmen. Die in der Gruppe aktuell gültige Richtlinie hat in der Verwaltungskonsole den Status *aktiv*.

Informationen über den Geltungsbereich einer Richtlinie werden im Systemaudit-Protokoll von Kaspersky Embedded Systems Security protokolliert. Diese Informationen stehen in der Programmkonsole unter dem Knoten **Protokollanalyse** zur Verfügung.

In Kaspersky Security Center bietet eine Methode zum Übernehmen von Richtlinien auf geschützten Geräten: *Bearbeitung von Einstellungen verbieten*. Nachdem eine Richtlinie übernommen wurde, verwendet Kaspersky Embedded Systems Security die Werte der Einstellungen, für die Sie in den Richtlinieneigenschaften die Option **Änderungen sind verboten** festgelegt haben. In diesem Fall verwendet Kaspersky Embedded Systems Security nicht die Werte der Einstellungen, die vor Anwendung der Richtlinie wirksam waren. Die Werte der aktiven Richtlinie, für die Sie in den Richtlinieneigenschaften die Option **Änderungen sind erlaubt** festgelegt haben, werden von Kaspersky Embedded Systems Security nicht übernommen.

Ist eine Richtlinie aktiv, so werden die Werte der Einstellungen, die in der Richtlinie mit dem Symbol markiert sind, in der Programmkonsole angezeigt, können jedoch nicht bearbeitet werden. Die Werte anderer Einstellungen können in der Anwendungskonsole bearbeitet werden.

Die in der aktiven Richtlinie festgelegten und mit dem Symbol markierten Einstellungen blockieren auch die Bearbeitung der Einstellungen in Kaspersky Security Center für ein einzelnes geschütztes Gerät im Fenster **Eigenschaften: <Name des geschützten Geräts>**.

Einstellungen, die angepasst und mithilfe einer aktiven Richtlinie an das geschützte Gerät übergeben wurden, werden nach der Deaktivierung der aktiven Richtlinie in den Einstellungen der lokalen Aufgaben gespeichert.

Wenn eine Richtlinie die Einstellungen einer momentan laufenden Echtzeit-Computerschutz-Aufgabe oder einer Aufgabe zum Schutz von netzgebundenen Speichern festlegt, ändern sich die durch die Richtlinie definierten Einstellungen sofort nach dem Anwenden der Richtlinie. Wenn die Aufgabe nicht ausgeführt wird, werden die Parameter aus der Richtlinie beim nächsten Aufgabenstart übernommen.

Richtlinie erstellen

Bevor Sie eine Richtlinie erstellen, müssen Sie das Verwaltungs-Plug-in klcfginst.exe installieren.

So erstellen Sie eine Richtlinie für eine Gruppe geschützter Geräte, auf denen eine Anwendung installiert ist und ausgeführt wird:

1. Erweitern Sie in der Struktur der Kaspersky Security Center-Verwaltungskonsole den Knoten **Verwaltete Geräte** und wählen Sie anschließend die Administrationsgruppe aus, für deren geschützte Geräte Sie eine Richtlinie erstellen möchten.

2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Richtlinien** und klicken Sie auf **Neue Richtlinie**, um den Assistenten für neue Richtlinien zu starten.

   Das Fenster **Assistent für das Erstellen einer Richtlinie** wird geöffnet.

3. Wählen Sie im Fenster **Anwendung für das Erstellen einer Gruppenrichtlinie auswählen** das Programm „Kaspersky Embedded Systems Security“ aus.

4. Klicken Sie auf **Weiter**.

5. Geben Sie einen Gruppenrichtliniennamen in das Feld **Name** ein.

   Die Namen von Richtlinien dürfen keines der folgenden Symbole enthalten: `" * < : > ? \ | .`

6. Gehen Sie wie folgt vor, um eine Richtlinienkonfiguration einer früheren Programmversion zu verwenden:

   a. Aktivieren Sie das Kontrollkästchen **Richtlinieneinstellungen für eine frühere Version der Anwendung verwenden**.

   b. Klicken Sie auf **Durchsuchen**.

   c. Wählen Sie die Richtlinie aus, die Sie übernehmen möchten.

   d. Klicken Sie auf **Weiter**.

7. Aktivieren Sie im Fenster **Vorgangsart auswählen** im Block **Echtzeitschutz für Dateien konfigurieren** das Kontrollkästchen **Echtzeitschutz für Dateien aktivieren** und geben Sie die Sicherheitsstufe an.

   Wenn kein Startmodus für die Aufgabe ausgewählt ist, können Sie nicht mit dem nächsten Schritt des Assistenten für neue Richtlinien fortfahren.

8. Konfigurieren Sie den Echtzeit-Computerschutz.

9. Konfigurieren Sie Untersuchungsausnahmen und vertrauenswürdige Programme.

10. Wählen Sie im Fenster **Erstellen einer neuen Gruppenrichtlinie für die Anwendung** einen der folgenden Richtlinienstatus aus:

    - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie sofort nach dem Erstellen in Kraft tritt. Wenn in der Gruppe bereits eine aktive Richtlinie existiert, dann wird diese deaktiviert und die eine neue Richtlinie übernommen.

    - **Inaktive Richtlinie**, wenn die Richtlinie nicht sofort in Kraft treten soll. Sie können diese Richtlinie später aktivieren.

- **Richtlinie für mobile Benutzer**, die Richtlinie wird nur aktiviert, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.

- Aktivieren Sie das Kontrollkästchen **Richtlinieneigenschaften sofort nach ihrer Erstellung öffnen**, damit der **Assistent für das Erstellen einer Richtlinie** automatisch geschlossen und die neu erstellte Richtlinie konfiguriert wird, nachdem Sie auf **Weiter** geklickt haben.

11. Klicken Sie auf **Fertigstellen**.

    Die erstellte Richtlinie wird in der Richtlinienliste auf der Registerkarte **Richtlinien** der ausgewählten Administrationsgruppe angezeigt. Im Fenster **Eigenschaften: <Name der Richtlinie>** können Sie andere Einstellungen, Aufgaben und Funktionen von Kaspersky Embedded Systems Security anpassen.

Nachdem eine neue Richtlinie erstellt wurde, wird eine Reihe von Erlaubnisregeln erstellt, um das Blockieren von Programmen zu verhindern und ihren unterbrechungsfreien Betrieb zu gewährleisten.

Standardmäßig erstellt Kaspersky Embedded Systems Security bei der Erstellung einer neuen Richtlinie einen Satz von Regeln für den eingehenden Netzwerkverkehr:

- Zwei Erlaubnisregeln für die Freigabe des Windows-Desktops mithilfe des Kaspersky Security Center Administrationsagenten, der sich in den Ordnern %Programme% und %Programme (x86)% befindet. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

- Zwei Erlaubnisregeln für den lokalen Port 15000. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

Standardmäßig erstellt Kaspersky Embedded Systems Security beim Erstellen einer neuen Richtlinie einen Satz von Regeln für den ausgehenden Netzwerkverkehr:

- Zwei Erlaubnisregeln für den Dienst Kaspersky Embedded Systems Security, der sich in den Ordnern %Programme% und %Programme (x86)% befindet. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

- Zwei Erlaubnisregeln für den Arbeitsprozess von Kaspersky Embedded Systems Security, der sich in den Ordnern %Programme% und %Programme (x86)% befindet. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

- Zwei Erlaubnisregeln für den lokalen Port 13000. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

Anpassen einer Richtlinie

Gehen Sie wie folgt vor, um die Richtlinieneinstellungen zu konfigurieren:

1. Öffnen Sie in der Struktur der Kaspersky Security Center-Verwaltungskonsole den Knoten **Verwaltete Geräte**.

2. Erweitern Sie die Administrationsgruppe, für die Sie die zugehörigen Richtlinieneinstellungen anpassen möchten und öffnen Sie die Registerkarte **Richtlinien** im Detailbereich.

3. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Richtlinienname>** zu öffnen:

- Wählen Sie im Kontextmenü der Richtlinie die Option **Eigenschaften** aus.
- Doppelklicken Sie auf die ausgewählte Richtlinie.

4. Aktivieren oder deaktivieren Sie die Richtlinie auf der Registerkarte **Allgemein** im Abschnitt **Richtlinienstatus**. Wählen Sie dazu eine der folgenden Varianten:
   - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie auf allen geschützten Geräten angewendet wird, die zur ausgewählten Administrationsgruppe gehören.
   - **Richtlinie für mobile Benutzer**, die Richtlinie wird nur aktiviert, wenn ein Computer den Perimeter des Unternehmensnetzwerks verlässt.
   - **Inaktive Richtlinie**, wenn Sie die Richtlinie später auf allen geschützten Geräten der ausgewählten Administrationsgruppe aktivieren möchten.
5. Konfigurieren Sie die Programmeinstellungen in den anderen Abschnitten der Richtlinie.

   Sie können die Ausführung einer beliebigen Aufgabe auf allen geschützten Geräten, die zu einer Administrationsgruppe gehören, mithilfe einer Richtlinie von Kaspersky Security Center aktivieren und deaktivieren.

   Sie können die Übernahme der in der Richtlinie festgelegten Einstellungen auf allen geschützten Geräten des Netzwerks für jede einzelne Programmkomponente festlegen.

6. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden in der Richtlinie übernommen.

Indikator des Schutzniveaus

Der Sicherheitsstufen-Indikator wird im oberen Bereich des Eigenschaftenfensters der Richtlinie angezeigt. Der Indikator kann einen der folgenden Werte annehmen:

- **Hohes Schutzniveau**. Der Indikator nimmt diesen Wert an und wird grün, wenn alle Komponenten der folgenden Kategorien aktiviert und mit markiert sind:
  - **Kritisch**. Diese Kategorie umfasst die folgenden Komponenten:
    - Echtzeitschutz für Dateien.
    - Verhaltensanalyse.
    - Exploit-Prävention.

- Rollback von schädlichen Aktionen.
- Meldungen für sicheren Desktop aktivieren.

- **Wichtig**. Diese Kategorie umfasst die Komponente KSN-Nutzung.

- **Mittleres Schutzniveau**. Der Indikator nimmt diesen Wert an und wird gelb, wenn eine wichtige Komponente deaktiviert oder mit markiert ist.
- **Niedriges Schutzniveau**. Der Indikator nimmt diesen Wert an und wird rot, wenn eine oder mehrere kritische Komponenten deaktiviert oder mit markiert sind.

Wenn der Indikator den Wert **Mittleres Schutzniveau** oder **Niedriges Schutzniveau** anzeigt, können Sie über einen Link rechts neben dem Indikator das Fenster **Empfohlene Schutzkomponenten** öffnen. In diesem Fenster können Sie die empfohlenen Schutzkomponenten separat aktivieren und das Deaktivieren dieser Komponenten verhindern.

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Embedded Systems Security, ihre Erstellung, die Konfiguration ihrer Ausführung sowie über den Start/die Beendigung von Aufgaben.

Über die Erstellung von Aufgaben in Kaspersky Security Center

Sie können Gruppenaufgaben für Administrationsgruppen und für Zusammenstellungen von geschützten Geräten erstellen. Sie können die folgenden Typen von Aufgaben über Kaspersky Security Center erstellen:

- *Aktivierung des Programms*
- *Schutz der Verbindung zum Administrationsserver*
- *Komponenten für Kaspersky Embedded Systems Security ändern*
- *Baseline-Überwachung der Systemintegrität*
- *Update*
- *Update-Rollback*
- *Untersuchung auf Befehl*
- *Kontrolle der Anwendungsintegrität*
- *Schlüssel löschen*
- *Erstellen von Regeln für die Kontrolle des Programmstarts*
- *Erstellen von Regeln für die Gerätekontrolle.*

Sie können lokale Aufgaben und Gruppenaufgaben auf folgende Art und Weise erstellen:

- Für ein bestimmtes geschütztes Gerät im Abschnitt **Aufgaben**.
- Für eine Administrationsgruppe: Im Ergebnisbereich des Knotens der ausgewählten Gruppe von geschützten Geräten auf der Registerkarte **Aufgaben**.
- Für eine Auswahl an geschützten Geräten: Im Ergebnisbereich des Knotens **Geräteauswahlen**.

Mithilfe von Richtlinien können Sie Zeitpläne für die lokalen Systemaufgaben *Update* und *Untersuchung auf Befehl* auf allen geschützten Geräten in derselben Administrationsgruppe deaktivieren.

Allgemeine Informationen über den Aufgaben in Kaspersky Security Center sind im *Hilfesystem von Kaspersky Security Center* zu finden.

Aufgabe mithilfe von Kaspersky Security Center erstellen

Gehen Sie folgendermaßen vor, um eine neue Aufgabe in der Kaspersky Security Center Verwaltungskonsole zu erstellen:

1. Starten Sie den Assistenten für neue Aufgaben nach einer der folgenden Methoden:
   - Für das Erstellen einer lokalen Aufgabe:
     a. In der Verwaltungskonsole klappen Sie den Knoten **Verwaltete Geräte** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
     b. Öffnen Sie im Ergebnisfenster der Registerkarte **Geräte** das Kontextmenü des geschützten Geräts und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im folgenden Fenster im Abschnitt **Aufgaben** auf die Schaltfläche **Hinzufügen**.
   - Für das Erstellen einer Gruppenaufgabe:
     a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole.
     b. Wählen Sie die Administrationsgruppe aus, für die Sie eine Aufgabe erstellen möchten.
     c. Öffnen Sie im Ergebnisfenster die Registerkarte **Aufgaben** und wählen Sie **Neue Aufgabe** aus.

   Darauf öffnet sich der Assistent für neue Aufgaben.
2. Wählen Sie im Fenster **Aufgabentyp auswählen** unter der Überschrift **Kaspersky Embedded Systems Security** den Typ der zu erstellenden Aufgabe aus.

3. Die Einstellungen können abhängig vom Aufgabentyp unterschiedlich sein:

   - Aufgabe zur Untersuchung auf Befehl erstellen.

   - Wenn Sie eine der Aufgaben zum Update erstellen, aktivieren Sie die gewünschten Aufgabenparameter nach Ihren Bedürfnissen:

     a. Im Block **Update-Quelle** können Sie den Kaspersky Security Center Administrationsserver oder die Kaspersky-Update-Server als Update-Quelle für das Programm-Update angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen.

     Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

     b. Konfigurieren Sie die Einstellungen für eine Funktion, die die Auslastung des Festplattensubsystems senkt:

     c. Sie können festlegen, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Updates für Programm-Module erforderlich sind oder nachdem die Installation wichtiger Updates abgeschlossen wurde. Darüber hinaus können Sie festlegen, ob Kaspersky Embedded Systems Security Informationen über verfügbare geplante Updates erhalten soll.

     d. Geben Sie die zu kopierenden Updates und den Pfad des Ordners an, in dem Kaspersky Embedded Systems Security die kopierten Updates speichert.

   - Um die Aufgabe *Aktivierung des Programms* zu erstellen:

     a. Geben Sie im Fenster **Aktivierungsparameter** die Schlüsseldatei oder den Aktivierungscode an, mit der bzw. dem Sie das Programm aktivieren möchten.

     b. Aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**, wenn Sie eine Aufgabe zur Verlängerung der Lizenz erstellen möchten.

   - Erstellen Sie die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts.

   - Erstellen Sie die Aufgabe Erstellen von Regeln für die Gerätekontrolle.

4. Passen Sie den Aufgabenzeitplan an.

5. Klicken Sie auf **OK**.

6. Wenn die Aufgabe für eine Zusammenstellung von geschützten Geräten erstellt wird, wählen Sie das Netzwerk (oder die Gruppe) der geschützten Geräte aus, an denen die Aufgabe ausgeführt werden soll.

7. Geben Sie im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll.

8. Geben Sie im Fenster **Aufgabenname festlegen** einen Aufgabennamen an (maximal 100 Zeichen, wobei folgende Zeichen unzulässig sind: `" * < > ? \ | :`).

   Wir empfehlen, dass Sie den Aufgabentyp zum Namen der Aufgabe hinzufügen (beispielsweise "Untersuchung von freigegebenen Ordnern auf Befehl").

9. Gehen Sie Fenster **Erstellung der Aufgabe abschließen** wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn die Aufgabe sofort nach ihrer Erstellung gestartet werden soll.

    b. Klicken Sie auf **Fertigstellen**.

Die erstellte Aufgabe erscheint in der Liste **Aufgaben**.

Zu den lokalen Aufgabeneinstellungen und den allgemeinen Programmeinstellungen für einen einzelnen Computer wechseln

Wenn das Programm der Kaspersky Security Center-Richtlinie unterliegt und diese Richtlinie die Änderung der Programmeinstellungen verbietet, können Sie diese Einstellungen für einen einzelnen Computer nicht bearbeiten.

So rufen Sie die lokalen Aufgabeneinstellungen für einen einzelnen Computer auf:

1. Öffnen Sie in der Struktur der Kaspersky Security Center Verwaltungskonsole den Knoten **Verwaltete Geräte**.
2. Wählen Sie die Gruppe aus, zu der das geschützte Gerät gehört.
3. Wählen Sie im Ergebnisfenster die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Name des geschützten Geräts>** zu öffnen:

    - Doppelklicken Sie auf den Namen des geschützten Geräts.
    - Wählen Sie im Kontextmenü des Namens des geschützten Geräts den Punkt **Eigenschaften** aus.

    Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.
5. Wechseln Sie in den Abschnitt **Aufgaben**.
6. Wählen Sie in der Aufgabenliste eine lokale Aufgabe aus, die Sie auf eine der folgenden Arten konfigurieren können:

    - Doppelklicken Sie auf den Aufgabennamen.
    - Wählen Sie eine Aufgabe aus der Liste aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
    - Wählen Sie im Kontextmenü des Aufgabennamens **Eigenschaften**.

    Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.

So rufen Sie die allgemeinen Programmeinstellungen für einen einzelnen Computer auf:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center-Verwaltungskonsole und wählen Sie die Gruppe aus, zu der das geschützte Gerät gehört.
2. Wählen Sie im Ergebnisfenster die Registerkarte **Geräte** aus.

3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Name des geschützten Geräts>** zu öffnen:

   - Doppelklicken Sie auf den Namen des geschützten Geräts.
   - Wählen Sie im Kontextmenü des Namens des geschützten Geräts den Punkt **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.

4. Wechseln Sie zum Abschnitt **Programme**.

5. Wählen Sie aus der Liste der installierten Programme Kaspersky Embedded Systems Security auf eine der folgenden Arten aus:

   - Doppelklicken Sie auf den Namen von Kaspersky Embedded Systems Security.
   - Wählen Sie in der Liste Kaspersky Embedded Systems Security aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
   - Wählen Sie im Kontextmenü des Namens von Kaspersky Embedded Systems Security den Punkt **Eigenschaften** aus.

   Das Fenster **Einstellungen** von **Kaspersky Embedded Systems Security** wird geöffnet.

Gruppenaufgaben in Kaspersky Security Center anpassen

Gehen Sie wie folgt vor, um eine Gruppenaufgabe für mehrere geschützte Geräte zu konfigurieren:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.

2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.

3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:

   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und klicken Sie auf den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

5. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.

6. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eines der Folgenden aus:

   - So konfigurieren Sie die *Untersuchung auf Befehl*-Aufgabe:

     - Legen Sie im Abschnitt **Untersuchungsbereich** einen Untersuchungsbereich fest.

     - Konfigurieren Sie im Abschnitt **Einstellungen** die Integration in andere Programmkomponenten sowie die Aufgabenpriorität.

   - So konfigurieren Sie die *Update*-Aufgabe:

     - Gehen Sie zum Abschnitt **Einstellungen** und geben Sie **Update-Einstellungen für Programm-Datenbanken und Module** an.

     - Wählen Sie eine auszuführende Aktion aus: Kopieren und installieren Sie wichtige Updates von Programm-Modulen oder nur danach suchen.

   - So konfigurieren Sie die *Aktivierung des Programms*-Aufgabe:

     - Geben Sie im Abschnitt **Einstellungen** die Schlüsseldatei oder den Aktivierungscode an, mit der bzw. dem Sie das Programm aktivieren möchten.

     - Aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**, wenn Sie einen Aktivierungscode oder eine Schlüsseldatei zur Verlängerung der Lizenz hinzufügen möchten.

   - Um die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* zu konfigurieren, geben Sie im Abschnitt **Einstellungen** die Einstellungen an, die Sie zum Erstellen von Gerätekontrolle-Regeln verwenden möchten.

7. Passen Sie den Aufgabenzeitplan im Abschnitt **Zeitplan** an.

8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.

9. Geben Sie bei Bedarf im Abschnitt **Ausschlüsse vom Gültigkeitsbereich der Aufgabe** die Objekte an, die Sie aus dem Aufgabenbereich ausschließen möchten. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.

10. Klicken Sie im Fenster Eigenschaften auf die Schaltfläche **OK**: **<Aufgabenname>**.

    Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Die konfigurierbaren Einstellungen für Gruppenaufgaben sind unten aufgeführt.

- Erstellen von Regeln für die Kontrolle des Programmstarts

  In den Einstellungen der Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* können Sie auf der Registerkarte **Regeln** auswählen, wie Erlaubnisregeln erstellt werden sollen:

  - **Erlaubnisregeln anhand von gestarteten Programmen erstellen**

  - **Erlaubnisregeln für Programme aus den Ordnern erstellen**

Auf der Registerkarte **Einstellungen** können Sie die folgenden Aktionen angeben, die beim Erstellen von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen:

- **Digitales Zertifikat verwenden**
- **Subjekt und Fingerabdruck des digitalen Zertifikats verwenden**
- **Falls kein Zertifikat vorhanden, verwende Folgendes**
- **SHA256-Hash verwenden**
- **Regeln für Benutzer und/oder Benutzergruppen generieren**.

Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.

Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

- Erstellen von Regeln für die Gerätekontrolle
  - Wählen Sie den Betriebsmodus aus: Berücksichtigen Sie Systemdaten über alle jemals angeschlossenen externen Geräte oder berücksichtigen Sie nur derzeit angeschlossene externe Geräte.
  - Passen Sie die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln an, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.
  - Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
- Aktivierung des Programms
  - Um das Programm zu aktivieren oder die Lizenz zu verlängern, können Sie eine Schlüsseldatei oder einen Aktivierungscode hinzufügen.
  - Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
- Update der Datenbanken und Programm-Module
  - Im Einstellungsblock **Update-Quelle** können Sie den Kaspersky Security Center Administrationsserver oder die Kaspersky-Update-Server als Update-Quelle für das Programm-Update angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen.

    Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.
  - Sie können die Einstellungen für eine Funktion konfigurieren, die die Auslastung des Festplattensubsystems senkt:
    - **Belastung des Festplatten-Subsystems verringern**
    - **Für die Optimierung genutzter Arbeitsspeicher (MB)**.
  - Sie können festlegen, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Updates für Programm-Module erforderlich sind oder nachdem die Installation wichtiger Updates abgeschlossen wurde. Darüber hinaus können Sie festlegen, ob Kaspersky Embedded Systems Security Informationen über verfügbare geplante Updates erhalten soll.

- Sie können die zu kopierenden Updates und den Pfad des Ordners angeben, in dem Kaspersky Embedded Systems Security die kopierten Updates speichert.
- Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

- Untersuchung auf Befehl
  - Sie können einen Untersuchungsbereich für die Aufgabe zur Untersuchung auf Befehl festlegen sowie zur Einstellung der Sicherheitsstufe wechseln.
  - Im Einstellungsblock **Heuristic analyzer** können Sie die Verwendung der heuristischen Analyse für die Aufgabe „Untersuchung auf Befehl“ aktivieren oder deaktivieren und die Analysestufe mithilfe eines Schiebereglers festlegen.
  - Im Block **Integration with other components** können Sie die folgenden Einstellungen konfigurieren:
    - Angegebene Aufgabe im Hintergrundmodus starten.
    - Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten.
    - Deaktivieren Sie den gleichzeitigen Start mehrerer Untersuchungsaufgaben.
  - Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
- Kontrolle der Anwendungsintegrität
  - Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
- Baseline-Überwachung der Systemintegrität
  - Sie können den Überwachungsmodus und die Regeln konfigurieren, die die Aktionen für Dateien, die Registrierung und Geräte festlegen.
  - Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Aufgabe zur Programmaktivierung

So konfigurieren Sie die Aktivierung des Programms-Aufgabe:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:

   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

   Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.

5. Geben Sie im Abschnitt **Aktivierungsparameter** die Schlüsseldatei an, mit der Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**, wenn Sie einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.

6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an.

7. Geben Sie bei Bedarf im Abschnitt **Ausnahmen vom Gültigkeitsbereich** der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

   Ausführliche Informationen zum Anpassen der Einstellungen in diesen Abschnitten finden Sie im Hilfesystem von Kaspersky Security Center.

8. Klicken Sie im Fenster Eigenschaften auf die Schaltfläche **OK**: **<Aufgabenname>**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Update-Aufgabe

So konfigurieren Sie die Update-Aufgabe:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.

2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.

3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:

   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

5. Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.

6. Gehen Sie im Abschnitt **Einstellungen** wie folgt vor:

   a. Wählen Sie über die Schaltfläche **Einstellungen** im Abschnitt **Update-Einstellungen für Programm-Datenbanken und Module** eine Update-Quelle aus:

      - Kaspersky Security Center Administrationsserver.
      - Kaspersky-Update-Server.
      - Andere HTTP-, FTP-Server oder Netzwerkressourcen.

      Um einen freigegebenen SMB-Ordner als Update-Quelle zu verwenden, müssen Sie ein Benutzerkonto für den Aufgabenstart festlegen.

      Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

   b. Konfigurieren Sie die Einstellungen für eine Funktion, die die Auslastung des Festplattensubsystems senkt:

      - **Belastung des Festplatten-Subsystems verringern**. Dieses Kontrollkästchen aktiviert oder deaktiviert den Prozess zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher. Das Kontrollkästchen ist standardmäßig deaktiviert.
      - **Für die Optimierung genutzter Arbeitsspeicher (MB)**

   c. Legen Sie fest, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Updates für Programm-Module verfügbar sind oder wenn Informationen über geplante Updates vorliegen.

   d. Geben Sie die Einstellungen für das Kopieren von Updates an.

7. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Update-Rollback anpassen).

8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird.

   Ausführliche Informationen zum Anpassen der Einstellungen in diesen Abschnitten finden Sie im Hilfesystem von Kaspersky Security Center.

9. Klicken Sie im Fenster **Eigenschaften <Aufgabenname>** auf **OK**.

Für die Aufgabe *Update-Rollback* können Sie nur die Standardaufgabeneinstellungen konfigurieren, die sich in Kaspersky Security Center in den Abschnitten **Benachrichtigungen** und **Ausnahmen vom Aufgabenbereich** befinden. Ausführliche Informationen zum Anpassen der Einstellungen in diesen Abschnitten finden Sie im Hilfesystem von Kaspersky Security Center.

Integritätsprüfung für Programme

So konfigurieren Sie die Gruppenaufgabe Kontrolle der Anwendungsintegrität:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.
5. Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.
6. Wählen Sie im Abschnitt **Geräte** die Geräte aus, für die Sie die Aufgabe zur *Kontrolle der Anwendungsintegrität* anpassen möchten.
7. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an.
8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird.
9. Geben Sie bei Bedarf im Abschnitt **Ausnahmen vom Gültigkeitsbereich** der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

   Ausführliche Informationen zum Anpassen der Einstellungen in diesen Abschnitten finden Sie im Hilfesystem von Kaspersky Security Center.
10. Klicken Sie im Fenster Eigenschaften auf die Schaltfläche **OK**: **<Aufgabenname>**.

Aufgaben planen

So planen Sie Aufgaben mithilfe des Verwaltungs-Plug-ins:

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.

4. Wechseln Sie zum Abschnitt **Aufgaben**.

5. Doppelklicken Sie, um das Eigenschaftenfenster der Aufgabe zu öffnen, für die Sie den Zeitplan konfigurieren möchten.

6. Wählen Sie den Abschnitt **Zeitplan** aus.

7. Konfigurieren Sie die Zeitplaneinstellungen (siehe folgende Tabelle) nach Ihren Anforderungen.

   Die Felder mit den Zeitplan-Einstellungen der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe stehen nicht zur Verfügung, wenn der Zeitplan dieser Aufgaben durch eine Richtlinie von Kaspersky Security Center blockiert wird.

8. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen für den Aufgabenstart zu speichern.

Wenn Sie Programmeinstellungen für eine einzelne Aufgabe mithilfe von Kaspersky Security Center konfigurieren möchten, siehe Abschnitt "Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen".

Einstellungen für den Aufgabenzeitplan

Einstellung	Beschreibung
Start nach Zeitplan	Wählen Sie den Funktionsmodus der Aufgabe aus: • **Alle n Stunden**. Die Aufgabe wird in regelmäßigen Abständen alle paar Stunden ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Stunden) an. • **Alle n Tage**. Die Aufgabe wird in regelmäßigen Abständen alle paar Tage ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Tagen) an. • **Alle n Minuten**. Die Aufgabe wird in regelmäßigen Abständen alle paar Minuten ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Minuten) an. • **Wöchentlich**. Die Aufgabe wird an einem bestimmten Wochentag ausgeführt. Geben Sie den Wochentag und die Startzeit an. • **Monatlich**. Die Aufgabe wird an einem bestimmten Tag des Monats ausgeführt. Geben Sie Datum und Uhrzeit des Starts an. • **Einmal**. Die Aufgabe wird einmal zum angegebenen Zeitpunkt (Datum und Uhrzeit) ausgeführt. • **Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. • **Nach dem Download von Updates in die Datenverwaltung**. Die Aufgabe wird jedes Mal ausgeführt, wenn Updates in die Datenverwaltung heruntergeladen werden. • **Nach Abschluss einer anderen Aufgabe**. Die Aufgabe wird ausgeführt, sobald eine andere Aufgabe abgeschlossen wird. Wählen Sie die Aufgabe und den Aufgabenstatus aus. Kaspersky Embedded Systems Security unterstützt den Modus **Nach Abschluss einer anderen Aufgabe** für die Zeitplanung lokaler Aufgaben nicht. • **Beim Erkennen eines Virenangriffs**. Die Aufgabe wird ausgeführt, wenn ein Virenangriff erkannt wird. • **Bei Anwendungsstart**. Die Aufgabe wird jedes Mal beim Start von Kaspersky Embedded Systems Security ausgeführt.
Übersprungene Aufgaben starten	Ist das Kontrollkästchen aktiviert, startet Kaspersky Embedded Systems 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 Embedded Systems Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Automatische zufällige Verzögerung für Aufgabenstarts verwenden	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe 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.

Einstellung	Beschreibung
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.
Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren	Wenn dieses Kontrollkästchen aktiviert ist, erhält das Betriebssystem des Computers eine bestimmte Vorlaufzeit für seinen Start, bevor die Aufgabe ausgeführt wird. Standardmäßig beträgt die Vorlaufzeit 5 Minuten. Aktivieren Sie das Kontrollkästchen, wenn Sie die Aufgabe auf allen Computern ausführen möchten, auch auf ausgeschalteten Computern.
Geräte nach Abschluss der Aufgabe herunterfahren	Wenn dieses Kontrollkästchen aktiviert ist, wird der Computer nach Abschluss der Aufgabe heruntergefahren. Sie können diese Funktion beispielsweise aktivieren, um den Computer freitags nach Feierabend untersuchen zu lassen. Nach Abschluss der Aufgabe schaltet das Programm den Computer für das Wochenende aus.
Aufgabe unterbrechen, wenn deren Ausführung länger dauert als	Ausführungszeit der Aufgabe begrenzen. Kaspersky Embedded Systems Security bricht die Aufgabe nach Ablauf des festgelegten Zeitraums ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Embedded Systems Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.
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 Embedded Systems Security auf die Leistung Ihres Computers bei hoher Auslastung zu minimieren. Diese Funktion ist nur für Aufgaben vom Typ Untersuchung auf Befehl verfügbar.
Zeitplan deaktivieren ab	Wenn das Kontrollkästchen aktiviert ist, beendet Kaspersky Embedded Systems Security ab dem angegebenen Datum die Ausführung der geplanten Aufgabe. Die Aufgabe wird in den Modus **Manuell** versetzt. Diese Funktion ist nur für Aufgaben vom Typ Untersuchung auf Befehl verfügbar.

Berichte in Kaspersky Security Center

Die Berichte von Kaspersky Security Center enthalten Informationen zum Status der verwalteten Geräte. Die Berichte basieren auf Informationen, die auf dem Administrationsserver gespeichert sind.

Ab Kaspersky Security Center 11 sind folgende Berichtstypen für Kaspersky Embedded Systems Security verfügbar:

- Bericht über den Status der Programmkomponenten
- Bericht über verbotene Programme
- Bericht über verbotene Programme im Testmodus

Ausführliche Informationen zur Arbeit mit Berichten von Kaspersky Security Center finden Sie in der Hilfe zu Kaspersky Security Center.

Bericht über den Status der Programmkomponenten von Kaspersky Embedded Systems Security

Sie können den Schutzstatus aller Netzwerkgeräte überwachen und eine strukturierte Übersicht der Komponentenauswahl auf jedem Gerät anzeigen lassen.

Der Bericht zeigt für jede Komponente eine der folgenden Statusvarianten an: *Wird ausgeführt*, *Angehalten*, *Abgebrochen*, *Nicht durch Lizenz abgedeckt*.

Der Status *Nicht installiert* bezieht sich auf die Komponente, nicht auf das Programm selbst. Wenn das Programm nicht installiert ist, wird in Kaspersky Security Center der Status N/A (Nicht verfügbar) zugewiesen.

Sie können eine Komponentenauswahl erstellen und den Filter verwenden, um Netzwerkgeräte mit einer festgelegten Auswahl an Komponenten samt Status anzuzeigen.

Nähere Informationen zur Erstellung und Verwendung einer Auswahl finden Sie in der Hilfe zu Kaspersky Security Center.

Um den aktuellen Status der Komponenten in den Programmeinstellungen zu überprüfen, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Kaspersky Security Center Verwaltungskonsole den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.
3. Wählen Sie den Abschnitt **Komponenten**.
4. Eine Tabelle mit Statusvarianten wird Ihnen angezeigt.

Um einen Standardbericht für Kaspersky Security Center anzusehen, gehen Sie wie folgt vor:

1. Wählen Sie in der Programmkonsolenstruktur den Knoten **Administrationsserver <Name des Administrationsservers>**.
2. Wählen Sie die Registerkarte **Berichte** aus.
3. Doppelklicken Sie auf das Listenelement **Bericht über den Status der Programmkomponenten**.

   Ein Bericht wird erstellt.
4. Passen Sie die folgenden Einstellungen für Anfragen an:
   - ein Schaubild
   - eine Übersichtstabelle mit Komponenten und der Gesamtanzahl der Netzwerkgeräte, auf denen jede Komponente installiert ist, sowie die Gruppen, zu denen sie gehören
   - eine detaillierte Tabelle mit dem Status, der Version, dem Gerät und der Gruppe der Komponente

Berichte über verbotene Programme im Modus "Aktiv" und "Statistik"

Basierend auf den Ergebnissen der Aufgabe Kontrolle des Programmstarts können zwei Arten von Berichten erstellt werden: ein Bericht über verbotene Programme (wenn die Aufgabe im aktiven Modus gestartet wurde) und ein Bericht über verbotene Programme im Testmodus (wenn die Aufgabe im Informieren-Modus gestartet wurde). Diese Berichte enthalten Informationen über blockierte Programme auf den geschützten Geräten im Netzwerk. Jeder Bericht wird für alle Administrationsgruppen erstellt und sammelt die Daten aller Kaspersky-Programme, die auf den geschützten Geräten installiert sind.

So zeigen Sie einen Bericht über verbotene Programme im Informieren-Modus an:

1. Starten Sie die Aufgabe zur Kontrolle des Programmstarts im Informieren-Modus.
2. Wählen Sie in der Programmkonsolenstruktur den Knoten **Administrationsserver <Name des Administrationsservers>**.
3. Wählen Sie die Registerkarte **Berichte** aus.
4. Doppelklicken Sie auf das Element **Bericht über verbotene Programme im Testmodus**.

   Ein Bericht wird erstellt.
5. Passen Sie die folgenden Einstellungen für Anfragen an:

   - Ein Schaubild mit den Top-10-Programmen, deren Start am häufigsten blockiert wurde.
   - Eine Übersichtstabelle mit den Fällen, in denen ein Programm blockiert wurde, mit Angabe des Namens der ausführbaren Datei, der Ursache, der Uhrzeit der Blockierung und der Anzahl der Geräte, auf denen sie stattgefunden hat.
   - Eine ausführliche Tabelle mit Daten zum Gerät, dem Dateipfad und den Kriterien für das Blockieren.

Um einen Bericht über verbotene Programme im Modus "Aktiv" anzuzeigen, gehen Sie wie folgt vor:

1. Führen Sie die Aufgabe Kontrolle des Programmstarts im Aktiv-Modus aus.
2. Wählen Sie in der Programmkonsolenstruktur den Knoten **Administrationsserver <Name des Administrationsservers>**.
3. Wählen Sie die Registerkarte **Berichte** aus.
4. Doppelklicken Sie auf das Element **Bericht über verbotene Programme**.

   Ein Bericht wird erstellt.

Dieser Bericht enthält die gleichen Daten über Blockierungen wie der Bericht über verbotene Programme im Testmodus.

Echtzeit-Schutzstatus

Kaspersky Embedded Systems 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 Gerät ab (siehe Tabelle unten).

Kaspersky Embedded Systems Security ermittelt den Echtzeit-Schutzstatus anhand des Status der folgenden Programmkomponenten:

- Echtzeitschutz für Dateien
- Gerätekontrolle
- Firewall
- Schutz vor Netzwerkbedrohungen
- AMSI-Scanner
- Schutz vor BadUSB-Angriffen
- Rollback von schädlichen Aktionen
- Exploit-Prävention.

Sie können den Echtzeit-Schutzstatus des Programms in einer Konsole von Kaspersky Security Center überprüfen.

So ermitteln Sie den Echtzeit-Schutzstatus in der Kaspersky Security Center Verwaltungskonsole

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 Geräts.
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.

Wert	Beschreibung
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 Embedded Systems Security aus der Liste aktiviert sind und das Programm aktiviert ist.

Verwendung der Konsole für Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zur Konsole für Kaspersky Embedded Systems Security und zur Verwaltung des Programms über die Programmkonsole, die auf dem geschützten Gerät oder auf einem anderen Gerät installiert ist.

Anwendungskonsole starten

So starten Sie die Anwendungskonsole:

1. Öffnen Sie das kompakte Diagnosefenster auf eine der folgenden Arten:

   - Führen Sie im Installationsordner des Programms auf dem geschützten Gerät die Datei avpui.exe aus. Die Datei befindet sich standardmäßig im Ordner C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.

   - Klicken Sie auf das Programmsymbol im Infobereich der Taskleiste.

2. Klicken Sie im folgenden Fenster „Kompakte Diagnose-Benutzeroberfläche“ auf den Link **Konsole für Kaspersky Embedded Systems Security**.

   Wenn Sie bereits eine Verbindung zu dem geschützten Gerät konfiguriert haben, wird die Anwendungskonsole geöffnet.

   Wenn Sie die Anwendungskonsole erstmals starten, gelangen Sie zum Fenster **Geschütztes Gerät auswählen**. Dort müssen Sie die Verbindung der Anwendungskonsole mit dem geschützten Computer konfigurieren.

   Die Programmkonsole der Version 4.0 ist nicht mit Kaspersky Embedded Systems Security 4.1 und höher kompatibel. Wenn Sie versuchen, eine Verbindung herzustellen, werden Sie aufgefordert, das Kompatibilitätspaket für die Programmkonsole zu installieren. Das Kompatibilitätspaket wird von dem Gerät heruntergeladen, zu dem Sie eine Verbindung herstellen.

Benutzeroberfläche der Konsole für Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zu den wichtigsten Elementen der Programmoberfläche.

Fenster "Konsole für Kaspersky Embedded Systems Security"

Nachdem eine Verbindung zu Kaspersky Embedded Systems Security hergestellt wurde, das auf einem anderen geschützten Gerät installiert ist, wird der Name des Knotens um den Namen des geschützten Geräts, auf dem das Programm installiert ist, und den Namen des Benutzerkontos, unter dem die Verbindung hergestellt wurde, ergänzt: **Kaspersky Embedded Systems Security <Name des geschützten Geräts> als <Benutzerkonto-Name>**. Wenn eine Verbindung zu Kaspersky Embedded Systems Security, das auf demselben geschützten Gerät wie die Konsole für Kaspersky Embedded Systems Security installiert ist, hergestellt wird, lautet der Knotenname „Kaspersky Embedded Systems Security“.

Konsolenstruktur

Die Struktur der Programmkonsole enthält den Hauptknoten **Kaspersky Embedded Systems Security** und die untergeordneten Knoten für die funktionellen Programmkomponenten.

Der Knoten **Kaspersky Embedded Systems Security** enthält die folgenden untergeordneten Knoten:

- **Echtzeit-Computerschutz** ermöglicht die Konfiguration der folgenden Aufgaben:
  - **Echtzeitschutz für Dateien**
  - **Kaspersky Security Network**
  - **Exploit-Prävention**
  - **Schutz vor Netzwerkbedrohungen**
  - **Verhaltensanalyse**
  - **Rollback von schädlichen Aktionen**
  - **AMSI-Scanner**.
- **Computer-Kontrolle**: Kontrolle der Programme, die auf dem geschützten Gerät und den angeschlossenen Geräten ausgeführt werden.
  - **Kontrolle des Programmstarts**
  - **Gerätekontrolle**
  - **Firewall**.
- **Automatisches Erstellen von Regeln**: Konfigurieren der automatischen Erstellung von Gruppen- und Systemregeln für die Komponente Kontrolle des Programmstarts und die Komponente Gerätekontrolle.
  - **Erstellen von Regeln für die Kontrolle des Programmstarts**
  - **Erstellen von Regeln für die Gerätekontrolle**

- Gruppenaufgaben für die Erstellung von Regeln **<Namen der Aufgaben>** (sofern vorhanden).

  Gruppenaufgaben werden mithilfe von Kaspersky Security Center erstellt. Gruppenaufgaben können nicht über die Konsole für Kaspersky Embedded Systems Security verwaltet werden.

- **System-Inspektion**: Konfigurieren der Einstellungen der Überwachung der Systemintegrität und der Analyse des Windows-Ereignisprotokolls.

  - **Protokollanalyse**
  - **Überwachung der Systemintegrität**.

- **Untersuchung auf Befehl**: Verwalten der Aufgabe zur Virensuche. Jede Aufgabe hat ihr eigenes Steuerelement:

  - **Untersuchung wichtiger Bereiche**
  - **Kontrolle der Anwendungsintegrität**
  - **Untersuchung von Wechseldatenträgern**
  - **Vollständige Untersuchung**
  - Benutzerdefinierte Aufgaben **<Namen der Aufgaben>** (sofern vorhanden)

  Im Knoten werden Systemaufgaben, bei der Installation erstellte Programme, benutzerdefinierte Aufgaben sowie Gruppenaufgaben zur Untersuchung auf Befehl angezeigt, die mithilfe von Kaspersky Security Center erstellt und an das geschützte Gerät übertragen wurden.

- **Update**: Verwaltung der Updates für die Datenbanken und Programm-Module von Kaspersky Embedded Systems Security und Möglichkeit zum Rollback des letzten Updates:

  - **Update der Datenbanken und Programm-Module**
  - **Rollback des letzten Updates**
  - **Programm-Update**.

  Im Knoten werden alle benutzerdefinierten Aufgaben und Gruppenaufgaben zum Update angezeigt, die mithilfe von Kaspersky Security Center erstellt und an das geschützte Gerät übertragen wurden.

- **Speicher**: Verwaltung der Backup-Einstellungen und der Liste für blockierte Netzwerksitzungen.

  - **Backup**
  - **Blockierte Netzwerksitzungen**.

- **Protokolle und Meldungen**: Verwaltung der Protokolle der lokalen Aufgaben und des Auditprotokolls von Kaspersky Embedded Systems Security System.

  - **Systemaudit**
  - **Kontrolle des Programmstarts**
  - **Gerätekontrolle**

- **Kontrolle der Anwendungsintegrität**
- **Protokollanalyse**
- **Überwachung der Systemintegrität**
- **Schutz vor Netzwerkbedrohungen**
- **Untersuchung auf Befehl**
- **Firewall**
- **Exploit-Prävention**
- **Verhaltensanalyse**
- **AMSI-Scanner**
- **Update**
- **Echtzeitschutz für Dateien**
- **Backup**.

- **Lizenzverwaltung**: Schlüssel für Kaspersky Embedded Systems Security hinzufügen oder löschen, Lizenzdetails anzeigen.

Ergebnisfenster

Im Ergebnisfenster werden Informationen über den ausgewählten Knoten angezeigt. Wenn der Knoten **Kaspersky Embedded Systems Security** ausgewählt ist, werden im Detailbereich Informationen über den aktuellen Schutzstatus des Geräts und Informationen über Kaspersky Embedded Systems Security, den Schutzstatus der funktionellen Komponenten und den Schlüsselstatus angezeigt.

Kontextmenü des Knotens Kaspersky Embedded Systems Security

Mithilfe der Befehle im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** können Sie folgende Aktionen ausführen:

- **Schutz anhalten**.
- **Einstellungen der vertrauenswürdigen Zone konfigurieren**. Einstellungen der vertrauenswürdigen Zone aufrufen und anpassen.
- **Untersuchung von Wechseldatenträgern**. Die Untersuchung von Wechseldatenträgern anpassen, die über den USB-Anschluss an das geschützte Gerät angeschlossen werden.
- **Benutzerberechtigungen für den Zugriff auf die Programmverwaltung**. Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security aufrufen und anpassen.

- **Benutzerberechtigungen für den Zugriff auf die KESS Service-Verwaltung**. Benutzerrechte für die Verwaltung von Kaspersky Embedded Systems Security Service anzeigen und anpassen.
- **Speicher**
- **Einstellungen exportieren**. Programmeinstellungen in einer Konfigurationsdatei im XML-Format speichern. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Einstellungen importieren**. Programmeinstellungen aus Konfigurationsdatei im xml-Format importieren. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Aktualisieren**. Inhalt des Fensters der Konsole für Kaspersky Embedded Systems Security aktualisieren. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Eigenschaften des Programms**. Einstellungen von Kaspersky Embedded Systems Security oder einer ausgewählten Aufgabe anzeigen und anpassen. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.

  Dazu können Sie auch den Link **Eigenschaften des Programms** im Detailbereich des Knotens Kaspersky Embedded Systems Security verwenden.
- **Hilfe**. Informationen hierzu finden Sie in der Hilfe zu Kaspersky Embedded Systems Security. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.

Symbolleiste und Kontextmenü der Aufgaben von Kaspersky Embedded Systems Security

Sie können die Programmaufgaben über die Einträge des Kontextmenüs der einzelnen Aufgaben in der Struktur der Konsole für Kaspersky Embedded Systems Security verwalten.

Mithilfe der Punkte im Kontextmenü der ausgewählten Aufgabe können Sie folgende Aktionen ausführen:

- **Fortsetzen/Anhalten**. Ausführung der Aufgabe anhalten/fortsetzen. Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden. Diese Aktion ist nur für Aufgaben zum Echtzeitschutz und zur Untersuchung auf Befehl verfügbar.
- **Aufgabe erstellen**. Neue benutzerdefinierte Aufgabe erstellen.
- **Aufgabe löschen**. Benutzerdefinierte Aufgabe löschen.
- **Einstellungen exportieren** / **Einstellungen importieren**. Aufgabeneinstellungen exportieren oder importieren.
- **Eigenschaften**. Öffnen Sie das Fenster mit den Aufgabeneinstellungen.
- **Hilfe**. Öffnen Sie das entsprechende Thema der Online-Hilfe.

Taskleistensymbol im Infobereich

Sofort nach der Installation von Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security zeigt die Warnung und eine Beschreibung des Problems im Computerschutz an.

Sie können das Kontextmenü des Taskleistensymbols mit der rechten Maustaste öffnen.

Das Kontextmenü enthält mehrere Befehle zur Anzeige der Programmfenster (s. Tabelle unten).

Befehle im Kontextmenü des Taskleistensymbols

Befehl	Beschreibung
Anwendungskonsole öffnen	Öffnet die Konsole für Kaspersky Embedded Systems Security (falls installiert).
Kompaktes Diagnosefenster öffnen	Öffnet das kompakte Diagnosefenster.
Über das Programm	Öffnet das Fenster **Über das Programm** mit Informationen zu Kaspersky Embedded Systems Security. Wenn Sie als Benutzer von Kaspersky Embedded Systems Security registriert sind, enthält das Fenster **Über das Programm** Informationen über die installierten kritischen Updates.
Ausblenden	Blendet das Taskleistensymbol im Infobereich der Taskleiste aus.

Sie können das ausgeblendete Taskleistensymbol jederzeit wieder einblenden.

Um das Taskleistensymbol wieder einzublenden,

wählen Sie im **Startmenü** von Microsoft Windows den Punkt **Alle Programme** > **Kaspersky Embedded Systems Security** aus. Das Symbol wird im Infobereich der Microsoft Windows-Taskleiste angezeigt.

Die Bezeichnungen der Einstellungen können je nach installiertem Betriebssystem unterschiedlich sein.

Allgemeine Einstellungen konfigurieren (in der Anwendungskonsole)

Die allgemeinen Einstellungen und die Einstellungen für die Crash-Diagnose von Kaspersky Embedded Systems Security legen die allgemeinen Bedingungen für den Einsatz des Programms fest. Diese Einstellungen ermöglichen Folgendes: Regelung der Anzahl der aktiven Prozesse, die von Kaspersky Embedded Systems Security verwendet werden; Wiederherstellung der Aufgaben von Kaspersky Embedded Systems Security nach deren Absturz aktivieren; Führen eines Protokolls; Anlegen von Dump-Dateien für Prozesse von Kaspersky Embedded Systems Security bei deren Absturz; andere allgemeine Einstellungen.

Die Programmeinstellungen können nicht in der Konsole für Kaspersky Embedded Systems Security konfiguriert werden, wenn die aktive Richtlinie von Kaspersky Security Center das Ändern dieser Einstellungen blockiert.

So konfigurieren Sie die allgemeinen Einstellungen von Kaspersky Embedded Systems Security:

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Eigenschaften des Programms**.
   - Wählen Sie im Kontextmenü des Knotens den Punkt **Eigenschaften des Programms** aus.

   Das Fenster **Eigenschaften des Programms** wird geöffnet.

2. Geben Sie auf der Registerkarte **Benutzeroberfläche** an, welche Warnungen über dem Taskleistensymbol von Kaspersky Embedded Systems Security angezeigt werden sollen.

3. Konfigurieren Sie auf der Registerkarte **Sicherheitseinstellungen** die folgenden Einstellungen:

   - Konfigurieren Sie im Abschnitt **Allgemein** die Option **Programm beim Hochfahren des Computers starten (empfohlen)**.
   - Konfigurieren Sie unter **Selbstschutz** den Schutz für Programm-Module und für Betriebssystemdienste.
   - Legen Sie im Abschnitt **Aktionen beim Wechsel auf USV-Stromversorgung** die von Kaspersky Embedded Systems Security beim Wechsel auf eine USV-Quelle erzeugte Belastungsbeschränkung auf den geschützten Geräten fest:
     - **Geplante Untersuchungsaufgaben nicht starten**
     - **Laufende Untersuchungsaufgaben abbrechen**
   - Konfigurieren Sie im Abschnitt **Kompatibilitätseinstellungen** die Einstellung **Kompatibilität mit Fernverwaltungsanwendungen**.
   - Konfigurieren Sie im Abschnitt **Untersuchungseinstellungen** das Limit der CPU-Auslastung für Untersuchungsaufgaben und erlauben Sie die Freigabe von Ressourcen für andere Programme.

4. Konfigurieren Sie auf der Registerkarte **Netzwerkeinstellungen** die folgenden Einstellungen:

   - Geben Sie im Abschnitt **Proxyserver** die Proxyserver-Einstellungen an: den Authentifizierungstyp und die notwendigen Daten für die Authentifizierung auf dem Proxyserver.
   - Geben Sie unter **Überwachte Ports** die Option für die Überwachung von Netzwerkports an:
     - **Alle Netzwerkports überwachen**. In diesem Modus zur Überwachung von Netzwerkports überwachen die Schutzkomponenten die Datenströme, die über beliebige offene Netzwerkports des Computers übertragen werden.
     - **Nur ausgewählte Netzwerkports überwachen**. In diesem Überwachungsmodus für Netzwerkports kontrollieren die Schutzkomponenten die ausgewählten Ports des Computers und die Netzwerkaktivität der ausgewählten Programme. Eine Liste der Netzwerkports, über die E-Mail-Nachrichten und Netzwerkverkehr gewöhnlich übertragen werden, ist gemäß der Empfehlungen der Kaspersky-Experten vorgegeben. Bei Bedarf können Sie die Liste der Netzwerkports bearbeiten.
   - Unter **Port für Remote-Verbindung** können Sie bei Bedarf den Port ändern, den die Programmkonsole für die Verbindung mit dem Computer verwendet, auf dem das Programm installiert ist.

     Die Standardportnummer für die Verbindung mit Windows-Anmeldedaten ist 13032, und die Standardportnummer für die Verbindung mit Anmeldedaten manuell erstellter Benutzer ist 13031. Bereich der möglichen Portnummern: 1 bis 65535.

     Die zuvor gespeicherten Portnummern werden verwendet, bis das Programm neu gestartet wird.

5. Klicken Sie auf der Registerkarte **Diagnose von Störungen** auf **Einstellungen** und konfigurieren Sie das Ablaufverfolgung und die Aufzeichnung von Speicherabbildern für das Programm.
6. Klicken Sie auf **OK**.

Die Einstellungen von Kaspersky Embedded Systems Security werden gespeichert.

Aufgaben von Kaspersky Embedded Systems Security verwalten

Dieser Abschnitt enthält Informationen zum Erstellen, Konfigurieren, Starten und Beenden der Aufgaben von Kaspersky Embedded Systems Security.

Aufgabenkategorien von Kaspersky Embedded Systems Security

Echtzeit-Computerschutz, Computer-Kontrolle, Automatisches Erstellen von Regeln, System-Inspektion, Untersuchung auf Befehl, Schutz für industrielle Netzwerke, Speicherverwaltung und Update sind in Kaspersky Embedded Systems Security als Aufgaben implementiert.

Aufgaben lassen sich über das Kontextmenü der jeweiligen Aufgabe in der Struktur der Konsole für Kaspersky Embedded Systems Security und im Ergebnisbereich verwalten. Informationen über den Aufgabenstatus werden im Ergebnisfenster angezeigt. Operationen, die sich auf die Verwaltung von Aufgaben beziehen, werden im Systemaudit-Protokoll protokolliert.

Es gibt zwei Typen von Aufgaben in Kaspersky Embedded Systems Security: *lokal* und *Gruppe*.

Lokale Aufgaben

Lokale Aufgaben können nur auf dem geschützten Gerät ausgeführt werden, für das sie erstellt wurden. Je nach Startmethode existieren folgende Typen lokaler Aufgaben:

- **Lokale Systemaufgaben**. Diese Aufgaben werden während der Installation von Kaspersky Embedded Systems Security automatisch erstellt. Sie können die Einstellungen aller lokalen Systemaufgaben ändern, unter Ausnahme der Aufgabe *Update-Rollback*. Sie können die lokalen Systemaufgaben nicht umbenennen oder löschen. Lokale Systemaufgaben und benutzerdefinierte Aufgaben zur Untersuchung auf Befehl können gleichzeitig gestartet werden.
- **Lokale benutzerdefinierte Aufgaben**. In der Anwendungskonsole können Sie Aufgaben zur Untersuchung auf Befehl, Update-Aufgaben und Aufgaben zur Baseline-Überwachung der Systemintegrität erstellen. In Kaspersky Security Center können Sie Aufgaben zur Untersuchung auf Befehl, Update-Aufgaben und andere Aufgaben erstellen. Sie können benutzerdefinierte Aufgaben umbenennen, konfigurieren oder löschen. Es können gleichzeitig mehrere benutzerdefinierte Aufgaben gestartet werden.

Gruppenaufgaben

Gruppenaufgaben und Aufgaben für Zusammenstellungen von geschützten Geräten können über Kaspersky Security Center verwaltet werden. Alle Gruppenaufgaben sind benutzerdefinierte Aufgaben. Gruppenaufgaben werden ebenso in der Programmkonsole angezeigt. In der Programmkonsole können Sie nur den Status von Gruppenaufgaben sehen. Sie können die Programmkonsole nicht zum Verwalten oder Konfigurieren von Gruppenaufgaben verwenden.

Manuelles Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe

Sie können Aufgaben manuell starten, anhalten, fortsetzen oder beenden. Diese Optionen sind nicht für alle Aufgaben von Kaspersky Embedded Systems Security verfügbar.

So können Sie eine Aufgabe starten, anhalten, fortsetzen oder beenden:

1. Öffnen Sie in der Programmkonsole das Kontextmenü der Aufgabe.
2. Wählen Sie einen der folgenden Befehle aus: **Start** oder **Anhalten**.

Die Operation wird ausgeführt und im Systemaudit-Protokoll erfasst.

Aufgaben planen

In der Konsole für Kaspersky Embedded Systems Security können Sie einen Zeitplan für die Ausführung lokaler System- und Benutzeraufgaben konfigurieren. Sie können jedoch keinen Zeitplan für die Ausführung von Gruppenaufgaben konfigurieren.

So planen Sie eine Aufgabe:

1. Wählen Sie in der Konsolenstruktur die Aufgabe aus, für die Sie den Zeitplan erstellen möchten.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.
3. Führen Sie im angezeigten Fenster im Abschnitt **Startmodus** eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Manuell**, um die Aufgabe zu einem für Sie passenden Zeitpunkt manuell auszuführen.
   - Aktivieren Sie das Kontrollkästchen **Nach Zeitplan**, wenn Sie den Aufgabenstart nach Zeitplan aktivieren möchten
4. Wenn Sie die Option **Nach Zeitplan** auswählen, konfigurieren Sie die Einstellungen für den Aufgabenzeitplan (siehe Tabelle unten).
5. Aktivieren Sie bei Bedarf das Kontrollkästchen **Aufgabe starten als** und geben Sie die Anmeldedaten des Benutzerkontos an, unter dem die Aufgabe ausgeführt werden soll.
6. Klicken Sie auf **OK**.

Die Zeitplan-Einstellungen werden gespeichert.

Einstellungen für den Aufgabenzeitplan

Einstellung	Beschreibung
Startmodus	Wählen Sie den Funktionsmodus der Aufgabe aus: • **Minuten**. Die Aufgabe wird in regelmäßigen Abständen alle paar Minuten ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Minuten) an. • **Stunden**. Die Aufgabe wird in regelmäßigen Abständen alle paar Stunden ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Stunden) an. • **Tage**. Die Aufgabe wird in regelmäßigen Abständen alle paar Tage ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Tagen) an. • **Wochen**. Die Aufgabe wird an den angegebenen Wochentagen in Intervallen von einer bestimmten Anzahl von Wochen ausgeführt. Legen Sie den Zeitplan fest, wählen Sie mithilfe der Kontrollkästchen die Wochentage aus, an denen die Aufgabe ausgeführt werden soll, und geben Sie die Startzeit für die Aufgabe an. • **Jeden Monat**. Die Aufgabe wird an einem bestimmten Tag des Monats ausgeführt. Geben Sie Datum und Uhrzeit des Starts an. • **Zum festgelegten Zeitpunkt**. Die Aufgabe wird einmal zum angegebenen Zeitpunkt (Datum und Uhrzeit) ausgeführt. • **Nach jedem Update**. Die Aufgabe wird jedes Mal ausgeführt, wenn Updates in die Datenverwaltung heruntergeladen werden. • **Nach dem Programmstart**. Die Aufgabe wird jedes Mal beim Start von Kaspersky Embedded Systems Security ausgeführt.
Übersprungene Aufgaben starten	Ist das Kontrollkästchen aktiviert, startet Kaspersky Embedded Systems 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 Embedded Systems Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Automatische zufällige Verzögerung für Aufgabenstarts verwenden	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe nicht streng nach Zeitplan ausgeführt, sondern zufällig in einem bestimmten Intervall, d. h. die Aufgabenstarts werden zeitlich verteilt. Zufällige Startzeiten verhindern, dass viele Computer gleichzeitig auf den Administrationsserver zugreifen, wenn die Aufgabe nach Zeitplan ausgeführt wird. Der Bereich der zufälligen Startzeiten wird beim Erstellen der Aufgabe automatisch berechnet. Dabei wird die Anzahl der Computer berücksichtigt, denen die Aufgabe zugewiesen ist. Anschließend wird die Aufgabe immer zur berechneten Startzeit ausgeführt. Die berechnete Startzeit ändert sich aber, wenn die Aufgabeneinstellungen geändert werden oder die Aufgabe manuell ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe exakt zum geplanten Zeitpunkt ausgeführt.

Einstellung	Beschreibung
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	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 Embedded Systems Security auf die Leistung Ihres Computers bei hoher Auslastung zu minimieren. Diese Funktion ist nur für Aufgaben vom Typ Untersuchung auf Befehl verfügbar.
Zeitplan deaktivieren ab	Wenn das Kontrollkästchen aktiviert ist, beendet Kaspersky Embedded Systems Security ab dem angegebenen Datum die Ausführung der geplanten Aufgabe. Die Aufgabe wird in den Modus **Manuell** versetzt. Diese Funktion ist nur für Aufgaben vom Typ Untersuchung auf Befehl verfügbar.

Verwendung von Benutzerkonten für den Aufgabenstart

Sie können Aufgaben starten, indem Sie das Systemkonto verwenden oder ein anderes Benutzerkonto angeben.

Über die Verwendung eines Benutzerkontos für den Aufgabenstart

Sie können das Konto angeben, um die folgenden Aufgaben von Kaspersky Embedded Systems Security auszuführen:

- *Erstellen von Regeln für die Kontrolle des Programmstarts*
- *Erstellen von Regeln für die Gerätekontrolle*
- *Protokollanalyse*
- *Kontrolle der Anwendungsintegrität*
- *Update*.

Die angegebenen Aufgaben werden standardmäßig mit den Rechten des Systemkontos ausgeführt.

In folgenden Fällen sollten Sie ein anderes Benutzerkonto mit ausreichenden Zugriffsrechten angeben:

- Für die Aufgabe *Update*:
  - Wenn Sie als Update-Quelle einen freigegebenen Ordner auf einem anderen Netzwerkgerät angegeben haben.
  - Wenn Sie für den Zugriff auf die Update-Quelle einen Proxyserver mit NTLM- oder Kerberos-Authentifizierung verwenden.
- Für die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts*: Wenn die generierten Regeln in eine Konfigurationsdatei exportiert werden, auf die das Systemkonto keinen Zugriff hat (z. B. in einem freigegebenen Ordner auf dem geschützten Gerät).

Sie können die aufgelisteten Aufgaben mit Systemkontoberechtigungen starten. Kaspersky Embedded Systems Security führt diese Aufgaben aus und greift auf die freigegebenen Ordner auf einem anderen Netzwerk-Gerät zu, wenn dieses Gerät in derselben Domäne wie das geschützte Gerät registriert ist. In diesem Fall muss das Systemkonto über die Zugriffsrechte für diese Ordner verfügen. Kaspersky Embedded Systems Security greift dann mit den Rechten des Kontos **<Domänenname \ Gerätename>** auf das Gerät zu.

Benutzerkonto für den Aufgabenstart festlegen

Die Option zur Angabe eines Benutzerkontos in der Anwendungskonsole ist nicht für alle Aufgaben verfügbar.

So legen Sie ein Konto für den Aufgabenstart fest:

1. Wählen Sie in der Struktur der Anwendungskonsole die Aufgabe aus, die Sie mit den Rechten eines bestimmten Benutzerkontos starten möchten.
2. Klicken Sie im Ergebnisbereich auf den Link **Startmodus**.

   Das Fenster **Zeitplan und Startmodus** wird geöffnet.
3. Führen Sie im angezeigten Fenster im Abschnitt **Benutzer** die folgenden Aktionen aus:
   a. Wählen Sie die Option **Aufgabe starten als** aus.
   b. Geben Sie den Namen und das Kennwort des Benutzers an, dessen Benutzerkonto Sie verwenden möchten.

   Der ausgewählte Benutzer muss auf dem geschützten Gerät oder in der gleichen Domäne wie dieser Computer registriert sein.
4. Klicken Sie auf **OK**.

Die Änderung der Einstellungen wird gespeichert.

Import und Export von Einstellungen

In diesem Abschnitt wird erläutert, wie Sie die Einstellungen von Kaspersky Embedded Systems Security exportieren. Außerdem erfahren Sie, wie Sie die Einstellungen für bestimmte Programmkomponenten in eine xml-Konfigurationsdatei exportieren und diese Einstellungen aus einer Konfigurationsdatei zurück in das Programm importieren.

Über den Import und Export von Einstellungen

Sie können die Einstellungen von Kaspersky Embedded Systems Security in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Embedded Systems Security importieren. In einer Konfigurationsdatei können entweder alle Einstellungen des Programms oder nur die Einstellungen bestimmter Programmkomponenten gespeichert werden.

Wenn Sie alle Einstellungen von Kaspersky Embedded Systems Security exportieren, dann werden die allgemeinen Programmeinstellungen und die Einstellungen der folgenden Komponenten und Funktionen von Kaspersky Embedded Systems Security in eine Datei geschrieben:

- Echtzeitschutz für Dateien
- Exploit-Prävention
- Schutz vor Netzwerkbedrohungen
- Verhaltensanalyse
- Rollback von schädlichen Aktionen
- AMSI-Untersuchung
- Kontrolle des Programmstarts
- Gerätekontrolle
- Firewall
- Erstellen von Regeln für die Kontrolle des Programmstarts
- Erstellen von Regeln für die Gerätekontrolle
- Protokollanalyse
- Überwachung der Systemintegrität
- Untersuchung wichtiger Bereiche
- Kontrolle der Anwendungsintegrität
- Untersuchung von Wechseldatenträgern
- Vollständige Untersuchung

- Update der Datenbanken und Programm-Module
- Rollback des letzten Updates
- Update

Ferner können Sie die allgemeinen Einstellungen von Kaspersky Embedded Systems Security und die Berechtigungen des Benutzerkontos in der Datei speichern.

Wenn zum Zeitpunkt des Exports von Einstellungen eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert das Programm die aus der Richtlinie übernommenen Werte.

Die Einstellungen von Gruppenaufgaben können nicht exportiert werden.

Kaspersky Embedded Systems Security exportiert alle Kennwörter, die vom Programm verwendet werden, beispielsweise die Anmeldeeinstellungen von Konten für den Start von Aufgaben oder für die Verbindungsaufnahme mit Proxyservern. Exportierte Kennwörter werden in der Konfigurationsdatei verschlüsselt gespeichert. Sie können Kennwörter mithilfe von Kaspersky Embedded Systems Security nur dann importieren, wenn dieses Programm auf demselben geschützten Gerät installiert ist und weder neu installiert noch aktualisiert wurde.

Sie können keine gespeicherten Kennwörter mithilfe von Kaspersky Embedded Systems Security importieren, wenn das Programm auf einem anderen geschützten Gerät installiert ist. Nachdem die Einstellungen auf das geschützte Gerät importiert wurden, müssen alle Kennwörter manuell eingegeben werden.

Wenn die Funktionalität **Kennwort zur Bestätigung kritischer Aktionen abfragen** beim Exportieren der Einstellungen aktiviert war, wird das auf dem Gerät festgelegte Kennwort exportiert und beim Import der Einstellungen automatisch auf dem anderen Gerät angewendet.

Die Einstellungen können aus einer Konfigurationsdatei importiert werden, die Einstellungen für einzelne Komponenten von Kaspersky Embedded Systems Security enthält (z. B. aus einer Datei, die in Kaspersky Embedded Systems Security erstellt wurde, das mit einem unvollständigen Satz von Komponenten installiert wurde). Nach dem Import der Einstellungen werden in Kaspersky Embedded Systems Security nur jene Einstellungen geändert, die in der Konfigurationsdatei vorhanden waren. Alle anderen Einstellungen bleiben unverändert.

Gesperrte Einstellungen der aktiven Richtlinie von Kaspersky Security Center werden beim Import von Einstellungen nicht verändert.

Einstellungen exportieren

So exportieren Sie Einstellungen in eine Konfigurationsdatei:

1. Um alle Einstellungen von Kaspersky Embedded Systems Security zu exportieren, wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** den Befehl **Einstellungen exportieren** aus.

   Um die Einstellungen einer einzelnen Komponente zu exportieren, klicken Sie im Ergebnisbereich auf **Einstellungen exportieren**.

   Die Einstellungen von Kaspersky Security Network können nicht exportiert werden. Kaspersky Security Network muss manuell konfiguriert werden.

2. Geben Sie im folgenden Fenster den Namen der xml-Datei an, in die Sie die Liste der Einstellungen exportieren möchten, und wählen Sie einen Ordner aus, in dem diese Datei gespeichert werden soll.

   Sie können Umgebungsvariablen des Systems verwenden, wenn Sie den Pfad angeben, jedoch keine benutzerdefinierten Umgebungsvariablen.

   > Wenn zum Zeitpunkt des Exports von Einstellungen eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert Kaspersky Embedded Systems Security die Einstellungen aus der Richtlinie.

3. Speichern Sie die Datei.

4. Klicken Sie im Fenster **Einstellungen wurden erfolgreich exportiert** auf **OK**.

   Kaspersky Embedded Systems Security exportiert die Liste der Einstellungen in die xml-Datei.

Um die Liste der vertrauenswürdigen Apps zu exportieren:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.

2. Wählen Sie den Punkt **Einstellungen der vertrauenswürdigen Zone konfigurieren**.

3. Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

4. Gehen Sie zum Abschnitt **Vertrauenswürdige Programme** und klicken Sie auf **Einstellungen**.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.

5. Wählen Sie die vertrauenswürdigen Apps aus, die Sie exportieren möchten.

   Wenn Sie keine vertrauenswürdige App auswählen, exportiert Kaspersky Embedded Systems Security alle vertrauenswürdigen Apps.

6. Klicken Sie auf den Pfeil und wählen Sie in der Dropdown-Liste den Punkt **Exportieren** aus.

7. 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.

8. Speichern Sie die Datei.

   Kaspersky Embedded Systems Security exportiert die Liste der vertrauenswürdigen Apps in die XLM-Datei.

Sie können auch die Einstellungen von Kaspersky Embedded Systems Security über die Befehlszeile exportieren.

Einstellungen importieren

So importieren Sie Einstellungen aus einer gespeicherten Konfigurationsdatei:

1. Um alle Einstellungen von Kaspersky Embedded Systems Security zu importieren, wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** den Befehl **Einstellungen importieren** aus.

   Um die Einstellungen einer einzelnen Komponente zu importieren, klicken Sie im Ergebnisbereich auf **Einstellungen importieren**.

Nachdem Sie allgemeine Einstellungen für Kaspersky Embedded Systems Security oder dessen funktionale Komponenten auf dem geschützten Gerät importiert haben, können Sie die vorherigen Einstellungen nicht wiederherstellen.

Die Einstellungen von Kaspersky Security Network können nicht importiert werden. Kaspersky Security Network muss manuell konfiguriert werden.

2. Wählen Sie im folgenden Fenster die xml-Konfigurationsdatei aus, aus der Sie die Einstellungen importieren möchten, und klicken Sie auf **Öffnen**.
3. Klicken Sie im Fenster **Einstellungen wurden erfolgreich importiert** auf **OK**.
4. Klicken Sie in der Symbolleiste der Programmkonsole auf die Schaltfläche **Update**.

Das Fenster der Programmkonsole zeigt die importierten Einstellungen an.

Kaspersky Embedded Systems Security importiert keine Kennwörter (Konto-Anmeldedaten für den Aufgabenstart oder für die Proxyserver-Verbindung) aus einer Datei, die auf einem anderen geschützten Gerät angelegt oder auf dem gleichen geschützten Gerät gespeichert wurde, nachdem Kaspersky Embedded Systems Security auf diesem neu installiert oder aktualisiert wurde. Die Kennwörter müssen nach dem Abschluss des Imports manuell eingegeben werden.

Um die Liste mit vertrauenswürdigen Apps zu importieren:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.
2. Wählen Sie den Punkt **Einstellungen der vertrauenswürdigen Zone konfigurieren**.
3. Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.
4. Gehen Sie zum Abschnitt **Vertrauenswürdige Programme** und klicken Sie auf **Einstellungen**.
5. Klicken Sie auf den Pfeil und wählen Sie in der Dropdown-Liste den Punkt **Importieren** aus.
6. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdiges Apps importieren möchten.
7. Öffnen Sie die Datei.

   Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Apps gibt, fragt Kaspersky Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.
8. Die Liste wird auf der Registerkarte **Vertrauenswürdige Programme** angezeigt. Klicken Sie auf **OK**.

Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen

Um Informationen über den Geräteschutzstatus von Kaspersky Embedded Systems Security anzuzeigen,

wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Knoten **Kaspersky Embedded Systems Security** aus.

Die Informationen im Ergebnisbereich der Konsole für Kaspersky Embedded Systems Security werden standardmäßig automatisch aktualisiert:

- alle 10 Sekunden bei lokaler Verbindung
- alle 15 Sekunden bei Remote-Verbindung

Sie können die Informationen manuell aktualisieren.

*Und die Informationen im Knoten **Kaspersky Embedded Systems Security** manuell zu aktualisieren,*

wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** den Befehl **Aktualisieren** aus.

Im Ergebnisbereich der Konsole für Kaspersky Embedded Systems Security werden die folgenden Programminformationen angezeigt:

- Status der Verwendung von Kaspersky Security Network.
- Schutzstatus des geschützten Geräts.
- Daten über das Datenbanken-Update und das Update der Programm-Module.
- Aktuelle Diagnoseinformationen.
- Daten zu den Steuerungsaufgaben des geschützten Geräts.
- Lizenzinformationen.
- Status der Integration in Kaspersky Security Center: Details des Servers, auf dem Kaspersky Security Center installiert und mit dem das Programm verknüpft ist; Daten über die Kontrolle der Programmaufgaben durch die aktive Richtlinie.

Der Schutzstatus wird durch eine Farbcodierung angezeigt:

- *Grün*. Aufgabe wird gemäß den vorgenommenen Einstellungen ausgeführt. Der Schutz ist aktiv.
- *Gelb*. Aufgabe ist angehalten, beendet oder nicht gestartet. Es besteht ein potentielles Sicherheitsrisiko. Die Aufgabe sollte konfiguriert und gestartet werden.
- *Rot*. Aufgabe ist fehlgeschlagen oder bei der Aufgabenausführung wurde eine Sicherheitsbedrohung erkannt. Es empfiehlt sich, die Aufgabe zu starten oder Maßnahmen zur Beseitigung der erkannten Sicherheitsbedrohung zu ergreifen.

Ein Teil der Informationen in diesem Block (beispielsweise Aufgabennamen oder Anzahl erkannter Bedrohungen) wird in Form von Links dargestellt, über die Sie zum Knoten der entsprechenden Aufgabe wechseln oder das Protokoll der Aufgabenausführung öffnen können.

Der Abschnitt **KSN-Nutzung** enthält den aktuellen Aufgabenstatus, z. B. *Wird ausgeführt*, *Abgebrochen* oder *Noch nicht ausgeführt*. Der Indikator kann folgende Werte annehmen:

- Wenn die Leiste grün ist, wird die Aufgabe **KSN-Nutzung** ausgeführt und Anfragen zum Status von Dateien werden an KSN gesendet.
- Wenn die Leiste gelb ist, wurde eine der Erklärungen akzeptiert, die Aufgabe wird aber nicht ausgeführt, oder die Aufgabe wird ausgeführt, aber es werden keine Dateianfragen an KSN gesendet.
- Wenn die Leiste rot ist, ist die Aufgabe fehlgeschlagen.

Computerschutz

Der Abschnitt **Computerschutz** (siehe Tabelle unten) enthält Informationen über den aktuellen Schutzstatus des Geräts.

Informationen über den Schutzstatus des Geräts

Abschnitt	Informationen
Statusanzeige für den Geräteschutz	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der in diesem Abschnitt ausgeführten Aufgaben. Der Indikator kann folgende Werte annehmen: • Grüne Leiste – Wird standardmäßig angezeigt und bedeutet, dass die Komponente Echtzeitschutz für Dateien installiert ist und die Aufgabe ausgeführt wird. • Gelbe Leiste – Die Komponente Echtzeitschutz für Dateien ist nicht installiert und die Aufgabe *Untersuchung wichtiger Bereiche* wurde lange nicht ausgeführt. • Rote Leiste – Die Aufgaben für den Echtzeitschutz für Dateien werden nicht ausgeführt.
Echtzeitschutz für Dateien	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*.
Untersuchung wichtiger Bereiche	**Datum der letzten Untersuchung** – Datum und Uhrzeit der letzten Untersuchung wichtiger Bereiche des Computers auf Viren und andere Bedrohungen der Computersicherheit. *Noch nicht ausgeführt* – Ereignis, das auftritt, wenn die Aufgabe zur *Untersuchung wichtiger Bereiche* seit mindestens 30 Tagen nicht mehr ausgeführt wurde (Standard). Sie können den Grenzwert für die Auslösung dieses Ereignisses ändern.
Schutz vor Netzwerkbedrohungen	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*.

Abschnitt	Informationen
Exploit-Prävention	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*. **Funktionsmodus** – einer der zwei verfügbaren Modi für die Komponente: Exploit-Prävention: **Blockieren** oder **Informieren**.
Verhaltensanalyse	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*. **Funktionsmodus** – einer der drei verfügbaren Modi der Aufgabe „Verhaltensanalyse“: **Löschen**, **Blockieren** oder **Informieren**.

Update

Der Abschnitt **Update** (siehe Tabelle unten) zeigt Informationen über die Aktualität der Datenbanken und Anwendungsmodule an.

Informationen über den Zustand der Datenbanken und Module von Kaspersky Embedded Systems Security

Abschnitt	Informationen
Statusindikator für Datenbanken und Programm-Module	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der Datenbanken und Programm-Module. Der Indikator kann folgende Werte annehmen: • Grüne Leiste – Wird standardmäßig angezeigt und bedeutet, dass die Programm-Datenbanken aktuell sind und dass das letzte Update der Programm-Datenbanken erfolgreich abgeschlossen wurde. • Gelbe Leiste – Bedeutet, dass die Datenbanken veraltet sind oder die letzte Aufgabe zum Update der Datenbanken und Module fehlgeschlagen ist. • Rote Leiste – Das Ereignis *Datenbanken sind stark veraltet* oder *Datenbanken sind aktuell* ist eingetreten.
Status der Datenbanken	Diese Option kann folgende Werte annehmen: • **Datenbanken sind aktuell** – die Programm-Datenbanken wurden vor höchstens 7 Tagen aktualisiert (Standard). • **Datenbanken sind veraltet** – die Programm-Datenbanken wurden zuletzt vor 7–14 Tagen aktualisiert (Standard). • **Datenbanken sind stark veraltet** – die Programm-Datenbanken wurden zuletzt vor mehr als 14 Tagen aktualisiert (Standard). Sie können die Grenzwerte für die Auslösung der Ereignisse *Datenbanken sind veraltet* und *Datenbanken sind stark veraltet* ändern.
Datenbanken vom	Datum und Uhrzeit der Veröffentlichung des letzten Updates für die Programm-Datenbanken. Datum und Uhrzeit werden in UTC angegeben.
Status der letzten abgeschlossenen Aufgabe zum Datenbanken-Update	Datum und Uhrzeit des letzten Datenbanken-Updates. Datum und Uhrzeit werden in der lokalen Zeit des geschützten Geräts angegeben. Der Wert in diesem Feld ist rot, wenn das Ereignis *Fehlerhaft* eintritt.

Kontrolle

Im Abschnitt **Kontrolle** (s. Tabelle unten) werden Informationen über den Status der Aufgaben „Kontrolle des Programmstarts“ und „Gerätekontrolle“ angezeigt.

Informationen über den Status der Gerätekontrolle

Abschnitt	Informationen
Statusindikator der Kontrolle geschützter Geräte	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der in diesem Abschnitt ausgeführten Aufgaben. Der Indikator kann folgende Werte annehmen: • Grüne Leiste: Wird standardmäßig angezeigt und bedeutet, dass die Komponente Kontrolle des Programmstarts installiert ist und die Aufgabe im Aktiv-Modus ausgeführt wird. Die Komponente Exploit-Prävention ist installiert und aktiv. • Die Leiste ist gelb, wenn eine oder mehrere der folgenden Bedingungen erfüllt sind: Exploit-Prävention wird nicht ausgeführt; die Aufgabe Kontrolle des Programmstarts wird im Informieren-Modus ausgeführt; Exploit-Prävention wird im Aktiv-Modus ausgeführt, und die Aufgabe Kontrolle des Programmstarts wird nicht ausgeführt oder ist fehlgeschlagen. • Rote Leiste: Die Aufgabe Kontrolle des Programmstarts wird nicht ausgeführt oder ist fehlgeschlagen, und die Exploit-Prävention wird nicht ausgeführt oder läuft im **Informieren**-Modus.
Kontrolle des Programmstarts	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*. **Funktionsmodus** – einer der zwei verfügbaren Modi der Aufgabe „Kontrolle des Programmstarts“: **Regeln anwenden** oder **Regeln testen**.
Gerätekontrolle	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*. **Funktionsmodus** – einer der zwei verfügbaren Modi der Aufgabe „Gerätekontrolle“: **Nach Regeln** oder **Informieren**.
Firewall	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*.

Diagnose

Der Abschnitt **Diagnose** (siehe folgende Tabelle) enthält Informationen über die Aufgaben Überwachung der Systemintegrität und Protokollanalyse.

Informationen über den Status der System-Diagnose

Abschnitt	Informationen
Statusindikator der Diagnose	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der in diesem Abschnitt ausgeführten Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Wird standardmäßig angezeigt und bedeutet, dass eine oder beide Komponenten der System-Inspektion installiert sind und dass Aufgaben ausgeführt werden. • Gelb: Beide Komponenten sind installiert, aber eine der System-Inspektionsaufgaben wird nicht ausgeführt. Das Ereignis *Wird nicht ausgeführt* ist eingetreten. • Rot – eine der Aufgaben ist fehlgeschlagen.
Überwachung der Systemintegrität	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*.
Protokollanalyse	**Status** – aktueller Status der Komponente, z. B. *Wird ausgeführt* oder *Deaktiviert*.

Informationen zur Lizenzverwaltung von Kaspersky Embedded Systems Security werden in der Zeile in der linken unteren Ecke des Detailbereichs des Knotens **Kaspersky Embedded Systems Security** angezeigt.

Sie können die Einstellungen von Kaspersky Embedded Systems Security anpassen, indem Sie auf den Link Eigenschaften des Programms klicken.

Sie können eine Verbindung zu einem anderem geschützten Gerät herstellen, indem Sie auf den Link Mit einem Remote-Computer verbinden klicken.

So konfigurieren Sie die Backup-Einstellungen (in der Anwendungskonsole)

So konfigurieren Sie die allgemeinen Backup-Einstellungen:

1. Öffnen Sie in der Struktur der Anwendungskonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security** und wählen Sie den Punkt **Speicher** aus.

2. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Speichereinstellungen

Einstellung	Beschreibung
Nehmen Sie auf der Registerkarte **Berichte** die folgenden Berichtseinstellungen vor:	
Berichte speichern für maximal	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 Embedded Systems Security automatisch die ältesten Einträge aus der Berichtsdatei.
Maximale Größe der Berichtsdatei	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 Embedded Systems Security automatisch die ältesten Einträge aus der Berichtsdatei. Dadurch ist gewährleistet, dass die maximale Berichtsdateigröße nicht überschritten wird.
Nehmen Sie auf der Registerkarte **Backup** die folgenden Backup-Einstellungen vor:	
Objekte speichern für maximal	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 Embedded Systems Security die ältesten Dateien aus dem Backup.
Maximale Größe des Backups	Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 400 MB. Nach Erreichen der maximalen Backup-Größe löscht Kaspersky Embedded Systems Security automatisch die ältesten Dateien. Dadurch ist gewährleistet, dass die maximale Backup-Größe nicht überschritten wird.
Grenzwert für verfügbaren Speicherplatz	Das Kontrollkästchen aktiviert oder deaktiviert die Verfolgung der minimalen Größe des freien Speicherplatzes im Backup (standardmäßig 100 MB). Ist der Umfang des freien Speicherplatzes kleiner als der vorgegebene Grenzwert, protokolliert Kaspersky Embedded Systems Security das Ereignis *Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* und benachrichtigt gemäß den Benachrichtigungseinstellungen über Ereignisse dieses Typs. Wenn dieses Kontrollkästchen aktiviert ist, verfolgt Kaspersky Embedded Systems Security die Größe des freien Speicherplatzes im Backup. Das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz** ist aktiv, wenn das Kontrollkästchen **Maximale Größe des Backups** aktiviert ist.

Arbeiten mit dem Web-Plug-in der Web Console und der Cloud Console

Dieser Abschnitt bietet Informationen über das Verwaltungs-Plug-in von Kaspersky Embedded Systems Security für die Web Console und beschreibt, wie das Programm verwaltet wird, wenn es auf einem geschützten Gerät oder einer Gruppe von Geräten installiert ist.

Kaspersky Embedded Systems Security über die Web Console und Cloud Console verwalten

Sie können mehrere geschützte Geräte, auf denen Kaspersky Embedded Systems Security installiert ist und die in einer Administrationsgruppe zusammengefasst sind, mit dem Web-Plug-in von Kaspersky Embedded Systems Security zentral verwalten. In der Web Console und der Cloud Console von Kaspersky Security Center können Sie auch die Einstellungen jedes geschützten Geräts, das zu der Administrationsgruppe gehört, separat konfigurieren.

Eine *Administrationsgruppe* wird manuell in der Kaspersky Security Center Web Console erstellt. Eine Gruppe beinhaltet mehrere Geräte, auf denen Kaspersky Embedded Systems Security installiert ist und für die Sie einheitliche Verwaltungs- und Schutzeinstellungen festlegen möchten. Ausführliche Informationen über die Verwendung von Administrationsgruppen finden Sie im Hilfesystem von Kaspersky Security Center.

Die Programmeinstellungen für ein einzelnes geschütztes Gerät sind nicht verfügbar, wenn die Arbeit von Kaspersky Embedded Systems Security auf dem geschützten Gerät durch die aktive Richtlinie von Kaspersky Security Center kontrolliert wird.

Sie können Kaspersky Embedded Systems Security auf folgende Arten über die Kaspersky Security Center Web Console verwalten:

- **Mithilfe der Richtlinien von Kaspersky Security Center**. Die Richtlinien von Kaspersky Security Center ermöglichen es, einheitliche Schutzeinstellungen für Gerätegruppen per Fernzugriff zu konfigurieren. Die in der aktiven Richtlinie festgelegten Aufgabeneinstellungen haben Priorität vor den Aufgabeneinstellungen, die lokal in der Anwendungskonsole oder per Remote-Zugriff im Fenster „Eigenschaften: <Name des geschützten Geräts>“ von Kaspersky Security Center konfiguriert wurden. Mithilfe von Richtlinien lassen sich allgemeine Programmeinstellungen, Einstellungen für Aufgaben zum Echtzeit-Computerschutz, Aufgaben zur Aktivitätskontrolle auf Geräten, Einstellungen für den Schutz von Netzwerkspeichern und Einstellungen für den Start lokaler Systemaufgaben nach einem Zeitplan konfigurieren.

- **Mit Hilfe der Gruppenaufgaben von Kaspersky Security Center**. Die Gruppenaufgaben von Kaspersky Security Center ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit einer begrenzten Ausführungsdauer für Gerätegruppen per Fernzugriff. Mithilfe von Gruppenaufgaben können Sie das Programm aktivieren sowie die Einstellungen der Aufgaben „Untersuchung auf Befehl“, der Update-Aufgabe und der Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts konfigurieren.

- **Mithilfe von Aufgaben für eine Auswahl von Geräten**. Aufgaben für eine Auswahl von Geräten ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit begrenzter Ausführungsdauer und für geschützten Geräte, die keiner Administrationsgruppe zugeordnet sind, per Fernzugriff.

- **Mithilfe des Konfigurationsfensters für ein einzelnes Gerät**. Im Fenster mit den Eigenschaften des Geräts können Sie die Aufgabeneinstellungen für ein einzelnes geschütztes Gerät, das einer Administrationsgruppe zugeordnet ist, per Fernzugriff konfigurieren. Sie können außerdem sowohl allgemeine Programmeinstellungen als auch Einstellungen für alle Aufgaben von Kaspersky Embedded Systems Security anpassen, wenn das ausgewählte geschützte Gerät sich nicht unter der Verwaltung der aktiven Richtlinie von Kaspersky Security Center befindet.

Die Kaspersky Security Center Web Console und die Cloud Console erlauben Ihnen die Anpassung der Programmeinstellungen und erweiterten Optionen, sowie die Arbeit mit Protokollen und Benachrichtigungen. Sie können diese Einstellungen sowohl für Gruppen von geschützten Geräten als auch für ein einzelnes geschütztes Gerät anpassen.

Einschränkungen für Web Plug-in

Das Web-Plug-in für Kaspersky Embedded Systems Security hat folgende Einschränkungen im Vergleich zum Verwaltungs-Plug-in für Kaspersky Embedded Systems Security:

- Die Regeln für die Komponente Kontrolle des Programmstarts können nicht mit digitalen Zertifikaten oder Kaspersky Security Center-Ereignissen erstellt werden.

- Die Regeln für die Komponente Gerätekontrolle können nicht anhand von verbundenen Geräten oder Systemdaten generiert werden.

Programmeinstellungen verwalten

Dieser Abschnitt enthält Informationen über die Konfiguration der allgemeinen Einstellungen von Kaspersky Embedded Systems Security in der Kaspersky Security Center Web Console.

Allgemeine Programmeinstellungen im Web-Plug-in konfigurieren

Sie können die allgemeinen Einstellungen von Kaspersky Embedded Systems Security im Web-Plug-in für Gruppen von geschützten Geräten und für ein einzelnes geschütztes Gerät konfigurieren.

Schnittstelle und Untersuchungseinstellungen im Web-Plug-in konfigurieren

So konfigurieren Sie die Einstellungen der Programmoberfläche:

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

2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Einstellungen der Benutzeroberfläche** auf **Anpassen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen für die Interaktion mit dem Benutzer und Untersuchungseinstellungen

Einstellung	Beschreibung
Interaktion mit dem Benutzer	**Benutzeroberfläche nicht anzeigen**. Auf dem Client-Computer sind keinerlei Merkmale für die Verwendung von Kaspersky Embedded Systems Security sichtbar. Auch das Symbol im Infobereich der Windows-Taskleiste und die Benachrichtigungen sind nicht verfügbar. **Benutzeroberfläche anzeigen**. Auf dem Client-Computer wird ein Symbol in der Windows-Taskleiste angezeigt. Der Benutzer kann im Kontextmenü des Symbols Vorgänge mit Kaspersky Embedded Systems Security ausführen. Kaspersky Embedded Systems Security zeigt Benachrichtigungen über dem Programmsymbol an. Über das Kontextmenü des Symbols in der Windows-Taskleiste können Sie das kompakte Diagnosefenster öffnen. Wenn Sie im kompakten Diagnosefenster auf einen Link klicken, wird die Anwendungskonsole geöffnet.
Programmstatus im Infobereich der Taskleiste anzeigen	Aktivieren Sie die Kontrollkästchen für jene Ereigniskategorien, über die im Infobereich der Microsoft Windows-Taskleiste Benachrichtigungen angezeigt werden sollen.

Einstellungen für Sicherheit und Zuverlässigkeit im Web-Plug-in konfigurieren

Um die Sicherheitsparameter manuell anzupassen, 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, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Sicherheit und Zuverlässigkeit** auf **Anpassen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen für Sicherheit und Zuverlässigkeit

Einstellung	Beschreibung
Programm beim Hochfahren des Computers starten (empfohlen)	Ist das Kontrollkästchen aktiviert, so wird Kaspersky Embedded Systems Security nach dem Laden des Betriebssystems gestartet und schützt den Computer während der gesamten Sitzung. Ist das Kontrollkästchen deaktiviert, so wird Kaspersky Embedded Systems 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.
Programmprozesse vor externen Bedrohungen schützen	Ist das Kontrollkästchen aktiviert, so verhindert Kaspersky Embedded Systems Security, dass Dateien des Programms auf der Festplatte, Prozesse im Arbeitsspeicher und Einträge in der Systemregistrierung verändert oder gelöscht werden.
Betriebssystemdienste schützen	Wenn der Schutz für die Betriebssystemdienste aktiviert ist, dürfen Drittanbieter-Programme die Prozesse des Betriebssystems nicht beeinflussen. Wenn der Schutz für die Betriebssystemdienste deaktiviert ist, können Drittanbieter-Programme die Prozesse des Betriebssystems beeinflussen.

Einstellung	Beschreibung
Geplante Aufgaben bei Akkubetrieb aufschieben	Wenn diese Option ausgewählt ist, ist der Energiesparmodus aktiviert. Kaspersky Embedded Systems 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: • *Update der Datenbanken und Programm-Module* • *Vollständige Untersuchung* • *Untersuchung wichtiger Bereiche* • *Benutzerdefinierte Untersuchung* • *Kontrolle der Anwendungsintegrität* • *IOC-Untersuchung*.
Computerstatus beim Anwenden von Einstellungen	Einstellungen für die Anzeige von Statusvarianten der Client-Computer, auf denen das Programm Kaspersky Embedded Systems 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*.
Kompatibilität mit Fernverwaltungsanwendungen	Wenn die Verwendung von Kaspersky Embedded Systems Security zusammen mit Remote Administration Tools (RAT) Probleme verursacht, 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 Embedded Systems 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 Embedded Systems 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.

Einstellung	Beschreibung
CPU-Auslastung für Untersuchungsaufgaben begrenzen	Während auf einem geschützten Gerät eine Untersuchung auf Befehl durchgeführt wird, begrenzt Kaspersky Embedded Systems Security die CPU-Nutzung auf dem Gerät mit dem im Feld **Obergrenze** angegeben Wert. Das Programm kann aber aufgrund anderer Komponenten trotzdem mehr CPU-Zeit beanspruchen. Das Aktivieren dieser Funktionalität kann sich negativ auf die Leistung von Kaspersky Embedded Systems Security auswirken. Diese Funktion ist standardmäßig deaktiviert.
Ressourcen für andere Programme freigeben	Während der Computer untersucht wird, beansprucht Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security mehr Zeit benötigt, um den Computer zu untersuchen. Der Modus zur Freigabe von Ressourcen für andere Programme ist standardmäßig aktiviert.

Anpassen der Verbindungseinstellungen im Web-Plug-in

Die angepassten Verbindungseinstellungen werden verwendet: für die Verbindungsaufnahme von Kaspersky Embedded Systems Security mit den Update- und Aktivierungsservern sowie bei der Integration des Programms in die Dienste von Kaspersky Security Network.

Zum Einrichten der Verbindungseinstellungen 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, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Verbindungseinstellungen** auf **Anpassen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Verbindungseinstellungen

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 Embedded Systems 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.
Keinen Proxyserver verwenden	Wenn diese Option ausgewählt ist, verwendet Kaspersky Embedded Systems Security keinen Proxyserver.
Proxyserver-Einstellungen automatisch ermitteln	Wenn diese Option ausgewählt ist, verwendet Kaspersky Embedded Systems Security die Proxyserver-Einstellungen des Betriebssystems.
Angegebene Proxyserver-Einstellungen verwenden	Wenn diese Option ausgewählt ist, verwendet Kaspersky Embedded Systems Security die manuell angegebenen Proxyserver-Einstellungen. Geben Sie die IP-Adresse oder den symbolischen Namen des Proxyservers sowie die Portnummer ein.

Einstellung	Beschreibung
Einen Proxyserver für lokale Adressen umgehen	Wenn diese Funktionalität aktiviert ist, erfolgt der Zugriff auf Geräte direkt aus dem Netzwerk, zu dem das geschützte Gerät mit installiertem Kaspersky Embedded Systems Security gehört. Diese Option ist standardmäßig aktiviert.
Einstellungen der Proxyserver-Authentifizierung	Um das Programm auf dem Proxyserver für den Internetzugang zu authentifizieren, müssen Sie die Anmeldedaten des Benutzers eingeben. Kaspersky Embedded Systems 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. **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 Embedded Systems Security abhängig von den Proxyserver-Einstellungen die Authentifizierung anhand des Kerberos- oder NTLM-Protokolls durchführen.
Alle Netzwerkports überwachen	In diesem Modus zur Überwachung von Netzwerkports überwachen die Schutzkomponenten 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.
Kaspersky Security Center als Proxyserver für die Programmaktivierung verwenden	Geben Sie an, ob Kaspersky Security Center als Proxyserver für die Programmaktivierung verwendet wird.

Geplanten Starts lokaler Aufgaben im Web-Plug-in konfigurieren

Sie können Richtlinien verwenden, um den Start von lokalen Systemaufgaben zur Untersuchung auf Befehl und zum Update zuzulassen oder zu blockieren. Dies erfolgt gemäß des Zeitplans, der lokal auf jedem geschützten Gerät in der Administrationsgruppe konfiguriert wurde:

- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie verboten ist, werden solche Aufgaben nicht auf dem geschützten Gerät gemäß Zeitplan ausgeführt. Sie können lokale Systemaufgaben manuell starten.

- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie erlaubt ist, werden solche Aufgaben gemäß den lokal für diese Aufgabe angepassten Zeitplan-Einstellungen ausgeführt.

Standardmäßig ist der Start von lokalen Systemaufgaben durch eine Richtlinie verboten.

Es wird empfohlen, den Start lokaler Systemaufgaben nicht zu erlauben, wenn die Updates oder die Untersuchungen auf Befehl anhand von Gruppenaufgaben von Kaspersky Security Center gesteuert werden.

Wenn Sie keine Gruppenaufgaben für Updates oder Untersuchungen auf Befehl verwenden, erlauben Sie den Start lokaler Systemaufgaben in einer Richtlinie: Kaspersky Embedded Systems Security wird Updates der Datenbanken und Programm-Module ausführen und alle lokalen Systemaufgaben zur Untersuchung auf Befehl gemäß den standardmäßigen Zeitplan-Einstellungen starten.

Mithilfe von Richtlinien können Sie den Start folgender lokaler Systemaufgaben nach Zeitplan erlauben oder verbieten:

- Aufgaben zur Untersuchung auf Befehl: *Untersuchung wichtiger Bereiche*, *Untersuchung beim Start des Betriebssystems*, *Kontrolle der Anwendungsintegrität*, *Baseline-Überwachung der Systemintegrität*.
- Die Aufgabe *Update*.

Wenn Sie ein geschütztes Gerät aus der Administrationsgruppe ausschließen, wird der Zeitplan der lokalen Systemaufgaben automatisch aktiviert.

So erlauben oder verbieten Sie den Start der lokalen Systemaufgaben von Kaspersky Embedded Systems Security nach Zeitplan in einer Richtlinie:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Lokale Systemaufgaben ausführen** auf **Anpassen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen für den Start lokaler Aufgaben

Einstellung	Beschreibung
Verwendung lokaler Aufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, werden die lokalen Aufgaben auf der lokalen Programmoberfläche von Kaspersky Embedded Systems Security angezeigt. Sofern die Richtlinie keine zusätzlichen Einschränkungen festlegt, kann der Benutzer Aufgaben anpassen und starten. Das Konfigurieren eines Ausführungszeitplan ist für den Benutzer jedoch weiterhin nicht verfügbar. Der Benutzer kann Aufgaben nur manuell ausführen. Ist dieses Kontrollkästchen deaktiviert, so können lokale Aufgaben nicht verwendet werden. In diesem Modus werden lokale Aufgaben nicht nach Zeitplan gestartet. Aufgaben können auf der lokalen Benutzeroberfläche von Kaspersky Embedded Systems Security nicht gestartet und geändert werden. Dies gilt auch bei Verwendung der Befehlszeile.
Verwaltung von Zeitplänen erlauben	Das Kontrollkästchen ist verfügbar, wenn das Kontrollkästchen **Verwendung lokaler Aufgaben erlauben** aktiviert ist. Wenn das Kontrollkästchen aktiviert ist, wird die Zeitplanverwaltung in den Eigenschaften der lokalen Aufgabe in der Anwendungskonsole verfügbar. Das Kontrollkästchen ist standardmäßig deaktiviert.
Anzeige von Gruppenaufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, werden Gruppenaufgaben auf der lokalen Programmoberfläche von Kaspersky Embedded Systems Security angezeigt. Der Benutzer kann die komplette Aufgabenliste in der Anwendungskonsole einsehen. Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Embedded Systems Security eine leere Aufgabenliste an.
Verwaltung von Gruppenaufgaben erlauben	Wenn das Kontrollkästchen aktiviert ist, kann der Benutzer die Gruppenaufgaben starten und anhalten, die in Kaspersky Security Center festgelegt wurden. Der Benutzer kann Aufgaben in der Anwendungskonsole oder auf der einfachen Programmoberfläche starten und anhalten. Wenn das Kontrollkästchen deaktiviert ist, startet entweder Kaspersky Embedded Systems Security die Aufgaben automatisch nach Zeitplan oder der Administrator startet die Aufgaben manuell in Kaspersky Security Center.

Backup-Einstellungen im Web-Plug-in konfigurieren

Um die Backup-Einstellungen in Kaspersky Security Center anzupassen, 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, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Zusätzlich** aus.
5. Klicken Sie im Unterabschnitt **Speicher** auf **Anpassen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Speichereinstellungen

Einstellung	Beschreibung
Nehmen Sie auf der Registerkarte **Berichte** die folgenden Berichtseinstellungen vor:	
Berichte speichern für maximal	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 Embedded Systems Security automatisch die ältesten Einträge aus der Berichtsdatei.
Maximale Größe der Berichtsdatei	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 Embedded Systems Security automatisch die ältesten Einträge aus der Berichtsdatei. Dadurch ist gewährleistet, dass die maximale Berichtsdateigröße nicht überschritten wird.
Nehmen Sie auf der Registerkarte **Backup** die folgenden Backup-Einstellungen vor:	
Objekte speichern für maximal	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 Embedded Systems Security die ältesten Dateien aus dem Backup.
Maximale Größe des Backups	Ist das Kontrollkästchen aktiviert, so ist die maximale Backup-Größe durch den festgelegten Wert beschränkt. Die maximale Größe beträgt standardmäßig 400 MB. Nach Erreichen der maximalen Backup-Größe löscht Kaspersky Embedded Systems Security automatisch die ältesten Dateien. Dadurch ist gewährleistet, dass die maximale Backup-Größe nicht überschritten wird.
Grenzwert für verfügbaren Speicherplatz	Das Kontrollkästchen aktiviert oder deaktiviert die Verfolgung der minimalen Größe des freien Speicherplatzes im Backup (standardmäßig 100 MB). Ist der Umfang des freien Speicherplatzes kleiner als der vorgegebene Grenzwert, protokolliert Kaspersky Embedded Systems Security das Ereignis „Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten" und benachrichtigt gemäß den Benachrichtigungseinstellungen über Ereignisse dieses Typs. Wenn dieses Kontrollkästchen aktiviert ist, verfolgt Kaspersky Embedded Systems Security die Größe des freien Speicherplatzes im Backup. Das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz** ist aktiv, wenn das Kontrollkästchen **Maximale Größe des Backups** aktiviert ist. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt bietet Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Embedded Systems Security auf mehreren geschützten Geräten.

Sie können in Kaspersky Security Center einheitliche Richtlinien erstellen, um den Schutz auf mehreren Geräten zu verwalten, auf denen Kaspersky Embedded Systems Security installiert ist.

Eine Richtlinie erzwingt die Einstellungen, Funktionen und Aufgaben von Kaspersky Embedded Systems Security auf allen geschützten Geräten einer Administrationsgruppe.

Sie können mehrere Richtlinien für eine Administrationsgruppe erstellen und sie temporär übernehmen. Die Richtlinie, die momentan für eine Gruppe aktiv ist, hat in der Web Console den Status *Aktiv*.

Informationen über den Geltungsbereich einer Richtlinie werden im Systemaudit-Protokoll von Kaspersky Embedded Systems Security protokolliert. Diese Informationen stehen in der Programmkonsole unter dem Knoten **Protokolle und Meldungen** zur Verfügung.

In Kaspersky Security Center existiert eine einzige Methode zur Übernahme von Richtlinien auf geschützten Geräten: *Änderung von Einstellungen verbieten*. Nachdem eine Richtlinie angewendet wurde, verwendet Kaspersky Embedded Systems Security die Einstellungen, für welche Sie das Zeichen in den Richtlinieneigenschaften auf geschützten Geräten ausgewählt haben. In diesem Fall werden die ausgewählten Einstellungen verwendet anstatt der Einstellungen, die vor dem Anwenden der Richtlinie wirksam waren. Einstellungen der aktiven Richtlinie, für die in den Richtlinieneigenschaften das Zeichen gesetzt ist, werden von Kaspersky Embedded Systems Security nicht übernommen.

Ist eine Richtlinie aktiv, so werden die Werte der Einstellungen, die in der Richtlinie mit dem Symbol markiert sind, in der Programmkonsole angezeigt, können jedoch nicht bearbeitet werden. Die Werte der restlichen Einstellungen (die in der Richtlinie mit dem Symbol markiert sind) können in der Programmkonsole bearbeitet werden.

Die in der aktiven Richtlinie festgelegten und mit dem Symbol markierten Einstellungen blockieren auch die Bearbeitung der Einstellungen in Kaspersky Security Center für ein einzelnes geschütztes Gerät im Fenster **Eigenschaften: <Name des geschützten Geräts>**.

Einstellungen, die angepasst und mithilfe einer aktiven Richtlinie an das geschützte Gerät übergeben wurden, werden nach der Deaktivierung der aktiven Richtlinie in den Einstellungen der lokalen Aufgaben gespeichert.

Wenn in einer Richtlinie Einstellungen für eine beliebige Aufgabe zum Echtzeit-Computerschutz oder zum Schutz von Netzwerkspeichern festgelegt sind, die gerade ausgeführt wird, werden die in der Richtlinie festgelegten Einstellungen sofort nach dem Übernehmen der Richtlinie geändert. Wenn die Aufgabe nicht ausgeführt wird, werden die Parameter aus der Richtlinie beim nächsten Aufgabenstart übernommen.

So erstellen Sie eine Richtlinie (in der Kaspersky Security Center Web Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Das Fenster **Neue Richtlinie** wird geöffnet.
4. Wählen Sie im Abschnitt **Anwendung auswählen** das Programm „Kaspersky Embedded Systems Security" aus.
5. Legen Sie die Modi von Kaspersky Embedded Systems Security auf geschützten Geräten fest.
6. Geben Sie bei Bedarf Dateien oder Ordner sowie Namen von Objekten an (gemäß der Viren-Enzyklopädie), die Sie von der Untersuchung durch alle oder bestimmte Programmkomponenten ausschließen möchten.

7. Auf der Registerkarte **Allgemein** können Sie folgende Aktionen ausführen:

   - Name der Richtlinie ändern

     > Die Namen von Richtlinien dürfen keines der folgenden Symbole enthalten: `" * < : > ? \ | .`

   - Auswählen des Richtlinienstatus:

     - **Aktiv**. Die Richtlinie wird auf diesem Computer nach der nächsten Synchronisierung als aktive Richtlinie verwendet.

     - **Inaktiv**. Ersatzrichtlinie. Eine inaktive Richtlinie kann erforderlichenfalls aktiviert werden.

     - **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. Das Kontrollkästchen **Einstellungen aus übergeordneter Richtlinie erben** wird in den Einstellungen der untergeordneten Richtlinie automatisch aktiviert. 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. Konfigurieren Sie die Richtlinieneinstellungen auf der Registerkarte **Anwendungseinstellungen** wie erforderlich.

9. Klicken Sie auf **Speichern**.

Nachdem eine neue Richtlinie erstellt wurde, wird eine Reihe von Erlaubnisregeln erstellt, um das Blockieren von Programmen zu verhindern und ihren unterbrechungsfreien Betrieb zu gewährleisten.

Standardmäßig erstellt Kaspersky Embedded Systems Security bei der Erstellung einer neuen Richtlinie einen Satz von Regeln für den eingehenden Netzwerkverkehr:

- Zwei Erlaubnisregeln für die Freigabe des Windows-Desktops mithilfe des Kaspersky Security Center Administrationsagenten, der sich in den Ordnern %Programme% und %Programme (x86)% befindet. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

- Zwei Erlaubnisregeln für den lokalen Port 15000. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

Standardmäßig erstellt Kaspersky Embedded Systems Security beim Erstellen einer neuen Richtlinie einen Satz von Regeln für den ausgehenden Netzwerkverkehr:

- Zwei Erlaubnisregeln für den Dienst Kaspersky Embedded Systems Security, der sich in den Ordnern %Programme% und %Programme (x86)% befindet. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.
- Zwei Erlaubnisregeln für den Arbeitsprozess von Kaspersky Embedded Systems Security, der sich in den Ordnern %Programme% und %Programme (x86)% befindet. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.
- Zwei Erlaubnisregeln für den lokalen Port 13000. Status: aktiviert. Erlaubte externe Adressen: alle. Protokolle: TCP und UPD – eine Regel pro Protokoll.

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Embedded Systems Security, ihre Erstellung, die Konfiguration ihrer Ausführung sowie über den Start/die Beendigung von Aufgaben.

Zur Erstellung von Aufgaben im Web-Plug-in

Sie können lokale Aufgaben und Gruppenaufgaben auf folgende Art und Weise erstellen:

- Für ein geschütztes Gerät: im Fenster **Eigenschaften: <Name des geschützten Geräts>** im Abschnitt **Aufgaben**.
- Für eine Administrationsgruppe: Im Ergebnisbereich des Knotens der ausgewählten Gruppe von geschützten Geräten auf der Registerkarte **Aufgaben**.
- Für eine Auswahl an geschützten Geräten: Im Ergebnisbereich des Knotens **Geräteauswahlen**.

Mithilfe von Richtlinien können Sie Zeitpläne für die lokalen Systemaufgaben *Update* und *Untersuchung auf Befehl* auf allen geschützten Geräten in derselben Administrationsgruppe deaktivieren.

Allgemeine Informationen über den Aufgaben in Kaspersky Security Center sind im Hilfesystem von Kaspersky Security Center zu finden.

Eine Aufgabe im Web-Plug-in erstellen

So erstellen Sie eine neue Aufgabe in der Kaspersky Security Center Web Console:

1. Starten Sie den Assistenten für neue Aufgaben nach einer der folgenden Methoden:

   - Für das Erstellen einer lokalen Aufgabe:

     a. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung** → **Assets (Geräte)** aus.

     b. Klicken Sie auf den Namen des geschützten Geräts.

     c. Wählen Sie im folgenden Fenster **<Name des Geräts>** die Registerkarte **Aufgaben** aus.

     d. Klicken Sie auf **Hinzufügen**.

   - Für das Erstellen einer Gruppenaufgabe:

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

     b. Klicken Sie auf **Hinzufügen**.

   Darauf öffnet sich der Assistent für neue Aufgaben.

2. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Embedded Systems Security** aus.

3. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Typ der Aufgabe aus, die Sie erstellen möchten.

4. Je nach Typ der gewählten Aufgabe führen Sie eine der folgenden Aktionen aus:

   - Aufgabe zur Untersuchung auf Befehl erstellen.

   - Wenn Sie eine der Aufgaben zum Update erstellen, aktivieren Sie die gewünschten Aufgabenparameter nach Ihren Bedürfnissen:

     a. Im Block **Update-Quellen** können Sie den Kaspersky Security Center Administrationsserver oder die Kaspersky-Update-Server als Update-Quelle für das Programm-Update angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen.

     Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

     b. Konfigurieren Sie die Einstellungen für eine Funktion, die die Auslastung des Festplattensubsystems senkt:

     c. Sie können festlegen, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Updates für Programm-Module erforderlich sind oder nachdem die Installation wichtiger Updates abgeschlossen wurde. Darüber hinaus können Sie festlegen, ob Kaspersky Embedded Systems Security Informationen über verfügbare geplante Updates erhalten soll.

     d. Geben Sie die zu kopierenden Updates und den Pfad des Ordners an, in dem Kaspersky Embedded Systems Security die kopierten Updates speichert.

- So erstellen Sie die Aufgabe Aktivierung des Programms:

  a. Geben Sie im Fenster **Einen Lizenzschlüssel auswählen** die Schlüsseldatei oder den Aktivierungscode an, mit der bzw. dem Sie das Programm aktivieren möchten.

  b. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie eine Aufgabe zur Verlängerung der Lizenz erstellen möchten.

- Erstellen und konfigurieren Sie die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts.

- Erstellen und konfigurieren Sie die Aufgabe Erstellen von Regeln für die Gerätekontrolle.

5. Klicken Sie auf **Weiter**.

6. Wenn die Aufgabe für eine Zusammenstellung von geschützten Geräten erstellt wird, wählen Sie das Netzwerk (oder die Gruppe) der geschützten Geräte aus, an denen die Aufgabe ausgeführt werden soll.

7. Klicken Sie auf **Weiter**.

8. Aktivieren Sie im Fenster **Erstellung der Aufgabe abschließen** das Kontrollkästchen **Nach Abschluss der Erstellung Aufgabendetails öffnen**, wenn Sie die Aufgabeneinstellungen konfigurieren möchten.

9. Klicken Sie auf **Fertigstellen**.

Die erstellte Aufgabe erscheint in der Liste **Aufgaben**.

Gruppenaufgaben im Web-Plug-in anpassen

Gehen Sie wie folgt vor, um eine Gruppenaufgabe für mehrere geschützte Geräte zu konfigurieren:

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

2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

   Das Fenster **<Aufgabenname>** wird geöffnet.

3. Gehen Sie auf die Registerkarte **Anwendungseinstellungen**.

4. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eines der Folgenden aus:

   - So konfigurieren Sie die *Untersuchung auf Befehl*-Aufgabe:

     a. Legen Sie im Abschnitt **Untersuchungsbereich** einen Untersuchungsbereich fest.

     b. Konfigurieren Sie im Abschnitt **Optionen** die Stufe der heuristischen Analyse und die Integration in andere Programmkomponenten.

   - Um die *Update*-Aufgabe zu konfigurieren, passen Sie die Aufgabeneinstellungen entsprechend an:

     a. Passen Sie im Abschnitt **Update-Quellen** die Einstellungen für die Update-Quelle an.

     b. Im Abschnitt **Update-Einstellungen** können Sie die Optimierungseinstellungen für das Laufwerksubsystem verwalten; festlegen, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Updates für Programm-Module verfügbar sind oder wenn Informationen über geplante Updates verfügbar sind; sowie die Kopiereinstellungen für Updates angeben.

- Um die Aufgabe *Aktivierung des Programms* zu konfigurieren, übernehmen Sie die Schlüsseldatei oder den Aktivierungscode, mit der bzw. dem Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**, wenn Sie einen Aktivierungscode oder eine Schlüsseldatei zur Verlängerung der Lizenz hinzufügen möchten.

- Um die automatische Generation von Erlaubnisregeln für die Gerätekontrolle zu konfigurieren, geben Sie die Einstellungen ein, die verwendet werden, um die Liste der Erlaubnisregeln zu erstellen.

5. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe *Update-Rollback* anpassen).

6. Geben Sie auf der Registerkarte **Einstellungen** im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im Hilfesystem von Kaspersky Security Center.

7. Klicken Sie auf **Speichern**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Aufgabe zur Programmaktivierung im Web-Plug-in konfigurieren

So konfigurieren Sie die Aktivierung des Programms-Aufgabe:

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

2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

   Das Fenster **<Aufgabenname>** wird geöffnet.

3. Geben Sie im Abschnitt **Anwendungseinstellungen** die Schlüsseldatei an, mit der Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.

4. Passen Sie den Aufgabenzeitplan im Abschnitt **Zeitplan** an.

5. Klicken Sie im Fenster **<Aufgabenname>** auf die Schaltfläche **Speichern**.

Update-Aufgabe im Web-Plug-in konfigurieren

So konfigurieren Sie die Update-Aufgabe:

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

2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

   Das Fenster <Aufgabenname> wird geöffnet.

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

4. Passen Sie im Abschnitt **Update-Quellen** die Einstellungen für die Update-Quelle an:

   a. Geben Sie den Kaspersky Security Center Administrationsserver oder die Kaspersky-Update-Server als Update-Quelle an. Sie können auch eine benutzerdefinierte Liste mit Update-Quellen erstellen, indem Sie andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen.

   Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

   b. Konfigurieren Sie die Einstellungen für eine Funktion, die die Auslastung des Festplattensubsystems senkt:

   - **Belastung des Festplatten-Subsystems verringern**
   - **Für die Optimierung genutzter Arbeitsspeicher (MB)**

   c. Legen Sie fest, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Updates für Programm-Module verfügbar sind oder wenn Informationen über geplante Updates vorliegen.

   d. Geben Sie die Einstellungen für das Kopieren von Updates an.

5. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe *Update-Rollback* anpassen).

6. Klicken Sie im Fenster **<Aufgabenname>** auf **OK**.

Aufgaben planen

In der Web Console können Sie lokale Systemaufgaben und benutzerdefinierte Aufgaben planen.

So planen Sie Gruppenaufgaben mithilfe der Web Console:

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

2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

   Das Fenster **<Aufgabenname>** wird geöffnet.

3. Gehen Sie zum Abschnitt **Zeitplan** und konfigurieren Sie die Zeitplaneinstellungen (siehe Tabelle unten).

   Die Felder mit den Zeitplan-Einstellungen der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe stehen nicht zur Verfügung, wenn der Zeitplan dieser Aufgaben durch eine Richtlinie von Kaspersky Security Center blockiert wird.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Einstellungen für den Aufgabenstart zu speichern.

Einstellungen für den Aufgabenzeitplan

Einstellung	Beschreibung
Start nach Zeitplan	Wählen Sie den Funktionsmodus der Aufgabe aus: • **Alle n Stunden**. Die Aufgabe wird in regelmäßigen Abständen alle paar Stunden ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Stunden) an. • **Alle n Tage**. Die Aufgabe wird in regelmäßigen Abständen alle paar Tage ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Tagen) an. • **Alle n Minuten**. Die Aufgabe wird in regelmäßigen Abständen alle paar Minuten ausgeführt. Geben Sie die Startzeit der Aufgabe und den Abstand (in Minuten) an. • **Nach Wochentagen**. Die Aufgabe wird an den angegebenen Wochentagen ausgeführt. Wählen Sie die Wochentage aus und geben Sie die Startzeit an. Wenn die Aufgabe in Intervallen von mehreren Wochen ausgeführt werden soll, geben Sie den gewünschten Wert in das Feld **Intervall** ein. • **Monatlich**. Die Aufgabe wird an einem bestimmten Tag des Monats ausgeführt. Geben Sie Datum und Uhrzeit des Starts an. • **Einmal**. Die Aufgabe wird einmal zum angegebenen Zeitpunkt (Datum und Uhrzeit) ausgeführt. • **Manuell**. Ein Ausführungsmodus, bei dem die Untersuchung manuell zu einem für Sie geeigneten Zeitpunkt gestartet werden kann. • **Nach dem Download neuer Updates in die Datenverwaltung**. Die Aufgabe wird jedes Mal ausgeführt, wenn Updates in die Datenverwaltung heruntergeladen werden. • **Nach Abschluss einer anderen Aufgabe**. Die Aufgabe wird ausgeführt, sobald eine andere Aufgabe abgeschlossen wird. Wählen Sie die Aufgabe und den Aufgabenstatus aus. Kaspersky Embedded Systems Security unterstützt den Modus **Nach Abschluss einer anderen Aufgabe** für die Zeitplanung lokaler Aufgaben nicht. • **Beim Erkennen eines Virenangriffs**. Die Aufgabe wird ausgeführt, wenn ein Virenangriff erkannt wird. • **Start in N Minuten nach dem Start der Anwendung**. Die Aufgabe wird jedes Mal beim Start von Kaspersky Embedded Systems Security mit einer festgelegten Verzögerung ausgeführt. Geben Sie im Feld **Verzögerung des Aufgabenstarts (Min.)** die Anzahl der Minuten an.
Übersprungene Aufgaben starten	Ist das Kontrollkästchen aktiviert, startet Kaspersky Embedded Systems 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 Embedded Systems Security übersprungene Aufgaben nicht aus. Stattdessen wird die nächste Aufgabe gemäß dem aktuellen Zeitplan ausgeführt.
Automatische zufällige Verzögerung für Aufgabenstarts verwenden	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe 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.
Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von	Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabe auf Computern innerhalb eines bestimmten Zeitraums zu einem zufälligen Zeitpunkt ausgeführt. Zufällige Startzeiten verhindern, dass viele Computer gleichzeitig auf den Administrationsserver zugreifen, wenn die Aufgabe nach Zeitplan ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe exakt zum geplanten Zeitpunkt ausgeführt.
Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren	Wenn dieses Kontrollkästchen aktiviert ist, erhält das Betriebssystem des Computers eine bestimmte Vorlaufzeit für seinen Start, bevor die Aufgabe ausgeführt wird. Standardmäßig beträgt die Vorlaufzeit 5 Minuten. Aktivieren Sie das Kontrollkästchen, wenn Sie die Aufgabe auf allen Computern ausführen möchten, auch auf ausgeschalteten Computern.
Geräte nach Abschluss der Aufgabe herunterfahren	Wenn dieses Kontrollkästchen aktiviert ist, wird der Computer nach Abschluss der Aufgabe heruntergefahren. Sie können diese Funktion beispielsweise aktivieren, um den Computer freitags nach Feierabend untersuchen zu lassen. Nach Abschluss der Aufgabe schaltet das Programm den Computer für das Wochenende aus.
Aufgabe unterbrechen, wenn deren Ausführung länger dauert als	Ausführungszeit der Aufgabe begrenzen. Kaspersky Embedded Systems Security bricht die Aufgabe nach Ablauf des festgelegten Zeitraums ab. Die Aufgabe wird nicht als abgeschlossen markiert. Wenn Kaspersky Embedded Systems Security die Aufgabe das nächste Mal ausführt, wird sie von vorne gestartet und wie geplant ausgeführt.

Einstellung	Beschreibung
Aufgabenausführung pausieren	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 Embedded Systems Security auf die Leistung Ihres Computers bei hoher Auslastung zu minimieren. Diese Funktion ist nur für Aufgaben vom Typ Untersuchung auf Befehl verfügbar.
Enddatum	Wenn das Kontrollkästchen aktiviert ist, beendet Kaspersky Embedded Systems Security ab dem angegebenen Datum die Ausführung der geplanten Aufgabe. Die Aufgabe wird in den Modus **Manuell** versetzt. Diese Funktion ist nur für Aufgaben vom Typ Untersuchung auf Befehl verfügbar.

Berichte in Kaspersky Security Center

Die Berichte von Kaspersky Security Center enthalten Informationen zum Status der verwalteten Geräte. Die Berichte basieren auf Informationen, die auf dem Administrationsserver gespeichert sind.

Ab Kaspersky Security Center 11 sind folgende Berichtstypen für Kaspersky Embedded Systems Security verfügbar:

- Bericht über den Status der Programmkomponenten
- Bericht über verbotene Programme
- Bericht über verbotene Programme im Testmodus

Detaillierte Informationen zu allen Berichten in Kaspersky Security Center und deren Konfiguration finden Sie in der Hilfe zu Kaspersky Security Center.

Bericht über den Status der Programmkomponenten von Kaspersky Embedded Systems Security

Sie können den Schutzstatus aller Netzwerkgeräte überwachen und eine strukturierte Übersicht der Komponentenauswahl auf jedem Gerät anzeigen lassen.

Der Bericht zeigt für jede Komponente eine der folgenden Statusvarianten an: *Wird ausgeführt*, *Angehalten*, *Abgebrochen*, *Nicht durch Lizenz abgedeckt*.

Der Status *Nicht installiert* bezieht sich auf die Komponente, nicht auf das Programm selbst. Wenn das Programm nicht installiert ist, wird in der Kaspersky Security Center Web Console der Status "N/A" (Nicht verfügbar) zugewiesen.

Sie können eine Komponentenauswahl erstellen und den Filter verwenden, um Netzwerkgeräte mit einer festgelegten Auswahl an Komponenten samt Status anzuzeigen.

Nähere Informationen zur Erstellung und Verwendung einer Auswahl finden Sie in der Hilfe zu Kaspersky Security Center.

So zeigen Sie den Status der Komponenten an (in der Kaspersky Security Center Web Console):

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Assets (Geräte)** → **Verwaltete Geräte** aus.
2. Klicken Sie auf den Gerätenamen und gehen Sie zum Abschnitt **Anwendungen**.
3. Klicken Sie auf den Namen des Programms von Kaspersky Embedded Systems Security.
4. Gehen Sie im folgenden Fenster auf der Registerkarte **Allgemein** zum Abschnitt **Komponenten**.
5. Eine Tabelle mit Statusvarianten wird Ihnen angezeigt.

So zeigen Sie einen Standardbericht an (in der Kaspersky Security Center Web Console):

1. Wählen Sie die Option **Überwachung** → **Berichte** aus.
2. Wählen Sie in der Liste **Bericht über den Status der Programmkomponenten** aus und klicken Sie darauf.
   Ein Bericht wird erstellt.
3. Passen Sie die folgenden Einstellungen für Anfragen an:
   - ein Schaubild
   - eine Übersichtstabelle mit Komponenten und der Gesamtanzahl der Netzwerkgeräte, auf denen jede Komponente installiert ist, sowie die Gruppen, zu denen sie gehören
   - eine detaillierte Tabelle mit dem Status, der Version, dem Gerät und der Gruppe der Komponente

Berichte über verbotene Programme im Modus "Aktiv" und "Statistik"

Basierend auf den Ergebnissen der Aufgabe zur Kontrolle des Programmstarts können zwei Arten von Berichten erstellt werden: ein Bericht über verbotene Programme (wenn die Aufgabe im aktiven Modus gestartet wurde) und ein Bericht über verbotene Programme im Testmodus (wenn die Aufgabe im Informieren-Modus gestartet wurde). Diese Berichte enthalten Informationen über blockierte Programme auf den geschützten Geräten im Netzwerk. Jeder Bericht wird für alle Administrationsgruppen erstellt und sammelt die Daten aller Kaspersky-Programme, die auf den geschützten Geräten installiert sind.

So zeigen Sie einen Bericht über verbotene Programme im Informieren-Modus an:

1. Führen Sie die Aufgabe Kontrolle des Programmstarts im Informieren-Modus aus.
2. Wählen Sie die Option **Überwachung** → **Berichte** aus.
3. Wählen Sie in der Liste **Bericht über verbotene Anwendungen im Testmodus** aus und klicken Sie darauf.
   Ein Bericht wird erstellt.

4. Passen Sie die folgenden Einstellungen für Anfragen an:

   - Ein Schaubild mit den Top-10-Programmen, deren Start am häufigsten blockiert wurde.
   - Eine Übersichtstabelle mit den Fällen, in denen ein Programm blockiert wurde, mit Angabe des Namens der ausführbaren Datei, der Ursache, der Uhrzeit der Blockierung und der Anzahl der Geräte, auf denen sie stattgefunden hat.
   - Eine ausführliche Tabelle mit Daten zum Gerät, dem Dateipfad und den Kriterien für das Blockieren.

Um einen Bericht über verbotene Programme im Modus "Aktiv" anzuzeigen, gehen Sie wie folgt vor:

1. Führen Sie die Aufgabe Kontrolle des Programmstarts im Aktiv-Modus aus.
2. Wählen Sie die Option **Überwachung** → **Berichte** aus.
3. Wählen Sie in der Liste **Bericht über verbotene Anwendungen** aus und klicken Sie darauf.

   Ein Bericht wird erstellt.

Dieser Bericht enthält die gleichen Daten über Blockierungen wie der Bericht über verbotene Programme im Testmodus.

Lizenzverwaltung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für das Programm zusammenhängen.

Über den Endbenutzer-Lizenzvertrag

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

Lesen Sie den Endbenutzer-Lizenzvertrag sorgfältig, bevor Sie erste Schritte mit dem Programm ausführen.

Die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie, welche die Verarbeitung und Übertragung von Daten beschreibt, können Sie wie folgt lesen:

- Während der Installation von Kaspersky Embedded Systems Security.
- Während der Installation der Konsole für Kaspersky Embedded Systems Security.
- In der Datei „license.txt“, die zum Lieferumfang gehört.
- Auf der Website von Kaspersky (https://www.kaspersky.de/business/eula).

Sie akzeptieren den Endbenutzer-Lizenzvertrag, indem Sie sich während der Installation des Programms mit seinen Bedingungen einverstanden erklären. Falls Sie den Bedingungen des Endbenutzer-Lizenzvertrags nicht zustimmen, müssen Sie die Programminstallation abbrechen und dürfen das Programm nicht verwenden.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, welches auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

Eine gültige Lizenz berechtigt Sie gemäß den Bedingungen des Endbenutzer-Lizenzvertrags zur Nutzung des Programms und, falls erforderlich, zur Inanspruchnahme des Technischen Supports.

Der Umfang dieses Dienstes und der Zeitraum der Programmnutzung sind von dem Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Sie können das Programm auf zwei Arten aktivieren:

- Unter Verwendung einer Schlüsseldatei, die Ihnen die Nutzung des Programms unter einer kommerziellen Lizenz gewährt.
- Unter Verwendung eines Aktivierungscodes, um eine kommerzielle Lizenz zu kaufen.

Nach Ablauf der kommerziellen Lizenz sind nur noch die folgenden Programmkomponenten und Aufgaben verfügbar (ohne Datenbanken-Updates):

- Echtzeitschutz für Dateien
- Überwachung der Systemintegrität
- Benutzerdefinierte Aufgaben zur Untersuchung auf Befehl

Um alle Funktionen von Kaspersky Embedded Systems Security weiterhin nutzen zu können, müssen Sie die kommerzielle Lizenz verlängern. Es wird empfohlen, die Lizenz rechtzeitig vor dem Ablaufdatum zu verlängern. Nur so lässt sich ein optimaler Schutz gewährleisten.

Wenn der Lizenzschlüssel entfernt wird, wird das Programm weiterhin ausgeführt. Die Komponente „Überwachung der Systemintegrität“ ist weiterhin verfügbar. Die übrigen Komponenten und Aufgaben sowie die Datenbanken-Updates für Kaspersky Embedded Systems Security sind nicht mehr verfügbar. Gleiches passiert, wenn Kaspersky Ihre Lizenz zur Deny-Liste hinzufügt.

Über das Lizenzzertifikat

Das *Lizenzzertifikat* ist ein Dokument, das Sie zusammen mit der Schlüsseldatei oder dem Aktivierungscode erhalten.

Das Lizenzzertifikat enthält folgende Informationen über die vorliegende Lizenz:

- Lizenz-ID oder Bestellnummer.
- Informationen über den Benutzer, für den die Lizenz ausgestellt wurde
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- quantitative Beschränkungen im Hinblick auf die Lizenzierungseinheiten (beispielsweise Geräte, auf denen das Programm mit dieser Lizenz verwendet werden darf)
- Datum für den Beginn der Lizenzgültigkeit
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über den Schlüssel

Der *Schlüssel* ist eine Abfolge von Bits, mit deren Hilfe Sie das Programm aktivieren und anschließend gemäß den Bedingungen des Endbenutzer-Lizenzvertrags verwenden können. Der Schlüssel wird von den Kaspersky-Experten generiert.

Mithilfe einer Schlüsseldatei oder eines Aktivierungscodes können Sie einen Schlüssel zum Programm hinzufügen. Nachdem Sie den Schlüssel im Programm hinzugefügt haben, wird er auf der Programmoberfläche als unikale Folge aus Buchstaben und Ziffern angezeigt.

Kaspersky kann aufgrund von Verstößen gegen des Lizenzvertrags einen Schlüssel zur Deny-Liste hinzufügen. Wenn ein Schlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um das Programm zu nutzen.

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

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

Ein *Reserveschlüssel* gewährt das Recht auf die Programmnutzung, wird aber momentan nicht verwendet. Ein Reserveschlüssel wird automatisch aktiviert, sobald die mit dem aktiven Schlüssel verknüpfte Lizenz abläuft. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn ein aktiver Schlüssel vorhanden ist.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Ihnen von Kaspersky bereitgestellt wird. Mit der Schlüsseldatei wird ein Lizenzschlüssel für die Programmaktivierung hinzugefügt.

Nachdem Sie Kaspersky Embedded Systems Security gekauft haben, wird eine Schlüsseldatei an die von Ihnen angegebene E-Mail-Adresse gesendet.

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

Über den Aktivierungscode

Bei einem *Aktivierungscode* handelt es sich um eine eindeutige Folge aus 20 Buchstaben und Ziffern. Sie müssen einen Aktivierungscode eingeben, um einen Schlüssel zur Aktivierung von Kaspersky Embedded Systems Security hinzuzufügen. Der Aktivierungscode wird an Ihre angegebene E-Mail-Adresse gesendet, nachdem Sie Kaspersky Embedded Systems Security gekauft haben.

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

Bei Verlust des Aktivierungscodes nach der Installation des Programms kann dieser wiederherstellt werden. Ein Aktivierungscode kann beispielsweise für die Registrierung eines Kaspersky CompanyAccount erforderlich sein. Um Ihren Aktivierungscode wiederherzustellen, wenden Sie sich bitte an den Partner von Kaspersky Lab, von dem Sie die Lizenz erworben haben.

Vergleich der Programmfunktionalität abhängig vom Lizenztyp

Der Funktionsumfang von Kaspersky Embedded Systems Security ist vom Lizenztyp abhängig (siehe folgende Tabelle).

Vergleich der Funktionen von Kaspersky Embedded Systems Security

Funktion	Kaspersky Embedded Systems Security	Kaspersky Embedded Systems Security Compliance Edition
Echtzeitschutz für Dateien	✓	✓
Untersuchung auf Befehl	✓	✓
Kontrolle des Programmstarts	✓	✓
Gerätekontrolle	✓	✓
Firewall	✓	✓
Überwachung der Datei-Integrität	–	✓
Protokollanalyse	–	✓

Aktivieren des Programms mit einer Schlüsseldatei

Sie können Kaspersky Embedded Systems Security aktivieren, indem Sie eine Schlüsseldatei anwenden.

So aktivieren Sie Kaspersky Embedded Systems Security mithilfe einer Schlüsseldatei:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Lizenzverwaltung**.
2. Klicken Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** auf den Link **Schlüssel hinzufügen**.
3. Klicken Sie im angezeigten Fenster auf **Durchsuchen**.
4. Wählen Sie eine Schlüsseldatei mit der Dateiendung .key aus.

   Sie können einen Schlüssel auch als Reserveschlüssel hinzufügen. Um einen Schlüssel als Reserveschlüssel hinzuzufügen, aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**.

5. Klicken Sie auf **OK**.

Die ausgewählte Schlüsseldatei wird angewendet. In diesem Fall gelten folgende Bedingungen:

- Wenn bereits ein aktiver Schlüssel hinzugefügt wurde, um das Programm zu aktivieren, und Sie einen weiteren Schlüssel als aktiven Schlüssel hinzufügen, wird der zuvor hinzugefügte Schlüssel durch den neuen ersetzt. Der zuvor hinzugefügte Schlüssel wird entfernt.

- Wenn bereits ein Reserveschlüssel hinzugefügt wurde, um das Programm zu aktivieren, und Sie einen weiteren Schlüssel als Reserveschlüssel hinzufügen, wird der zuvor hinzugefügte Schlüssel durch den neuen ersetzt. Der zuvor hinzugefügte Reserveschlüssel wird entfernt.

- Wenn bereits ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt wurden, um das Programm zu aktivieren, und Sie einen neuen Schlüssel als aktiven Schlüssel hinzufügen, wird der zuvor hinzugefügte aktive Schlüssel durch den neuen ersetzt. Der Reserveschlüssel wird nicht entfernt.

Informationen über den hinzugefügten Schlüssel stehen im Knoten **Lizenzverwaltung** zur Verfügung.

Aktivieren des Programms mit einem Aktivierungscode

Um das Programm mit einem Aktivierungscode zu aktivieren, muss das geschützte Gerät mit dem Internet verbunden sein.

Sie können Kaspersky Embedded Systems Security aktivieren, indem Sie einen Aktivierungscode anwenden.

Bei der Aktivierung des Programms mit dieser Methode sendet Kaspersky Embedded Systems Security Daten an den Aktivierungsserver, um den eingegebenen Code zu überprüfen:

- Ist die Überprüfung des Aktivierungscodes erfolgreich, wird das Programm aktiviert.

- Schlägt die Überprüfung des Aktivierungscodes fehl, wird eine entsprechende Benachrichtigung angezeigt. In diesem Fall müssen Sie sich an den Softwarehändler wenden, von dem Sie Ihre Lizenz für Kaspersky Embedded Systems Security erworben haben.

- Wenn die für den Aktivierungscode zulässige Anzahl Aktivierungen überschritten wird, wird eine entsprechende Benachrichtigung angezeigt. Der Aktivierungsvorgang der Anwendung wird unterbrochen, und die Anwendung fordert Sie auf, den technischen Support zu kontaktieren.

Sie können Kaspersky Embedded Systems Security wie folgt aktivieren: mit einem Aktivierungscode über die Anwendungskonsole, oder indem Sie die Gruppenaufgabe *Aktivierung des Programms* über das Verwaltungs-Plug-in oder über das Web-Plug-in erstellen.

So aktivieren Sie Kaspersky Embedded Systems Security mit einem Aktivierungscode in der Programmkonsole:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Lizenzverwaltung**.

2. Klicken Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** auf den Link **Aktivierungscode hinzufügen**.

3. Geben Sie im folgenden Fenster im Feld **Aktivierungscode** den Aktivierungscode ein.

   - Wenn Sie den Aktivierungscode als Reserveschlüssel verwenden möchten, aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**.

   - Um Informationen über eine Lizenz anzuzeigen, klicken Sie auf die Schaltfläche **Lizenzinformationen anzeigen**. Die Informationen werden im Block **Lizenzinformationen** angezeigt.

4. Klicken Sie auf **OK**.

   Kaspersky Embedded Systems Security wird Informationen über die ausgewählten Objekttypen an den Administrationsserver übertragen.

Aufrufen von Informationen über die aktive Lizenz

Lizenzstatus anzeigen

Die Informationen zur aktuellen Lizenz werden im Bereich mit Details zum Knoten **Kaspersky Embedded Systems Security** der Programmkonsole angezeigt. Der Lizenzstatus kann die folgenden Werte haben:

- **Schlüsselstatus wird überprüft** – Kaspersky Embedded Systems Security überprüft die hinzugefügte Schlüsseldatei und wartet auf eine Antwort zum aktuellen Lizenzstatus.

- **Gültig bis** – Kaspersky Embedded Systems Security ist bis zum angegebenen Datum aktiviert. Der Status ist in folgenden Fällen gelb hervorgehoben:

  - Die Lizenz läuft in 30 Tagen ab und es wurde kein Reserveschlüssel hinzugefügt.

  - Der hinzugefügte Schlüssel wurde in die Deny-Liste aufgenommen und seine Blockierung steht unmittelbar bevor.

- **Das Programm ist nicht aktiviert** – Kaspersky Embedded Systems Security ist nicht aktiviert, da der Schlüssel nicht hinzugefügt wurde. Der Status ist rot hervorgehoben.

- **Lizenz ist abgelaufen** – Kaspersky Embedded Systems Security ist nicht aktiviert, da die Lizenz abgelaufen ist. Der Status ist rot hervorgehoben.

- **Endbenutzer-Lizenzvertrag wurde verletzt** – Kaspersky Embedded Systems Security ist nicht aktiviert, da die Bedingungen des Endbenutzer-Lizenzvertrags verletzt wurden. Der Status ist rot hervorgehoben.

- **Schlüssel steht auf Deny-List** – Der hinzugefügte Schlüssel ist blockiert und durch Kaspersky auf die Deny-Liste gesetzt, beispielsweise wenn der Schlüssel durch Unbefugte zur illegalen Programmaktivierung verwendet wurde. Der Status ist rot hervorgehoben.

Aufrufen von Informationen über die aktive Lizenz

Um die Informationen über die aktuelle Lizenz einzusehen,

Öffnen Sie in der Programmkonsolenstruktur den Knoten **Lizenzverwaltung**.

Im Ergebnisbereich des Knotens **Lizenzverwaltung** werden allgemeine Informationen über die aktive Lizenz angezeigt (s. Tabelle unten).

Allgemeine Lizenzinformationen im Knoten Lizenzverwaltung

Feld	Beschreibung
Status des Aktivierungscodes oder Schlüsselstatus	Status des Aktivierungscodes oder des Schlüssels: *Aktiver Schlüssel* oder *Reserve*.
Gültig bis	Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Lizenztyp	Lizenztyp: *Kommerzielle Lizenz*.
Aktivierungsstatus	Für den Aktivierungsstatus sind die folgenden Werte möglich: • **Angewendet** – wenn Sie das Programm mithilfe eines Schlüssels aktiviert haben. • **Aktivierung des Programms** – wenn Sie einen Aktivierungscode für die Aktivierung des Programms verwendet haben und der Aktivierungsprozess noch nicht abgeschlossen ist. Der Status ändert sich zu **Angewendet**, sobald die Aktivierung des Programms abgeschlossen ist und die Inhalte des Detailbereichs des Knotens aktualisiert wurden. • **Aktivierungsfehler** – wenn das Programm nicht aktiviert werden konnte. Die Ursache für das Fehlschlagen der Aktivierung finden Sie im Protokoll der Aufgabenausführung.
Schlüssel	Nummer des Schlüssels, mit dem Sie das Programm aktiviert haben.

Um Details über die Lizenz einzusehen,

öffnen Sie im Detailbereich des Knotens **Lizenzverwaltung** das Kontextmenü für die gewünschte Lizenz und wählen Sie **Eigenschaften** aus.

Detaillierter Lizenzinformationen im Fenster „Eigenschaften <Schlüsselnummer>“

Feld	Beschreibung
Schlüssel	Nummer des Schlüssels, mit dem Sie das Programm aktiviert haben.
Programm	Name des Programms, das mit dem hinzugefügten Schlüssel aktiviert wurde.
Lizenztyp	Lizenztyp: kommerziell oder Probe
Gültigkeitsdauer der Lizenz	Anzahl der Tage, für die Lizenz gültig ist (ab dem Aktivierungsdatum des Programms).
Aktivierungsdatum	Datum, an dem der Schlüssel zum Programm hinzugefügt wurde.
Gültig bis	Ablaufdatum der Lizenz, die mit dem aktiven Schlüssel verknüpft ist. Wenn Sie das Programm auf Basis eines unbefristeten Abonnements aktivieren, wird der Feldwert *Unbefristet* angezeigt. Wenn Kaspersky Embedded Systems Security das Ablaufdatum der Lizenz nicht ermitteln kann, wird der Wert *Unbekannt* angezeigt.
Läuft ab in (Tagen)	Anzahl der Tage bis zum Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Anspruch auf Technischen Support	Informationen darüber, ob Kaspersky oder seine Partner den Kunden gemäß den Lizenzbedingungen technische Unterstützung bieten.
Support-Informationen	Kontaktinformationen von Kaspersky oder seines Partners, der technischen Support leistet. Dieses Feld kann leer sein, wenn kein technischer Support geleistet wird.
Informationen zum Eigentümer	Informationen zum Lizenznehmer: Name des Kunden und Name des Unternehmens, für den bzw. das die Lizenz erworben wurde.
Lizenzinformationen	Nummer und Typ der aktuellen Lizenz.
Funktionalität	Programmfunktionen, die im Rahmen der Lizenz verfügbar sind.

Verlängerung der Lizenz

Standardmäßig benachrichtigt Sie Kaspersky Embedded Systems Security, wenn die Lizenz noch 30 Tage abläuft.

Sie können die Lizenz schon vor dem Ablaufdatum verlängern, indem Sie einen Reserveschlüssel hinzufügen. So vermeiden Sie, dass das Gerät nach Ablauf der Laufzeit der aktuellen Lizenz bis zur Aktivierung des Programms mit der neuen Lizenz ungeschützt ist.

So verlängern Sie eine Lizenz:

1. Besorgen Sie sich einen neuen Aktivierungscode oder eine Schlüsseldatei für das Programm.
2. Wählen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
3. Führen Sie im Ergebnisfenster des Knotens **Lizenzverwaltung** eine der folgenden Aktionen aus:
   - Wenn Sie die Lizenz mithilfe einer Schlüsseldatei verlängern möchten:
     a. Klicken Sie auf den Link **Schlüssel hinzufügen**.
     b. Klicken Sie im angezeigten Fenster auf **Durchsuchen**.
     c. Wählen Sie eine neue Schlüsseldatei mit der Dateiendung .key aus.
     d. Aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**.
   - Wenn Sie die Lizenz mithilfe eines Aktivierungscodes verlängern möchten:
     a. Klicken Sie auf den Link **Aktivierungscode hinzufügen**.
     b. Geben Sie den erworbenen Aktivierungscode im erscheinenden Fenster ein.
     c. Aktivieren Sie das Kontrollkästchen **Als zusätzlichen Schlüssel verwenden**.

   Für die Übernahme des Aktivierungscodes ist eine Internetverbindung erforderlich.
4. Klicken Sie auf **OK**.

Der Reserveschlüssel wird hinzugefügt und nach Ablauf der aktiven Lizenz für Kaspersky Embedded Systems Security automatisch angewendet.

Löschen des Schlüssels

Wenn Sie den Reserveschlüssel entfernen, können Sie ihn durch die erneute Anwendung der Schlüsseldatei wiederherstellen.

So entfernen Sie den zuvor hinzugefügten Schlüssel:

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
2. Wählen Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** in der Tabelle mit Informationen über die hinzugefügten Schlüssel den Schlüssel aus, den Sie entfernen möchten.

3. Wählen Sie im Kontextmenü der Zeile mit den Informationen über den ausgewählten Schlüssel den Punkt **Löschen** aus.

4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um das Löschen des Schlüssels zu bestätigen.

Der ausgewählte Schlüssel wird gelöscht.

Starten und Beenden von Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen darüber, wie Kaspersky Embedded Systems Security gestartet und beendet wird und wie die Konsole für Kaspersky Embedded Systems Security und das Verwaltungs-Plug-ins der Kaspersky Security Center-Verwaltungskonsole gestartet werden.

Programm starten und beenden

Nach der Installation von Kaspersky Embedded Systems Security auf dem Benutzercomputer wird das Programm automatisch gestartet. Künftig wird Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security geladen, wenn das Betriebssystem bereits gestartet wurde, so wird das Schutzniveau des Computers dadurch nicht negativ beeinflusst.

So konfigurieren Sie den automatischen Programmstart (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Programmeinstellungen → Sicherheit und Zuverlässigkeit** aus und klicken Sie auf **Einstellungen**.
4. Aktivieren oder deaktivieren Sie auf der Registerkarte **Sicherheit** das Kontrollkästchen **Programm beim Hochfahren des Computers starten (empfohlen)**, um den automatischen Start des Programms zu aktivieren oder zu deaktivieren.
5. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den automatischen Programmstart (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Programmeinstellungen → Sicherheit und Zuverlässigkeit**.

5. Klicken Sie auf **Anpassen**.

   Das Fenster **Sicherheit und Zuverlässigkeit** wird geöffnet.

6. Verwenden Sie das Kontrollkästchen **Programm beim Hochfahren des Computers starten (empfohlen)**, um den automatischen Start des Programms zu aktivieren oder zu deaktivieren.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den automatischen Programmstart (in der Anwendungskonsole)

1. wählen Sie in der Programmkonsolenstruktur den Knoten **Kaspersky Embedded Systems Security** aus.

2. Wählen Sie im Kontextmenü des Knotens den Punkt **Eigenschaften des Programms** aus.

3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheitseinstellungen** aus.

4. Verwenden Sie das Kontrollkästchen **Programm beim Hochfahren des Computers starten (empfohlen)**, um den automatischen Start des Programms zu aktivieren oder zu deaktivieren.

5. Speichern Sie die vorgenommenen Änderungen.

Sie können Kaspersky Embedded Systems Security starten und beenden, wenn Sie auf dem geschützten Gerät zur Administratorengruppe gehören.

So aktivieren oder beenden Sie das Programm (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.

2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.

3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.

4. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.

5. Wählen Sie in der Liste der auf dem Computer installierten Kaspersky-Programme den Punkt **Kaspersky Embedded Systems Security für Windows (4.0.1)** aus.

6. Führen Sie einen der folgenden Schritte 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 aktivieren oder deaktivieren Sie das Programm (in der Kaspersky Security Center 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 Embedded Systems Security starten oder beenden möchten.

   Das Eigenschaftenfenster des Computers wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Aktivieren Sie das Kontrollkästchen für **Kaspersky Embedded Systems Security für Windows (4.0.1)**.
5. Klicken Sie auf die Schaltfläche **Starten** oder **Stoppen**.

So aktivieren oder beenden Sie das Programm (in der Anwendungskonsole)

1. So beenden Sie Kaspersky Embedded Systems Security:

   a. Öffnen Sie die Programmkonsole.

   > Das Benutzerkonto muss über Berechtigungen für den Zugriff auf die Funktion **Programm beenden** verfügen.

   b. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.

   c. Wählen Sie den Punkt **Programm beenden**.

   d. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um das Beenden des Programms zu bestätigen.

   Das Programm wird beendet.
2. So starten Sie **Kaspersky Embedded Systems Security**:

   a. Führen Sie im Installationsordner der Programmkonsole auf dem geschützten Gerät die Datei avpui.exe aus. Die Datei befindet sich standardmäßig im Ordner C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security Console.

   Das Fenster **Geschütztes Gerät auswählen** wird geöffnet.

   b. Wenn Kaspersky Embedded Systems Security und die Anwendungskonsole auf demselben Computer installiert sind, wählen Sie **Lokaler Computer (Computer, auf dem die Programmkonsole ausgeführt wird)** aus.

   c. Wenn Kaspersky Embedded Systems Security und die Anwendungskonsole auf verschiedenen Computern installiert sind:

      1. Wählen Sie den Punkt **Anderes Gerät**.
      2. Klicken Sie auf **Durchsuchen** und geben Sie den Namen des Computers an, auf dem das Programm installiert ist.

3. Geben Sie den Port für die Verbindung zu dem Computer an, auf dem das Programm installiert ist:

   - **Mittels Windows-Anmeldedaten**. Ein Port für die Verbindung mit Windows-Anmeldeinformationen. Der Standardwert ist 13032.

   - **Mittels Anmeldedaten von manuell erstellten Benutzern**. Ein Port für die Verbindung mit den Anmeldedaten manuell erstellter Benutzer. Der Standardwert ist 13031.

d. Aktivieren Sie bei Bedarf die Funktion **Authentifizierung verwenden** und geben Sie die Anmeldedaten ein, um die Programmkonsole mit dem Computer zu verbinden, auf dem das Programm installiert ist. Das angegebene Benutzerkonto muss über Berechtigungen für den Zugriff auf die Funktionen **Einstellungen lesen** und **Remote-Verbindung zum Programm** auf dem Computer verfügen, auf dem das Programm installiert ist.

e. Klicken Sie auf **Dienst zur Anwendungsverwaltung**.

f. Klicken Sie im angezeigten Fenster auf **Start**.

   Das Programm wird gestartet.

Das Fenster **Geschütztes Gerät auswählen** wird auch angezeigt, wenn die Verbindung zu dem Computer, auf dem das Programm installiert ist, unterbrochen wird oder wenn der KESS-Dienst fehlschlägt. Sie können den KESS-Dienst wiederherstellen, indem Sie auf **Starten** klicken.

Sie können das Programm auch über die Befehlszeile starten oder 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 Embedded Systems Security vorübergehend deaktiviert.

Der Programmstatus wird mit dem Programmsymbol im Infobereich der Taskleiste angezeigt.

- 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. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.

2. Wählen Sie den Punkt **Schutz anhalten**.

3. Wählen Sie eine der vorgeschlagenen Varianten aus:

   - **Anhalten für bestimmten Zeitraum <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 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.

   Kaspersky Embedded Systems Security hält alle Schutz- und Kontrollkomponenten an, die in der Richtlinie kein Vorhängeschloss (🔒) haben.

Gehen Sie folgendermaßen vor, um den Schutz und die Kontrolle des Computers fortzusetzen:

1. Öffnen Sie das Kontextmenü des Programmsymbols, 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.

Kompaktes Diagnosefenster

Dieser Abschnitt beschreibt die Verwendung der kompakten Diagnose-Benutzeroberfläche.

Über das kompakte Diagnosefenster

Die Komponente „Kompaktes Diagnosefenster“ wird gemeinsam mit der Komponente „Taskleistensymbol“ unabhängig von der Programmkonsole installiert bzw. deinstalliert. Sie kann verwendet werden, wenn die Programmkonsole nicht auf dem geschützten Gerät installiert ist. Die kompakte Diagnoseschnittstelle wird über das Symbol in der Taskleiste oder durch Ausführen von avpui.exe aus dem Anwendungsordner auf dem geschützten Gerät gestartet.

In der kompakten Diagnoseschnittstelle können Sie Folgendes tun:

- Das Fenster **Über das Programm** mit der Liste der installierten Updates und verfügbaren Patches öffnen.
- Informationen über den allgemeinen Programmstatus überprüfen.
- Eingetretene Sicherheitsereignisse überprüfen.
- Aktuelle Aktivitäten auf dem geschützten Gerät überprüfen.
- Das Erstellen von Dump-Dateien und Protokolldateien starten und stoppen.
- Öffnen Sie die Programmkonsole.

Die kompakte Diagnoseschnittstelle ist auch dann verfügbar, wenn der Zugriff auf die Funktionen von Kaspersky Embedded Systems Security passwortgeschützt ist. Es ist kein Kennwort erforderlich.

Die Komponente der kompakten Diagnoseschnittstelle kann nicht über Kaspersky Security Center konfiguriert werden.

Status von Kaspersky Embedded Systems Security mithilfe des kompakten Diagnosefensters überprüfen

Um den Programmstatus mithilfe des kompakten Diagnosefensters anzuzeigen:

1. Öffnen Sie das kompakte Diagnosefenster auf eine der folgenden Arten:
   - Führen Sie im Installationsordner des Programms auf dem geschützten Gerät die Datei avpui.exe aus. Die Datei befindet sich standardmäßig im Ordner C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.
   - Klicken Sie auf das Programmsymbol im Infobereich der Taskleiste.

2. Überprüfen Sie den aktuellen Status des Schlüssels sowie der Aufgaben zum Echtzeit-Computerschutz und Update im Abschnitt **Schutzstatus**. Verschiedene Farben vermitteln dem Benutzer den aktuellen Schutzstatus (s. Tabelle unten).

Farbliche Kennzeichnung im Fenster der kompakten Diagnose-Benutzeroberfläche

Abschnitt	Status
Echtzeitschutz-Status	Die Leiste ist *grün*, wenn die folgenden Bedingungen erfüllt sind: • Die Komponente Echtzeitschutz für Dateien ist aktiviert. • Die Komponente Kontrolle des Programmstarts wird im **Verbieten**-Modus ausgeführt.
	Die Leiste ist *gelb*, wenn eine oder mehrere der folgenden Bedingungen zutreffen: • Die Komponente Echtzeitschutz für Dateien ist deaktiviert. • Die Komponente Kontrolle des Programmstarts wird im **Informieren**-Modus ausgeführt.
	Die Leiste ist *rot*, wenn beide der folgenden Bedingungen zutreffen: • Die Komponente Echtzeitschutz für Dateien ist deaktiviert oder nicht installiert. • Die Komponente Kontrolle des Programmstarts ist nicht installiert oder wird im **Informieren**-Modus ausgeführt.
Lizenzverwaltung	Die Leiste ist *grün*, wenn die aktuelle Lizenz gültig ist.
	Die Leiste ist *gelb*, wenn eines der folgenden Ereignisse eingetreten ist: • *Der Lizenzstatus wird geprüft.* • *Die Restlaufzeit der Lizenz beträgt noch 14 Tage, und es wurde kein Reserveschlüssel oder Aktivierungscode hinzugefügt.* • *Der hinzugefügte Schlüssel wurde in die Deny-Liste aufgenommen und seine Blockierung steht unmittelbar bevor.*
	Die Leiste ist *rot*, wenn eines der folgenden Ereignisse eingetreten ist: • *Das Programm ist nicht aktiviert.* • *Lizenz ist abgelaufen.* • *Endbenutzer-Lizenzvertrag wurde verletzt.* • *Schlüssel steht auf Deny-List.*
Aktualisieren	Die Leiste ist *grün*, wenn die Programm-Datenbanken aktuell sind.
	Die Leiste ist *gelb*, wenn die Programm-Datenbanken veraltet sind.
	Die Leiste ist *rot*, wenn die Programm-Datenbanken stark veraltet sind.

Überprüfung der Sicherheitsereignis-Statistik

Im Abschnitt **Statistik** werden alle Sicherheitsereignisse angezeigt. Jede Schutzaufgaben-Statistik wird in einem separaten Block angezeigt, in dem die Anzahl der Vorfälle sowie Datum und Uhrzeit des letzten Vorfalls angegeben sind. Wenn ein Ereignis registriert wird, wechselt die Blockfarbe zu rot.

So zeigen Sie die Statistik an:

1. Öffnen Sie das kompakte Diagnosefenster auf eine der folgenden Arten:

   - Führen Sie im Installationsordner des Programms auf dem geschützten Gerät die Datei avpui.exe aus. Die Datei befindet sich standardmäßig im Ordner C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.

   - Klicken Sie auf das Programmsymbol im Infobereich der Taskleiste.

2. Wechseln Sie zum Abschnitt **Statistik**.

3. Überprüfen Sie die Sicherheitsvorfälle für die Schutzaufgaben.

Aktuelle Programmaktivität überprüfen

Um die aktuelle Programmaktivität auf dem geschützten Gerät zu überprüfen, gehen Sie wie folgt vor:

1. Öffnen Sie das kompakte Diagnosefenster auf eine der folgenden Arten:
    - Führen Sie im Installationsordner des Programms auf dem geschützten Gerät die Datei avpui.exe aus. Die Datei befindet sich standardmäßig im Ordner C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.
    - Klicken Sie auf das Programmsymbol im Infobereich der Taskleiste.
2. Wechseln Sie zum Abschnitt **Aktuelle Anwendungsaktivität**.

Für die Darstellung der Programmaktivität werden verschiedene Farben verwendet:

- Im Abschnitt **Aufgaben**:
    - *Grün*. Es gibt keine Bedingungen, die Gelb oder Rot erfordern würden.
    - *Gelb*. Untersuchung wichtiger Bereiche liegt lange zurück.
    - *Rot*. Mindestens eine der folgenden Bedingungen trifft zu:
        - Es wurden keine Aufgaben gestartet und der Zeitplan für den Aufgabenstart wurde für keine Aufgabe konfiguriert.
        - Fehler beim Programmstart werden als kritische Ereignisse protokolliert.
- Im Abschnitt **Kaspersky Security Network**:
    - *Grün*. Die Aufgabe **KSN-Nutzung** wird gestartet.
    - *Gelb*. Die KSN-Erklärung wurde akzeptiert, aber die Aufgabe wurde nicht gestartet.

Anwendungsnachverfolgung und die Aufzeichnung von Speicherauszugsdateien konfigurieren

So konfigurieren Sie die Anwendungsnachverfolgung und die Aufzeichnung von Speicherauszugsdateien:

1. Öffnen Sie das kompakte Diagnosefenster auf eine der folgenden Arten:
    - Führen Sie im Installationsordner des Programms auf dem geschützten Gerät die Datei avpui.exe aus. Die Datei befindet sich standardmäßig im Ordner C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0.
    - Klicken Sie auf das Programmsymbol im Infobereich der Taskleiste.
2. Wechseln Sie zum Abschnitt **Diagnose von Störungen**.

3. Verwenden Sie das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Schutz für Dump-Dateien und Protokolldateien zu aktivieren oder zu deaktivieren.

   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.

4. Verwenden Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei schreiben**, um die Ablaufverfolgung von Programmvorgängen zu aktivieren oder zu deaktivieren.

   Die Ablaufverfolgung von Programmvorgängen ist standardmäßig deaktiviert.

5. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Klicken Sie dazu auf **Durchsuchen** und wählen Sie den gewünschten Ordner aus.

   > Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

   Für die Protokolldateien erstellt Kaspersky Embedded Systems Security im ausgewählten Ordner einen Unterordner namens logs-Kaspersky Embedded Systems Security-<uid>, wobei <uid> eine eindeutige Protokoll-ID aus 8 Zeichen ist.

6. Wählen Sie die Protokollierungsstufe für die Debug-Informationen aus:

   - **Normal** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie Informationen über den normalen Betrieb des Programms gespeichert (Standard).
   - **Kritisch** bedeutet: In der Ablaufverfolgungsdatei werden nur Meldungen über schwerwiegende Fehler gespeichert.
   - **Diagnose** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler sowie Warnungen gespeichert.
   - **Wichtig** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie zusätzliche Informationen gespeichert.
   - **Detailliert** bedeutet: In der Ablaufverfolgungsdatei werden alle Informationen über den Betrieb des Programms gespeichert.

   Ein Mitarbeiter des technischen Supports bestimmt den Detailgrad, der zur Lösung möglicher Probleme erforderlich ist.

7. Um alte Protokolldateien zu löschen, aktivieren Sie die Funktionalität **Älteste Protokolldateien entfernen**.

   Wenn diese Funktionalität aktiviert ist, können Sie die maximale Größe und die Anzahl der Protokolldateien anpassen:

   a. Geben Sie die **Maximale Größe einer Protokolldatei (MB)** an.

      Verfügbare Werte: von 1 bis 4095 MB. Der Standardwert ist 100 MB.

   b. Geben Sie die **Maximale Anzahl der Protokolldateien** an.

      Verfügbare Werte: von 1 bis 999. Der Standardwert ist 5.

8. Verwenden Sie das Kontrollkästchen **Bei Absturz eine Dump-Datei in diesem Ordner erstellen**, um die Ablaufverfolgung von Programmvorgängen zu aktivieren oder zu deaktivieren.

   Die Speicher-Dump-Aufzeichnung ist standardmäßig deaktiviert.

9. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Klicken Sie dazu auf **Durchsuchen** und wählen Sie den gewünschten Ordner aus.

   Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

10. Klicken Sie auf **Übernehmen**.

Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security

Der Selbstschutz verhindert Aktionen von anderen Programmen, die den Betrieb von Kaspersky Embedded Systems Security stören können. Die Selbstschutzmechanismen schützen das Programm davor, dass seine Ordner, Speicherprozesse und Systemregistrierungseinträge gelöscht oder geändert werden. Kaspersky Embedded Systems Security unterstützt die Microsoft-Technologie Antimalware Protected Process Light (AM-PPL), die Programmprozesse vor schädlichen Aktivitäten schützt. Außerdem ermöglicht das Programm die Verwaltung von Benutzerzugriffsberechtigungen für die Programmfunktionen und von separaten Berechtigungen für den Programmdienst.

Selbstschutz-Mechanismus aktivieren und deaktivieren

Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security, die von nicht vertrauenswürdigen übergeordneten Prozessen initiiert wurden.

Die Selbstschutzmechanismen von Kaspersky Embedded Systems Security sind standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie den Selbstschutz (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Anwendungseinstellungen**.
4. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheit** aus.
6. Verwenden Sie im Block **Selbstschutz** das Kontrollkästchen **Programmprozesse vor externen Bedrohungen schützen**, um den Selbstschutz zu aktivieren oder zu deaktivieren.
7. Verriegeln Sie das Vorhängeschloss , um die Richtlinie auf die Computer anzuwenden.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie den Selbstschutz (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und klicken Sie im Ergebnisbereich auf den Link **Eigenschaften des Programms**.
2. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheitseinstellungen** aus.
3. Verwenden Sie im Block **Selbstschutz** das Kontrollkästchen **Programmprozesse vor externen Bedrohungen schützen**, um den Selbstschutz zu aktivieren oder zu deaktivieren.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie den Selbstschutz (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf **Anpassen**.

   Das Fenster **Sicherheit und Zuverlässigkeit** wird geöffnet.
6. Verwenden Sie im Block **Selbstschutz** das Kontrollkästchen **Programmprozesse vor externen Bedrohungen schützen**, um den Selbstschutz zu aktivieren oder zu deaktivieren.
7. Verriegeln Sie das Vorhängeschloss, um die Richtlinie auf die Computer anzuwenden.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Unterstützung der AM-PPL-Technologie

Kaspersky Embedded Systems Security unterstützt die Technologie Antimalware Protected Process Light (im Folgenden „AM-PPL") von Microsoft. AM-PPL schützt die Prozesse von Kaspersky Embedded Systems Security vor schädlichen Aktionen (z. B. Beenden des Programms). AM-PPL erlaubt nur den Start von vertrauenswürdigen Prozessen. Die Prozesse von Kaspersky Embedded Systems 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 Embedded Systems 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.

Das Programm registriert den Dienst „Kaspersky Embedded Systems Security“ (AVP) und den Dienst „Kaspersky Seamless Update Service“ (AVPSUS). Die AM-PPL-Technologie schützt nur den AVP-Dienst.

Lassen Sie die AM-PPL-Technologie immer aktiviert. AM-PPL ist eine wichtige Komponente für den Schutz des Betriebssystems. Eine Deaktivierung von AM-PPL ist nur in einer separaten Testumgebung zulässig, wenn Fehler im Programm behoben werden sollen.

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 Embedded Systems Security befindet.

4. Um die Unterstützung der AM-PPL-Technologie zu aktivieren, führen Sie den folgenden Befehl aus:

   ```
   klpsm.exe enable
   ```

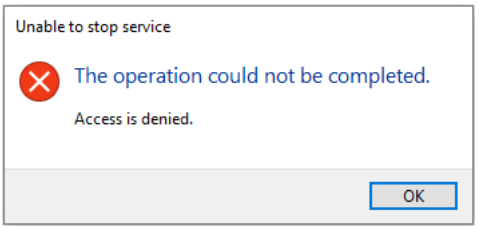
5. Um die Unterstützung der AM-PPL-Technologie zu deaktivieren, führen Sie den folgenden Befehl aus:

   ```
   klpsm.exe disable
   ```

6. Kaspersky Embedded Systems Security neu starten

7. Setzen Sie das Modul für den Selbstschutz des Programms fort.

Wenn künftig ein Benutzer versucht, den AVP-Dienst zu beenden, wird ein Systemfenster mit einer Fehlermeldung angezeigt. Der Benutzer kann die App-Dienste nur über die Oberfläche von Kaspersky Embedded Systems Security verwalten.



Fehler beim Zugriff auf App-Dienste

Betriebssystemdienste schützen

Sie können die Funktionalität Betriebssystemdienste schützen verwenden, um Drittanbieter-Programmen die Beeinflussung von Betriebssystemdiensten zu erlauben oder zu verbieten.

So aktivieren oder deaktivieren Sie den Schutz für Betriebssystemdienste (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Anwendungseinstellungen**.
4. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheit** aus.
6. Verwenden Sie das Kontrollkästchen **Betriebssystemdienste schützen**, um den Schutz für die Betriebssystemdienste zu aktivieren oder zu deaktivieren.

   Wenn der Schutz für die Betriebssystemdienste aktiviert ist, dürfen Drittanbieter-Programme die Prozesse des Betriebssystems nicht beeinflussen.

   Wenn der Schutz für die Betriebssystemdienste deaktiviert ist, können Drittanbieter-Programme die Prozesse des Betriebssystems beeinflussen.

   Nachdem Sie die Funktion aktiviert oder deaktiviert haben, müssen Sie den Computer neu starten, damit die Änderungen übernommen werden.
7. Verriegeln Sie das Vorhängeschloss , um die Richtlinie auf die Computer anzuwenden.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie den Schutz für Betriebssystemdienste (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und klicken Sie im Ergebnisbereich auf den Link **Eigenschaften des Programms**.
2. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheitseinstellungen** aus.
3. Verwenden Sie das Kontrollkästchen **Betriebssystemdienste schützen**, um den Schutz für die Betriebssystemdienste zu aktivieren oder zu deaktivieren.

   Wenn der Schutz für die Betriebssystemdienste aktiviert ist, dürfen Drittanbieter-Programme die Prozesse des Betriebssystems nicht beeinflussen.

   Wenn der Schutz für die Betriebssystemdienste deaktiviert ist, können Drittanbieter-Programme die Prozesse des Betriebssystems beeinflussen.

   Nachdem Sie die Funktion aktiviert oder deaktiviert haben, müssen Sie den Computer neu starten, damit die Änderungen übernommen werden.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie den Schutz für Betriebssystemdienste (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf **Anpassen**.

   Das Fenster **Sicherheit und Zuverlässigkeit** wird geöffnet.
6. Verwenden Sie das Kontrollkästchen **Betriebssystemdienste schützen**, um den Schutz für die Betriebssystemdienste zu aktivieren oder zu deaktivieren.

   Wenn der Schutz für die Betriebssystemdienste aktiviert ist, dürfen Drittanbieter-Programme die Prozesse des Betriebssystems nicht beeinflussen.

   Wenn der Schutz für die Betriebssystemdienste deaktiviert ist, können Drittanbieter-Programme die Prozesse des Betriebssystems beeinflussen.

   Nachdem Sie die Funktion aktiviert oder deaktiviert haben, müssen Sie den Computer neu starten, damit die Änderungen übernommen werden.
7. Verriegeln Sie das Vorhängeschloss, um die Richtlinie auf die Computer anzuwenden.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Benutzerberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security konfigurieren

Standardmäßig sind alle Funktionen von Kaspersky Embedded Systems Security für die folgenden Personen verfügbar: Mitglieder der Administratorengruppe auf dem geschützten Gerät, Mitglieder der ESS-Administratorengruppe, die bei der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät erstellt wurde, sowie für die Gruppe „SYSTEM".

Wenn ein Benutzer nicht in die Liste der Benutzer von Kaspersky Embedded Systems Security registriert ist, kann er die Programmkonsole nicht öffnen.

Sie können den Zugriff auf spezielle Funktionen von Kaspersky Embedded Systems Security für bestimmte Benutzer oder Benutzergruppen erlauben oder verbieten.

Über Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security

Zugriffsrechte	Beschreibung
Aufgaben verwalten	Berechtigung zum Starten, Beenden, Anhalten bzw. Fortsetzen der Aufgaben von Kaspersky Embedded Systems Security.
Aufgaben erstellen und löschen	Berechtigung zum Erstellen und Löschen von Aufgabe zur Untersuchung auf Befehl.
Einstellungen bearbeiten	Berechtigungen: • Einstellungen von Kaspersky Embedded Systems Security aus einer Konfigurationsdatei importieren • Programmeinstellungen bearbeiten

Zugriffsrechte	Beschreibung
Einstellungen lesen	Berechtigungen: • Allgemeine Einstellungen und Aufgabeneinstellungen für Kaspersky Embedded Systems Security anzeigen. • Exportieren der Einstellungen von Kaspersky Embedded Systems Security in eine Konfigurationsdatei. • Einstellungen für Protokolle der Aufgabenausführung, für das Systemaudit-Protokoll und für Benachrichtigungen anzeigen.
Speicher verwalten	Berechtigungen: • Objekte in Quarantäne verschieben • Objekte aus der Quarantäne und dem Backup löschen • Objekte aus der Quarantäne und dem Backup wiederherstellen
Protokolle verwalten	Berechtigung zum Löschen von Protokollen der Aufgabenausführung und zum Leeren des Systemaudit-Protokolls
Protokolle lesen	Berechtigung zur Anzeige der Ereignisse von Anti-Virus in Protokollen der Aufgabenausführung und im Systemaudit-Protokoll.
Statistik abrufen	Berechtigung zum Anzeigen der Statistik für die einzelnen Aufgaben von Kaspersky Embedded Systems Security.
App-Lizenzen verwalten	Berechtigung zum Aktivieren von Kaspersky Embedded Systems Security.
Die App deinstallieren	Berechtigung zum Deinstallieren von Kaspersky Embedded Systems Security.
Leserechte	Berechtigung zum Anzeigen der Liste der Benutzer von Kaspersky Embedded Systems Security und der Benutzerzugriffsrechte.
Bearbeitungsrechte	Berechtigungen: • Liste der Benutzer ändern, die Zugriff auf die Programmverwaltung haben • Benutzerzugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security bearbeiten
Remote-Verbindung zum Programm	Berechtigung, mithilfe der Anwendungskonsole eine Remote-Verbindung zum Programm herzustellen. Für den Fernzugriff muss der Benutzer außerdem über Zugriffsrechte auf die Funktion **Einstellungen lesen** verfügen.
Programm beenden	Berechtigung, das Programm mithilfe der Anwendungskonsole zu beenden.
Richtlinie für Kaspersky Security Center deaktivieren	Berechtigung, die Richtlinie für Kaspersky Security Center zu deaktivieren.
Einstellungen exportieren	Möglichkeit zum Exportieren der Einstellungen von Kaspersky Embedded Systems Security.
Diagnose von Störungen bearbeiten	Möglichkeit zum Konfigurieren der Programm-Ablaufverfolgung und der Aufzeichnung von Speicherauszugsdateien.

So konfigurieren Sie die Benutzerberechtigungen zur Verwaltung von Kaspersky Embedded Systems Security (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Zusätzlich** aus.
4. Klicken Sie im Abschnitt **Benutzerberechtigungen für den Zugriff auf die Programmverwaltung** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Aktivieren Sie in diesem Fenster das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden** und legen Sie ein Kennwort für das Benutzerkonto KLAdmin fest. Das Benutzerkonto wird automatisch zur Liste der Benutzerkonten hinzugefügt.

6. Fügen Sie bei Bedarf Benutzerkonten hinzu, denen Sie Zugriff auf die Programmverwaltung gewähren möchten. Klicken Sie dazu in der Tabelle der Benutzerkonten auf **Hinzufügen**.

   Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.

7. Wählen Sie aus, mit welcher Methode die Benutzer hinzugefügt werden sollen:

   - **Benutzer oder Gruppe aus Active Directory auswählen**. Sie können Kaspersky Embedded Systems 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 **Programm beenden** erteilen.

   - **Benutzer/Benutzergruppe manuell hinzufügen**. 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 **Protokolle lesen** 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.

     Um einen Benutzer oder eine Benutzergruppe manuell hinzuzufügen, müssen Sie den Kennwortschutz aktivieren.

8. Wählen Sie einen Benutzer oder eine Benutzergruppe aus, dem bzw. der Sie die Verwaltung des Programms erlauben möchten.

9. Konfigurieren Sie in der Liste **Berechtigungen** die Benutzerzugriffsberechtigungen für die Programmfunktionen.

10. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Benutzerberechtigungen zur Verwaltung von Kaspersky Embedded Systems Security (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Benutzerberechtigungen für den Zugriff auf die Programmverwaltung** aus.

2. Dadurch wird ein Fenster geöffnet. Aktivieren Sie in diesem Fenster das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden** und legen Sie ein Kennwort für das Benutzerkonto KLAdmin fest. Das Benutzerkonto wird automatisch zur Liste der Benutzerkonten hinzugefügt.

3. Fügen Sie bei Bedarf Benutzerkonten hinzu, denen Sie Zugriff auf die Programmverwaltung gewähren möchten. Klicken Sie dazu in der Tabelle der Benutzerkonten auf **Hinzufügen**.

   Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.

4. Wählen Sie aus, mit welcher Methode die Benutzer hinzugefügt werden sollen:

   - **Benutzer oder Gruppe aus Active Directory auswählen**. Sie können Kaspersky Embedded Systems 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 **Programm beenden** erteilen.

   - **Benutzer/Benutzergruppe manuell hinzufügen**. 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 **Protokolle lesen** 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.

     Um einen Benutzer oder eine Benutzergruppe manuell hinzuzufügen, müssen Sie den Kennwortschutz aktivieren.

5. Wählen Sie einen Benutzer oder eine Benutzergruppe aus, dem bzw. der Sie die Verwaltung des Programms erlauben möchten.

6. Konfigurieren Sie in der Liste **Berechtigungen** die Benutzerzugriffsberechtigungen für die Programmfunktionen.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Benutzerzugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Zusätzlich → Benutzerberechtigungen für den Zugriff auf die Programmverwaltung** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Dadurch wird ein Fenster geöffnet. Aktivieren Sie in diesem Fenster das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden** und legen Sie ein Kennwort für das Benutzerkonto KLAdmin fest. Das Benutzerkonto wird automatisch zur Liste der Benutzerkonten hinzugefügt.

6. Fügen Sie bei Bedarf Benutzerkonten hinzu, denen Sie Zugriff auf die Programmverwaltung gewähren möchten. Klicken Sie dazu in der Tabelle der Benutzerkonten auf **Hinzufügen**.

   Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.

7. Wählen Sie aus, mit welcher Methode die Benutzer hinzugefügt werden sollen:

   - **Benutzer oder Gruppe aus Active Directory auswählen**. Sie können Kaspersky Embedded Systems 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 **Programm beenden** erteilen.

   - **Benutzer/Benutzergruppe manuell hinzufügen**. 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 **Protokolle lesen** 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.

     Um einen Benutzer oder eine Benutzergruppe manuell hinzuzufügen, müssen Sie den Kennwortschutz aktivieren.

8. Wählen Sie einen Benutzer oder eine Benutzergruppe aus, dem bzw. der Sie die Verwaltung des Programms erlauben möchten.

9. Konfigurieren Sie in der Liste **Berechtigungen** die Benutzerzugriffsberechtigungen für die Programmfunktionen.

10. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

Benutzerzugriffsberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security Service konfigurieren

Während der Installation registriert Kaspersky Embedded Systems Security den Programmdienst „*Kaspersky Embedded Systems Security Service*“ in Windows. Das Programm enthält funktionale Komponenten, die beim Start des Betriebssystems gestartet werden. Dritte könnten mithilfe des Programmdienstes auf die Programmfunktionen und Sicherheitseinstellungen des geschützten Geräts zugreifen. Um dieses Risiko zu verringern, können Sie die Berechtigungen für die Verwaltung von Kaspersky Embedded Systems Security Service einschränken.

Standardmäßig wird Benutzern in der Administratorengruppe auf dem geschützten Gerät das Recht zur Verwaltung von Kaspersky Embedded Systems Security Service gewährt. Leserechte werden den Gruppen "SERVICE" und "INTERACTIVE" erteilt, Lese- und Ausführungsrechte werden der Gruppe "SYSTEM" gewährt.

Sie können das Benutzerkonto "SYSTEM" weder löschen noch dessen Rechte ändern. Wenn die Rechte des Kontos "SYSTEM" geändert werden, werden beim Speichern der Änderungen die maximalen Berechtigungen für dieses Konto wiederhergestellt.

Benutzer, die Zugriff auf Funktionen der Ebene „Berechtigungen bearbeiten“ haben, können anderen Benutzern, die auf dem geschützten Gerät registriert oder in der Domäne enthalten sind, Zugriffsrechte für die Verwaltung von Kaspersky Embedded Systems Security Service erteilen.

Sie können eine der folgenden vordefinierten Stufen für den Verwaltungszugriff auf Kaspersky Embedded Systems Security Service für einen Benutzer oder eine Gruppe von Kaspersky Embedded Systems Security auswählen:

- **Vollständige Kontrolle**: Berechtigung zum Anzeigen und Ändern der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Embedded Systems Security Service sowie zum Starten und Beenden von Kaspersky Embedded Systems Security Service.
- **Lesen**: Berechtigung zum Anzeigen der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Embedded Systems Security Service.
- **Ändern**: Berechtigung zum Anzeigen und Ändern der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Embedded Systems Security Service.
- **Ausführen**: Berechtigung zum Starten und Beenden von Kaspersky Embedded Systems Security Service.

Außerdem können Sie erweiterte Einstellungen für die Zugriffsrechte vornehmen: Zugriff auf bestimmte Funktionen von Kaspersky Embedded Systems Security erlauben oder verbieten (siehe Tabelle unten).

Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security Service

Funktion	Beschreibung
Lesen der Einstellungen des Dienstes	Berechtigung zum Anzeigen der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Embedded Systems Security Service.
Dienst-Status vom Service Control Manager abrufen	Berechtigung zur Abfrage des Ausführungsstatus von Kaspersky Embedded Systems Security Service beim Service Control Manager von Microsoft Windows.
Dienststatus abfragen	Berechtigung zur Abfrage des Ausführungsstatus des Dienstes bei Kaspersky Embedded Systems Security Service.
Lesen der Liste der abhängigen Dienste	Berechtigung zum Anzeigen der Liste der Dienste, von denen Kaspersky Embedded Systems Security Service abhängt, sowie der Dienste, die von Kaspersky Embedded Systems Security Service abhängen.
Dienst-Konfiguration ändern	Berechtigung zum Anzeigen und Ändern der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Embedded Systems Security Service.
Dienst starten	Berechtigung zum Starten von Kaspersky Embedded Systems Security Service.
Dienst beenden	Berechtigung zum Beenden von Kaspersky Embedded Systems Security Service.
Dienst pausieren / fortsetzen	Berechtigung zum Anhalten und Fortsetzen von Kaspersky Embedded Systems Security Service.
Leserechte	Berechtigung zum Anzeigen der Benutzerliste von Kaspersky Embedded Systems Security Service und der Zugriffsrechte der einzelnen Benutzer.
Bearbeitungsrechte	Berechtigungen: • Benutzer von Kaspersky Embedded Systems Security Service hinzufügen oder entfernen. • Benutzerzugriffsrechte für Kaspersky Embedded Systems Security Service bearbeiten.
Dienst entfernen	Berechtigung zum Aufheben der Registrierung von Kaspersky Embedded Systems Security Service beim Service Control Manager von Microsoft Windows.
Benutzeranfragen an den Dienst	Berechtigung zum Erstellen und Senden von Benutzeranfragen an Kaspersky Embedded Systems Security Service.

Sie können die Liste der Benutzer und Benutzergruppen, die zur Verwaltung von Kaspersky Embedded Systems Security Service berechtigt sind, sowie die Zugriffsrechte dieser Benutzer und Benutzergruppen bearbeiten.

So konfigurieren Sie die Benutzerberechtigungen zur Verwaltung von Kaspersky Embedded Systems Security Service in der Kaspersky Security Center Verwaltungskonsole

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 Fenster mit den Richtlinieneigenschaften den Punkt **Zusätzlich** aus.
4. Klicken Sie im Abschnitt **Benutzerberechtigungen für den Zugriff auf die KESS Service-Verwaltung** auf **Einstellungen**.

   Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.
5. Fügen Sie einen Active Directory-Benutzer oder eine Active Directory-Gruppe hinzu, für den bzw. die Sie die Benutzerberechtigungen für Kaspersky Embedded Systems Security Service konfigurieren möchten.
6. Wählen Sie einen Benutzer oder eine Benutzergruppe aus, dem bzw. der Sie die Verwaltung des Programms erlauben möchten.
7. Konfigurieren Sie in der Berechtigungsliste die Benutzerberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security Service.
8. Konfigurieren Sie bei Bedarf spezielle Berechtigungen für die Benutzer:

   a. Klicken Sie auf **Erweitert**.

   b. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster ein Benutzerkonto aus.

   c. Doppelklicken Sie, um die Eigenschaften des Benutzerkontos zu öffnen.

   d. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf den Link **Zusätzliche Berechtigungen anzeigen**.

   e. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die speziellen Berechtigungen für den Benutzer.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Benutzerberechtigungen zur Verwaltung von Kaspersky Embedded Systems Security Service in der Programmkonsole

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Benutzerberechtigungen für den Zugriff auf die KESS Service-Verwaltung** aus.
2. Klicken Sie im folgenden Fenster im Block **Berechtigungen** auf die Schaltfläche **Hinzufügen**.

   Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.
3. Fügen Sie einen Active Directory-Benutzer oder eine Active Directory-Gruppe hinzu, für den bzw. die Sie die Benutzerberechtigungen für Kaspersky Embedded Systems Security Service konfigurieren möchten.
4. Wählen Sie einen Benutzer oder eine Benutzergruppe aus, dem bzw. der Sie die Verwaltung des Programms erlauben möchten.

5. Konfigurieren Sie in der Berechtigungsliste die Benutzerberechtigungen für die Verwaltung von Kaspersky Embedded Systems Security Service.

6. Konfigurieren Sie bei Bedarf spezielle Berechtigungen für die Benutzer:

   a. Klicken Sie auf **Erweitert**.

   b. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster ein Benutzerkonto aus.

   c. Doppelklicken Sie, um die Eigenschaften des Benutzerkontos zu öffnen.

   d. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf den Link **Zusätzliche Berechtigungen anzeigen**.

   e. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die speziellen Berechtigungen für den Benutzer.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Benutzerberechtigungen zur Verwaltung von Kaspersky Embedded Systems Security Service 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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Zusätzlich** → **Benutzerberechtigungen für den Zugriff auf die KESS Service-Verwaltung** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Benutzerberechtigungen für den Zugriff auf die KESS Service-Verwaltung** wird geöffnet.

5. Fügen Sie einen Active Directory-Benutzer oder eine Active Directory-Gruppe hinzu, für den bzw. die Sie die Benutzerberechtigungen für Kaspersky Embedded Systems Security Service konfigurieren möchten.

6. Wählen Sie einen Benutzer oder eine Benutzergruppe aus, dem bzw. der Sie die Verwaltung des Programms erlauben möchten.

   Sie können keine speziellen Berechtigungen konfigurieren, um den Programmdienst in der Web Console zu verwalten.

7. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste beschränken, indem Sie die Benutzerberechtigungen konfigurieren. Außerdem können Sie kritische Vorgänge zusätzlich schützen, indem Sie in den Einstellungen von Kaspersky Embedded Systems Security einen Kennwortschutz einrichten.

Wenn ein Benutzer versucht, eine kennwortgeschützte Aktion auszuführen, fordert Kaspersky Embedded Systems Security ihn zur Eingabe des Benutzernamens und des Kennworts oder zur Verwendung eines Tokens für die Authentifizierung auf.

Benutzername und Kennwort

Der Kennwortschutz unterstützt die Verwendung der folgenden Benutzerkonten:

- **KLAdmin**. Ein Administratorkonto mit uneingeschränktem Zugriff auf Kaspersky Embedded Systems 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 Embedded Systems 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.

In der Benutzeroberfläche von Kaspersky Embedded Systems Security wird das angegebene Kennwort auf dem Bildschirm verborgen. Kaspersky Embedded Systems Security speichert das Kennwort in Form einer Prüfsumme, die bei der Eingabe des Kennworts berechnet wird.

Kaspersky Embedded Systems Security prüft nicht die Kennwortstärke und sperrt auch nicht die Kennworteingabe nach mehreren Fehleingaben.

Wenn Sie ein Kennwort erstellen, sollten Sie folgende Empfehlungen beachten:

- Das Kennwort darf weder Kontoname noch Computername enthalten.
- Das Kennwort ist mindestens 8 Zeichen lang.
- Das Kennwort enthält Zeichen aus mindestens drei der folgenden Kategorien:
  - Lateinische Großbuchstaben (A–Z)
  - Lateinische Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Ausrufezeichen (!), Dollarzeichen ($), Raute (#) und Prozentzeichen (%)

Token

Um auf die Funktionen von Kaspersky Embedded Systems Security zuzugreifen, müssen Sie das entsprechende Benutzerzertifikat aus der Liste der Zertifikate auswählen, die auf dem angeschlossenen 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.

So schützen Sie den Zugriff auf die Funktionalität von Kaspersky Embedded Systems Security durch ein Kennwort (in der Kaspersky Security Center Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Zusätzlich** aus.
4. Klicken Sie im Abschnitt **Benutzerberechtigungen für den Zugriff auf die Programmverwaltung** auf **Einstellungen**.
5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden**.
6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Kennwort zur Bestätigung kritischer Aktionen abfragen**.

   Ist diese Funktion aktiviert, so fragt das Programm den Benutzernamen und das Kennwort ab, wenn das Programm gelöscht, geändert oder wiederhergestellt werden soll, oder wenn über die Befehlszeile Aktionen ausgeführt werden, die die Schutzstufe des Geräts verringern können.

   Wenn diese Funktion deaktiviert ist und der aktuelle Benutzer über die erforderlichen Rechte verfügt, fragt Kaspersky Embedded Systems Security die Anmeldedaten nicht ab. Diese Option ist standardmäßig aktiviert.

   > Wenn für den aktuellen Benutzer ein leeres Windows-Kennwort festgelegt ist, müssen Sie die Anmeldedaten eines Benutzers eingeben, der über die erforderlichen Rechte verfügt und dessen Kennwort nicht leer ist.

7. Geben Sie das Kennwort für das Benutzerkonto „KLAdmin“ an.
8. Fügen Sie bei Bedarf Benutzerkonten hinzu, denen Sie Zugriff auf die Programmverwaltung gewähren möchten:

   a. Klicken Sie auf **Hinzufügen**.

      Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.

   b. Wählen Sie im angezeigten Fenster die Methode zum Hinzufügen von Benutzern aus: **Benutzer/Benutzergruppe manuell hinzufügen**.

c. Geben Sie einen Benutzernamen und ein Kennwort an.

d. Konfigurieren Sie in der Liste **Berechtigungen** die Benutzerzugriffsberechtigungen für die Programmfunktionen.

9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So schützen Sie den Zugriff auf die Funktionalität von Kaspersky Embedded Systems Security durch ein Kennwort (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Benutzerberechtigungen für den Zugriff auf die Programmverwaltung** aus.

2. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden**.

3. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Kennwort zur Bestätigung kritischer Aktionen abfragen**.

   Ist diese Funktion aktiviert, so fragt das Programm den Benutzernamen und das Kennwort ab, wenn das Programm gelöscht, geändert oder wiederhergestellt werden soll, oder wenn über die Befehlszeile Aktionen ausgeführt werden, die die Schutzstufe des Geräts verringern können.

   Wenn diese Funktion deaktiviert ist und der aktuelle Benutzer über die erforderlichen Rechte verfügt, fragt Kaspersky Embedded Systems Security die Anmeldedaten nicht ab. Diese Option ist standardmäßig aktiviert.

   > Wenn für den aktuellen Benutzer ein leeres Windows-Kennwort festgelegt ist, müssen Sie die Anmeldedaten eines Benutzers eingeben, der über die erforderlichen Rechte verfügt und dessen Kennwort nicht leer ist.

4. Geben Sie das Kennwort für das Benutzerkonto „KLAdmin“ an.

5. Fügen Sie bei Bedarf Benutzerkonten hinzu, denen Sie Zugriff auf die Programmverwaltung gewähren möchten:

   a. Klicken Sie auf **Hinzufügen**.

      Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.

   b. Wählen Sie im angezeigten Fenster die Methode zum Hinzufügen von Benutzern aus: **Benutzer/Benutzergruppe manuell hinzufügen**.

   c. Geben Sie einen Benutzernamen und ein Kennwort an.

   d. Konfigurieren Sie in der Liste **Berechtigungen** die Benutzerzugriffsberechtigungen für die Programmfunktionen.

6. Speichern Sie die vorgenommenen Änderungen.

So schützen Sie den Zugriff auf die Funktionalität von Kaspersky Embedded Systems Security durch ein Kennwort (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Zusätzlich → Benutzerberechtigungen für den Zugriff auf die Programmverwaltung** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden**.

6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Kennwort zur Bestätigung kritischer Aktionen abfragen**.

   Ist diese Funktion aktiviert, so fragt das Programm den Benutzernamen und das Kennwort ab, wenn das Programm gelöscht, geändert oder wiederhergestellt werden soll, oder wenn über die Befehlszeile Aktionen ausgeführt werden, die die Schutzstufe des Geräts verringern können.

   Wenn diese Funktion deaktiviert ist und der aktuelle Benutzer über die erforderlichen Rechte verfügt, fragt Kaspersky Embedded Systems Security die Anmeldedaten nicht ab. Diese Option ist standardmäßig aktiviert.

   > Wenn für den aktuellen Benutzer ein leeres Windows-Kennwort festgelegt ist, müssen Sie die Anmeldedaten eines Benutzers eingeben, der über die erforderlichen Rechte verfügt und dessen Kennwort nicht leer ist.

7. Geben Sie das Kennwort für das Benutzerkonto „KLAdmin“ an.

8. Fügen Sie bei Bedarf Benutzerkonten hinzu, denen Sie Zugriff auf die Programmverwaltung gewähren möchten:

   a. Klicken Sie auf **Hinzufügen**.

      Dadurch wird ein Formular zur Konfiguration der Benutzerzugriffsberechtigungen geöffnet.

   b. Wählen Sie im angezeigten Fenster die Methode zum Hinzufügen von Benutzern aus: **Benutzer/Benutzergruppe manuell hinzufügen**.

   c. Geben Sie einen Benutzernamen und ein Kennwort an.

   d. Konfigurieren Sie in der Liste **Berechtigungen** die Benutzerzugriffsberechtigungen für die Programmfunktionen.

9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

> Das festgelegte Kennwort kann nicht wiederhergestellt werden. Wenn Sie Ihr Kennwort vergessen, können Sie das Programm nicht mehr verwalten und kontrollieren. Darüber hinaus können Sie das Programm nicht mehr von dem geschützten Gerät entfernen.

Sie können das Kennwort jederzeit zurücksetzen. Deaktivieren Sie dazu das Kontrollkästchen **Bestätigung von Aktionen mit dem Programm erlauben, wenn Anmeldedaten von manuell erstellten Benutzern verwendet werden** und speichern Sie die Änderungen. Der Kennwortschutz wird deaktiviert und die alte Prüfsumme des Kennworts entfernt. Wiederholen Sie den Kennworterstellungsprozess mit einem neuen Kennwort.

Benachrichtigungen des sicheren Desktops

Kaspersky Embedded Systems Security unterstützt die Funktionalität (Secure Desktop). 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.

Kaspersky Embedded Systems Security zeigt Benachrichtigungen des sicheren Desktops an, um die folgenden Aktionen bestätigen zu lassen:

- Ablaufverfolgung wurde aktiviert oder deaktiviert
- Programmeinstellungen wurden exportiert oder importiert
- Schutz wurde angehalten
- Programm wurde beendet
- Aktiver Schlüssel wurde gelöscht
- Kaspersky Embedded Systems Security wurde deinstalliert
- Gerätekontrolle wurde deaktiviert
- Echtzeitschutz für Dateien wurde deaktiviert
- Richtlinie für Kaspersky Security Center wurde deaktiviert
- Berichte wurden angezeigt
- Dateien aus dem Backup wurden wiederhergestellt
- Einstellungen für Kaspersky Embedded Systems Security wurden geändert
- Programmaufgaben (unter Ausnahme des Aufgabenstarts) wurden verwaltet

So aktivieren oder deaktivieren Sie Benachrichtigungen des sicheren Desktops (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Anwendungseinstellungen**.
4. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf **Einstellungen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheit** aus.

6. Aktivieren oder deaktivieren Sie im Block **Selbstschutz** das Kontrollkästchen **Meldungen für sicheren Desktop aktivieren**, um die Benachrichtigungen des sicheren Desktops zu aktivieren oder zu deaktivieren.

   Wenn die Selbstschutz-Mechanismen deaktiviert sind, ist das Kontrollkästchen **Meldungen für sicheren Desktop aktivieren** nicht verfügbar.

7. Verriegeln Sie das Vorhängeschloss , um die Richtlinie auf die Computer anzuwenden.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie die Benachrichtigungen des sicheren Desktops (in der Verwaltungskonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und klicken Sie im Ergebnisbereich auf den Link **Eigenschaften des Programms**.

2. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Sicherheitseinstellungen** aus.

3. Aktivieren oder deaktivieren Sie im Block **Selbstschutz** das Kontrollkästchen **Meldungen für sicheren Desktop aktivieren**, um die Benachrichtigungen des sicheren Desktops zu aktivieren oder zu deaktivieren.

   Wenn die Selbstschutz-Mechanismen deaktiviert sind, ist das Kontrollkästchen **Meldungen für sicheren Desktop aktivieren** nicht verfügbar.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie die Benachrichtigungen des sicheren Desktops (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.

5. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf **Anpassen**.

   Das Fenster **Sicherheit und Zuverlässigkeit** wird geöffnet.

6. Aktivieren oder deaktivieren Sie im Block **Selbstschutz** das Kontrollkästchen **Meldungen für sicheren Desktop aktivieren**, um die Benachrichtigungen des sicheren Desktops zu aktivieren oder zu deaktivieren.

   Wenn die Selbstschutz-Mechanismen deaktiviert sind, ist das Kontrollkästchen **Meldungen für sicheren Desktop aktivieren** nicht verfügbar.

7. Verriegeln Sie das Vorhängeschloss , um die Richtlinie auf die Computer anzuwenden.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Vertrauenswürdige Zone

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Embedded Systems 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 Embedded Systems 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.

Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme wurden der vertrauenswürdigen Zone hinzugefügt. Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme helfen dabei, Kaspersky Embedded Systems Security schnell zu konfigurieren, ohne manuell eine vertrauenswürdige Zone zu erstellen.

Erstellung von Untersuchungsausnahmen

Eine *Untersuchungsausnahme* ist eine Kombination von Bedingungen. Sind diese Bedingungen erfüllt, so untersucht Kaspersky Embedded Systems Security ein Objekt nicht auf Viren und andere bedrohliche Programme.

Untersuchungsausnahmen können von den folgenden Programmkomponenten und Aufgaben verwendet werden:

- **Echtzeitschutz für Dateien**
- **Untersuchung auf Befehl**
- **Verhaltensanalyse**
- **AMSI-Scanner**
- **Schutz vor Netzwerkbedrohungen**

Ein Objekt wird nicht von Kaspersky Embedded Systems 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.

Ausschlusslisten dürfen in Kaspersky Embedded Systems Security maximal 5.000 Objekte enthalten.

So erstellen Sie eine Untersuchungsausnahme (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Zusätzlich → Vertrauenswürdige Zone** aus und klicken Sie auf **Einstellungen**.

4. Wählen Sie die Registerkarte **Untersuchungsausnahmen** aus.

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. Ist dieses Kontrollkästchen deaktiviert, blendet Kaspersky Embedded Systems Security die konsolidierte Liste der Untersuchungsausnahmen in der Anwendungskonsole 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 Embedded Systems Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Neue Ausnahme zur ausgewählten Kategorie**. Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.

   - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Ausnahmen aus der Liste der vordefinierten Untersuchungsausnahmen hinzufügen.

8. Um eine Datei oder einen Ordner von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Datei oder Ordner**. Klicken Sie auf den Link **Datei oder Ordner auswählen** und wählen Sie im folgenden Fenster eine Datei oder einen Ordner aus, indem Sie auf **Durchsuchen** klicken.

Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Embedded Systems 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.

9. Um einen vordefinierten Bereich von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Vordefinierter Bereich**. Klicken Sie auf den Link **vordefinierten Bereich auswählen** und wählen Sie im folgenden Fenster einen der Standardbereiche auf dem geschützten Gerät aus.

10. Um bestimmte Objekte von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Typ des erkannten Objekts**. Klicken Sie auf den Link **Objektnamen eingeben**, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im folgenden Fenster den Namen des Objekttyps an. Folgen Sie dabei der Klassifizierung 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 Embedded Systems Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

11. Um eine bestimmte Datei von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Hash des Objekts**. Klicken Sie auf den Link **Hash des Objekts eingeben** und geben Sie im folgenden Fenster einen Datei-Hash ein.

    Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

12. Wählen Sie im Block **Gültigkeitsbereich der Regel** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

13. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

14. Speichern Sie die Änderungen, um die Ausnahme zur Liste hinzuzufügen. Sie können eine Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen neben dem Objekt.

So erstellen Sie eine Untersuchungsausnahme (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Zusätzlich → Vertrauenswürdige Zone** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Wählen Sie die Registerkarte **Untersuchungsausnahmen** aus.
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. Ist dieses Kontrollkästchen deaktiviert, blendet Kaspersky Embedded Systems Security die konsolidierte Liste der Untersuchungsausnahmen in der Anwendungskonsole 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 Embedded Systems Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.
   - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Ausnahmen aus der Liste der vordefinierten Untersuchungsausnahmen hinzufügen.
9. Wenn Sie eine Datei oder einen Ordner von der Untersuchung ausschließen möchten, wählen Sie **Datei oder Ordner** aus und aktivieren Sie das Kontrollkästchen im gleichnamigen Feld. Geben Sie einen Datei- oder Ordnerpfad an.

Kaspersky Embedded Systems 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.

10. Um einen vordefinierten Bereich von der Untersuchung auszuschließen, wählen Sie **Vordefinierter Bereich** aus. Wählen Sie in der Dropdown-Liste einen der Standardbereiche auf dem geschützten Gerät aus.

11. Wenn Sie bestimmte Objekte von der Untersuchung ausschließen möchten, aktivieren Sie das Kontrollkästchen **Typ des erkannten Objekts** und geben Sie den Namen des Objekttyps an. Folgen Sie dabei der Klassifizierung 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 Embedded Systems Security die Objekte *Client-IRC*, *Client-P2P* und *Client-SMTP* von Untersuchungen aus.

12. Um eine einzelne Datei von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Hash des Objekts** und fügen Sie einen Hash aus einer Datei oder einer Ereignisliste hinzu.

    Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

13. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

14. Wählen Sie im Block **Schutzkomponenten** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

15. Die neue Ausnahme wird der Liste hinzugefügt. Sie können die Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen in der Spalte **Status**.

16. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Untersuchungsausnahme (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

   Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

2. Klicken Sie im Abschnitt **Ausnahmen** auf die Schaltfläche **Einstellungen** neben dem Block **Untersuchungsausnahmen**.

3. 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 Embedded Systems Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.

   - **Neue Ausnahme zur ausgewählten Kategorie**. Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.

   - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Ausnahmen aus der Liste der vordefinierten Untersuchungsausnahmen hinzufügen.

4. Um eine Datei oder einen Ordner von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Datei oder Ordner**. Klicken Sie den Link **Wählen Sie eine Datei oder einen Ordner aus** und wählen Sie im folgenden Fenster eine Datei oder einen Ordner aus, indem Sie auf **Durchsuchen** klicken.

   Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Embedded Systems 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.

5. Um einen vordefinierten Bereich von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Vordefinierter Bereich**. Klicken Sie auf den Link **vordefinierten Bereich auswählen** und wählen Sie im folgenden Fenster einen der Standardbereiche auf dem geschützten Gerät aus.

6. Um bestimmte Objekte von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Typ des erkannten Objekts**. Klicken Sie auf den Link **Objektnamen eingeben**, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im folgenden Fenster den Namen des Objekttyps an. Folgen Sie dabei der Klassifizierung 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 Embedded Systems Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

7. Um eine bestimmte Datei von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Hash des Objekts**. Klicken Sie auf den Link **Hash des Objekts eingeben** und geben Sie im folgenden Fenster einen Datei-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 **Gültigkeitsbereich der Regel** 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. Speichern Sie die Änderungen, um die Ausnahme zur Liste hinzuzufügen. Sie können eine Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen neben dem Objekt.

Beispiele für Pfadmasken:
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 im Ordner C:\dir\, 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 zu Dateien mit der Erweiterung .EXE im Ordner C:\dir\, jedoch nicht in den Unterordnern 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 zu Dateien mit der Erweiterung .EXE in Ordnern mit dem Namen „dir“, jedoch 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.

Erkennbare Objekttypen wählen

Gehen Sie folgendermaßen vor, um die Typen der erkennbaren Objekte zu wählen:

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Einstellungen der vertrauenswürdigen Zone konfigurieren**.
   - Wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

   Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.
2. Klicken Sie im Abschnitt **Typen der zu erkennenden Objekte** auf **Einstellungen**.

3. Aktivieren Sie im folgenden Fenster die Kontrollkästchen für die Objekttypen, die Kaspersky Embedded Systems Security erkennen soll:

- **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. *Überschreibende Viren* (Overwriting) schreiben ihren Code anstelle des Codes einer infizierten Datei und zerstören deren Inhalt. Die infizierte Datei funktioniert nicht mehr und kann nicht repariert werden. *Parasitäre Viren* (Parasitic) verändern Dateien, wobei diese vollständig oder teilweise funktionsfähig bleiben. *Companion-Viren* (Companion) verändern Dateien nicht, sondern legen Zwillingsdateien an. Beim Öffnen einer infizierten Datei wird ihr Zwilling gestartet, der ein Virus ist. Außerdem gibt es noch folgende Virentypen: *Linkviren* (Link), Viren, *die Objektmodule* (OBJ), *Compiler-Bibliotheken* (LIB) oder *den Quelltext von Programmen* infizieren, u.a.

  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.

Typ	Name	Beschreibung
IRC-Worm	Würmer für Internet-Chats	Sie verbreiten sich über Internet Relay Chats. Dies sind Chat-Systeme, mit denen über das Internet in Echtzeit Gespräche mit mehreren 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**

  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.

Typ	Name	Beschreibung
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.

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: 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.

Typ	Name	Beschreibung
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 Embedded Systems 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 Embedded Systems Security untersucht gepackte Dateien.

4. Speichern Sie die vorgenommenen Änderungen.

Liste mit vertrauenswürdigen Programmen erstellen

Die *Liste der vertrauenswürdigen Programme* ist eine Liste mit Programmen, deren Datei- oder Netzwerkaktivität nicht von Kaspersky Embedded Systems Security überwacht wird (selbst wenn diese schädlich ist). Gleiches gilt für den Zugriff dieser Programme auf die Systemregistrierung. Kaspersky Embedded Systems 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 Embedded Systems Security die Überwachung der Programmaktivitäten.

Untersuchungsausnahmen und vertrauenswürdige Programme unterscheiden sich wie folgt: Bei Ausnahmen untersucht Kaspersky Embedded Systems 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 Embedded Systems Security die Datei und beseitigt die Bedrohung. Wenn der Ordner zu den Ausnahmen gehört, überspringt Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems Security und anderen Anwendungen zu vermeiden (z. B. das Problem einer doppelten Untersuchung des Netzwerkverkehrs eines fremden Computers durch Kaspersky Embedded Systems 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 Embedded Systems Security auszuschließen.

Listen für vertrauenswürdige Programme dürfen in Kaspersky Embedded Systems Security maximal 5.000 Objekte enthalten.

So fügen Sie ein Programm zur vertrauenswürdigen Liste hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Zusätzlich** aus.
4. Klicken Sie im Block **Vertrauenswürdige Zone** auf **Einstellungen**.

5. Wählen Sie im folgenden Fenster die Registerkarte **Vertrauenswürdige Programme** aus.

   Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.

6. Aktivieren Sie das Kontrollkästchen **Vorgänge beim Anlegen eines Datei-Backups nicht untersuchen**, damit die Untersuchung von Lesevorgängen für Dateien übersprungen werden, wenn solche Vorgänge von auf dem geschützten Gerät installierten Backup-Tools ausgeführt werden.

7. 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

8. Aktivieren Sie das Kontrollkästchen **Bearbeitung 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. Ist dieses Kontrollkästchen deaktiviert, blendet Kaspersky Embedded Systems Security die konsolidierte Liste der vertrauenswürdigen Programme in der Anwendungskonsole aus.

9. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**, um die Untersuchung von Dateivorgängen für vertrauenswürdige Prozesse zu überspringen.

10. 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 Embedded Systems Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.

    - **Neue Ausnahme zur ausgewählten Kategorie**. Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.

    - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Programme aus der Liste der vordefinierten vertrauenswürdigen Programme hinzufügen.

11. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen** und geben Sie den Pfad der Datei ein, um festzustellen, ob der Prozess vertrauenswürdig ist.

    Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

Die Umgebungsvariable `%userprofile%` wird von Kaspersky Embedded Systems 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.

12. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

13. 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.

14. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie ein Programm zur vertrauenswürdigen Liste hinzu (in der Kaspersky Security Center Web Console)

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. Klicken Sie auf den Namen der Richtlinie von Kaspersky Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

5. Gehen Sie zu **Zusätzlich** → **Vertrauenswürdige Zone** und klicken Sie auf die Schaltfläche **Anpassen**.

6. Wählen Sie im folgenden Fenster die Registerkarte **Vertrauenswürdige Programme** aus.

7. Aktivieren Sie das Kontrollkästchen **Vorgänge beim Anlegen eines Datei-Backups nicht untersuchen**, damit die Untersuchung von Lesevorgängen für Dateien übersprungen werden, wenn solche Vorgänge von auf dem geschützten Gerät installierten Backup-Tools ausgeführt werden.

8. 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

9. Aktivieren Sie das Kontrollkästchen **Bearbeitung 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. Ist dieses Kontrollkästchen deaktiviert, blendet Kaspersky Embedded Systems Security die konsolidierte Liste der vertrauenswürdigen Programme in der Anwendungskonsole aus.

10. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**, um die Untersuchung von Dateivorgängen für vertrauenswürdige Prozesse zu überspringen.

11. 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 Embedded Systems Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.
    - **Neue Ausnahme zur ausgewählten Kategorie**. Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.
    - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Programme aus der Liste der vordefinierten vertrauenswürdigen Programme hinzufügen.

12. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen** und geben Sie den Pfad der Datei ein, um festzustellen, ob der Prozess vertrauenswürdig ist.

    Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

    > Die Umgebungsvariable `%userprofile%` wird von Kaspersky Embedded Systems 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.

13. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

14. 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 **Aktion**.

15. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie ein Programm zur vertrauenswürdigen Liste hinzu (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

   Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

2. Klicken Sie im Abschnitt **Ausnahmen** auf die Schaltfläche **Einstellungen** neben dem Block **Vertrauenswürdige Programme**.

3. 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 Embedded Systems Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.
   - **Neue Ausnahme zur ausgewählten Kategorie**. Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.
   - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Programme aus der Liste der vordefinierten vertrauenswürdigen Programme hinzufügen.

4. Wählen Sie eine Datei aus der Liste aus oder geben Sie den Pfad der ausführbaren Datei des vertrauenswürdigen Programms ein.

   Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

   > Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen. Außerdem konvertiert Kaspersky Embedded Systems Security 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 Embedded Systems 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.

5. Konfigurieren Sie die erweiterten Einstellungen für die vertrauenswürdigen Programme (siehe nachstehende Tabelle).

6. 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 Namen des Objekts.

7. Speichern Sie die vorgenommenen Änderungen.

Einstellungen für vertrauenswürdige Programme

Einstellung	Beschreibung
Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen	Kaspersky Embedded Systems Security verwendet den vollständigen Ordnerpfad, um festzustellen, ob der Prozess vertrauenswürdig ist.
Vertrauenswürdigkeit anhand des Prozess-Datei-Hashs bestimmen	Kaspersky Embedded Systems Security verwendet den Hash der ausgewählten Datei, um den Vertrauensstatus des Prozesses zu bestimmen. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der Hashwert der Datei nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

Einstellung	Beschreibung
Verwendung der Regeln	Sie können eine Liste der Komponenten von Kaspersky Embedded Systems Security konfigurieren, die die Aktivität eines vertrauenswürdigen Programms nicht überwachen sollen: • **Echtzeitschutz für Dateien**. Wenn diese Funktion aktiviert ist, schließt Kaspersky Embedded Systems Security alle Dateien von der Untersuchung aus, die mit einem vertrauenswürdigen Programm geöffnet werden. Diese Option ist standardmäßig aktiviert. • **Überwachung des Registrierungszugriffs**. Wenn diese Funktion aktiviert ist, überwacht Kaspersky Embedded Systems Security keine Änderungen an Registrierungsschlüsseln im Überwachungsbereich der Komponente Überwachung der Systemintegrität, die von einem vertrauenswürdigen Programm vorgenommen werden. Die Funktionalität ist standardmäßig deaktiviert. • **Verhaltensanalyse und Exploit-Prävention**. Wenn diese Funktion aktiviert ist, überwacht Kaspersky Embedded Systems Security mithilfe der Komponenten Verhaltensanalyse und Exploit-Prävention nicht die Datei- und Netzwerkaktivität eines vertrauenswürdigen Programms im Betriebssystem. Die Funktionalität ist standardmäßig deaktiviert. • **Interaktion mit AMSI-Scanner-Komponente**. Wenn diese Funktion aktiviert ist, überwacht Kaspersky Embedded Systems Security keine Anfragen eines vertrauenswürdigen Programms an die Komponente AMSI-Scanner. Die Funktionalität ist standardmäßig deaktiviert. • **Überwachung der Datei-Integrität**. Wenn diese Funktion aktiviert ist, überwacht Kaspersky Embedded Systems Security keine Änderungen, die von einem vertrauenswürdigen Programm an Dateien im Überwachungsbereich der Komponente Überwachung der Systemintegrität vorgenommen werden. Die Funktionalität ist standardmäßig deaktiviert. • **Kontrolle des Programmstarts**. Wenn diese Funktion aktiviert ist, überwacht Kaspersky Embedded Systems Security den Start eines vertrauenswürdigen Programms über die Komponente Kontrolle des Programmstarts nicht. Die Funktionalität ist standardmäßig deaktiviert. Für vordefinierte vertrauenswürdige Programme sind standardmäßig alle Funktionen mit Ausnahme von **Kontrolle des Programmstarts** aktiviert.
Interaktion mit der Programmoberfläche zulassen	Kaspersky Embedded Systems Security blockiert alle Versuche, bei denen Programmdienste von einem Remote-Computer aus verwaltet werden sollen. Ist dieses Kontrollkästchen aktiviert, wird einem Remote-Administrationsprogramm erlaubt, Einstellungen für Kaspersky Embedded Systems Security über die Benutzeroberfläche von Kaspersky Embedded Systems Security zu verwalten.
Aktivität von Unterprogrammen nicht überwachen	Kaspersky Embedded Systems Security überwacht nicht die Datei- und Netzwerkaktivität der Programme, die von diesem Programm gestartet werden. Sie können die Ausnahme rekursiv anwenden. In diesem Fall überwacht das Programm die Aktivität der gesamten Kette untergeordneter Programme nicht.
Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen	Die für den übergeordneten Prozess konfigurierten Einschränkungen werden von Kaspersky Embedded Systems Security nicht auf einen untergeordneten Prozess angewendet. Der übergeordnete Prozess wird von einem Programm gestartet, für das Programmrechte und Netzwerkregeln für das Programm konfiguriert sind.
Prozess-Speicher nicht untersuchen	Kaspersky Embedded Systems Security untersucht den Arbeitsspeicher des Prozesses nicht.

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 **Bearbeitung lokaler vertrauenswürdiger Programme erlauben** auf den Registerkarten **Untersuchungsausnahmen** und **Vertrauenswürdige Programme** im Abschnitt **Vertrauenswürdige Zone** der Richtlinie.

Wenn ein Administrator das Erstellen einer lokalen vertrauenswürdigen Zone erlaubt, kann der Benutzer über die Anwendungskonsole eigene Untersuchungsausnahmen und vertrauenswürdige Programme 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 Embedded Systems Security blendet die Listen der Untersuchungsausnahmen und vertrauenswürdigen Programme in der Anwendungskonsole aus, wenn der Administrator die Konfiguration der vertrauenswürdigen Zone in der Konsole blockiert hat (Symbol „verriegeltes Schloss“) und lokale Untersuchungsausnahmen und vertrauenswürdige Programme verboten sind.

So fügen Sie ein Objekt zur lokalen vertrauenswürdigen Zone hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu der die betreffenden Client-Computer gehören.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
4. Wählen Sie im Eigenschaftenfenster des Computers den Abschnitt **Anwendungen** aus.
5. Wählen Sie in der Liste der Kaspersky-Programme, die auf dem Computer installiert sind, den Punkt **Kaspersky Embedded Systems Security** aus und öffnen Sie durch Doppelklick die Programmeigenschaften.
6. Wählen Sie im Programmkonfigurationsfenster den Punkt **Zusätzlich → Vertrauenswürdige Zone** aus und klicken Sie auf **Einstellungen**.
7. Erstellen Sie auf der Registerkarte **Untersuchungsausnahmen** eine Liste mit lokalen Untersuchungsausnahmen.

   Lokale Untersuchungsausnahmen werden nach den gleichen Regeln erstellt wie allgemeine Ausnahmen. Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:
8. Erstellen Sie auf der Registerkarte **Vertrauenswürdige Programme** eine Liste mit lokalen vertrauenswürdigen Programmen. Dadurch wird ein Fenster mit einer Liste der lokalen vertrauenswürdigen Anwendungen geöffnet.

   Für das Hinzufügen von Anwendungen zur Liste der lokalen vertrauenswürdigen Anwendungen gelten die gleichen Regeln wie bei der allgemeinen Liste. Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:
9. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie ein Objekt zur lokalen vertrauenswürdigen Zone hinzu (in der Kaspersky Security Center 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 dem Benutzer die Ausführung der blockierten Aktion erlauben möchten.
3. Wählen Sie die Registerkarte **Anwendungen** aus.
4. Klicken Sie auf **Kaspersky Embedded Systems Security**.

   Die lokalen Programmeinstellungen werden geöffnet.

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

6. Wählen Sie im Programmkonfigurationsfenster den Punkt **Zusätzlich** → **Vertrauenswürdige Zone** aus und klicken Sie auf **Anpassen**.

   Das Fenster **Ausnahmen und Typen der zu erkennenden Objekte** wird geöffnet.

7. Erstellen Sie auf der Registerkarte **Untersuchungsausnahmen** eine Liste mit lokalen Untersuchungsausnahmen.

   Lokale Ausnahmen werden nach den gleichen Regeln erstellt wie allgemeine Ausnahmen. Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

8. Erstellen Sie auf der Registerkarte **Vertrauenswürdige Programme** eine Liste mit lokalen vertrauenswürdigen Programmen.

   Für das Hinzufügen von Anwendungen zur Liste der lokalen vertrauenswürdigen Anwendungen gelten die gleichen Regeln wie bei der allgemeinen Liste. Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

9. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine lokale Untersuchungsausnahme (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

   Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

2. Klicken Sie im Abschnitt **Untersuchungsausnahmen und vertrauenswürdige Programme** auf die Schaltfläche **Einstellungen** neben dem Block **Lokale Untersuchungsausnahmen**.

   Kaspersky Embedded Systems Security blendet die Liste der Untersuchungsausnahmen in der Anwendungskonsole aus, wenn der Administrator die Konfiguration von Untersuchungsausnahmen in der Konsole blockiert hat (Symbol „verriegeltes Schloss“) und lokale Untersuchungsausnahmen verboten sind (das Kontrollkästchen **Verwendung lokaler Ausnahmen erlauben** ist deaktiviert).

3. 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 Embedded Systems Security fügt eine neue Untersuchungsausnahme am Anfang der Liste hinzu.
   - **Neue Ausnahme zur ausgewählten Kategorie**. Um eine neue Untersuchungsausnahme zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.
   - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Ausnahmen aus der Liste der vordefinierten Untersuchungsausnahmen hinzufügen.

4. Durch die Auswahl von **Neue Ausnahme** wird das Fenster **Untersuchungsausnahme** geöffnet.

5. Um eine Datei oder einen Ordner von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Datei oder Ordner**. Klicken Sie den Link **Wählen Sie eine Datei oder einen Ordner aus** und wählen Sie im folgenden Fenster eine Datei oder einen Ordner aus, indem Sie auf **Durchsuchen** klicken.

Außerdem können Sie den Pfad auch manuell eingeben. Kaspersky Embedded Systems 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.

6. Um einen vordefinierten Bereich von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Vordefinierter Bereich**. Klicken Sie auf den Link **vordefinierten Bereich auswählen** und wählen Sie im folgenden Fenster einen der Standardbereiche auf dem geschützten Gerät aus.

7. Um bestimmte Objekte von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Typ des erkannten Objekts**. Klicken Sie auf den Link **Objektnamen eingeben**, klicken Sie auf die Schaltfläche **Hinzufügen** und geben Sie im folgenden Fenster den Namen des Objekttyps an. Folgen Sie dabei der Klassifizierung 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 Embedded Systems Security die Objekte `Client-IRC`, `Client-P2P` und `Client-SMTP` von Untersuchungen aus.

8. Um eine bestimmte Datei von der Untersuchung auszuschließen, aktivieren Sie das Kontrollkästchen **Hash des Objekts**. Klicken Sie auf den Link **Hash des Objekts eingeben** und geben Sie im folgenden Fenster einen Datei-Hash ein.

   Wenn die Datei geändert wird, wird auch der Dateihash geändert. Wenn dies geschieht, wird die geänderte Datei nicht den Ausnahmen hinzugefügt.

9. Wählen Sie im Block **Gültigkeitsbereich der Regel** die Komponenten aus, auf die die Untersuchungsausnahme angewendet werden soll.

10. Geben Sie erforderlichenfalls im Feld **Kommentar** einen kurzen Kommentar für die neue Untersuchungsausnahme an.

11. Speichern Sie die Änderungen, um die Ausnahme zur Liste hinzuzufügen. Sie können eine Ausnahme jederzeit deaktivieren. Dazu dient das Kontrollkästchen neben dem Objekt.

So fügen Sie ein Programm zur Liste der lokalen vertrauenswürdigen Programme hinzu (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

   Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

2. Klicken Sie im Abschnitt **Ausnahmen** auf die Schaltfläche **Einstellungen** neben dem Block **Lokale vertrauenswürdige Programme**.

   Kaspersky Embedded Systems Security blendet die konsolidierte Liste der vertrauenswürdigen Programme in der Anwendungskonsole aus, wenn der Administrator die Konfiguration von vertrauenswürdigen Programmen in der Konsole blockiert hat (Symbol „verriegeltes Schloss“) und lokale vertrauenswürdige Programme verboten sind (das Kontrollkästchen **Bearbeitung lokaler vertrauenswürdiger Programme erlauben** ist deaktiviert).

3. 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 Embedded Systems Security fügt ein neues vertrauenswürdiges Programm am Anfang der Liste hinzu.
   - **Neue Ausnahme zur ausgewählten Kategorie**. Um ein neues vertrauenswürdiges Programm zu einer bestimmten Kategorie hinzuzufügen, wählen Sie eine Kategorie aus.
   - **Ausnahme aus Liste auswählen**. Um Kaspersky Embedded Systems Security schnell zu konfigurieren, können Sie Programme aus der Liste der vordefinierten vertrauenswürdigen Programme hinzufügen.

4. Durch die Auswahl von **Neue Ausnahme** wird das Fenster **Untersuchungsausnahme** geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigkeit anhand des vollständigen Prozesspfads auf dem Laufwerk bestimmen** und geben Sie den Pfad der ausführbaren Datei des vertrauenswürdigen Programms ein.

   Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen und die Zeichen `*` und `?` bei der Eingabe einer Maske:

   Kaspersky Embedded Systems Security unterstützt Umgebungsvariablen. Außerdem konvertiert Kaspersky Embedded Systems Security 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 Embedded Systems 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. Speichern Sie die Änderungen, um die Ausnahme zur Liste hinzuzufügen.

Vertrauenswürdige Zone exportieren und importieren

Die *vertrauenswürdige Zone* ist eine Liste mit Objekten und Programmen, die nicht von Kaspersky Embedded Systems Security untersucht werden. Diese Liste wird vom Systemadministrator erstellt. Die vertrauenswürdige Zone besteht aus den folgenden Listen: *Untersuchungsausnahmen* und *vertrauenswürdige Programme*. 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.

Die *Liste für Ausnahmen* und vertrauenswürdige Programme wird im xml-Format exportiert und importiert.

Ausschlusslisten und Listen für vertrauenswürdige Programme dürfen in Kaspersky Embedded Systems Security maximal 5.000 Objekte enthalten.

So exportieren und importieren Sie die Liste der vertrauenswürdigen Zone (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Zusätzlich** → **Vertrauenswürdige Zone** aus und klicken Sie auf **Einstellungen**.

4. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie die Registerkarte **Untersuchungsausnahmen** aus.

   b. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

   c. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

      1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

      2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

   d. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

   Kaspersky Embedded Systems Security exportiert die Liste in die xml-Datei.

5. Um die Liste der vertrauenswürdigen Apps zu exportieren:

   a. Wählen Sie die Registerkarte **Vertrauenswürdige Programme** aus.

   b. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

   c. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

      1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

      2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

   d. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

      Kaspersky Embedded Systems Security exportiert die Liste in die xml-Datei.

6. So importieren Sie die Ausnahmeliste:

   a. Wählen Sie die Registerkarte **Untersuchungsausnahmen** aus.

      Dies öffnet ein Fenster mit einer Liste der Ausnahmen.

   b. Klicken Sie auf das Ordnersymbol und wählen Sie in der Dropdown-Liste den Punkt **Import** aus.

   c. Wählen Sie im folgenden Fenster die XML-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 Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.

7. Um eine Liste mit vertrauenswürdigen Apps zu importieren:

   a. Wählen Sie die Registerkarte **Vertrauenswürdige Programme** aus.

      Dies öffnet ein Fenster mit einer Liste von vertrauenswürdigen Programmen.

   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 Embedded Systems 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 oder importieren Sie die vertrauenswürdige Zone (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Zusätzlich → Vertrauenswürdige Zone** und klicken Sie auf die Schaltfläche **Anpassen**.
5. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie auf der Registerkarte **Untersuchungsausnahmen und vertrauenswürdige Programme** die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die drei Punkte und wählen Sie den Punkt **Export** aus.

   c. Bestätigen Sie, dass Sie nur die ausgewählten Ausnahmen exportieren möchten, oder exportieren Sie die gesamte Liste der Ausnahmen.

   Kaspersky Embedded Systems Security exportiert die Liste in die xml-Datei.
6. Um die Liste der vertrauenswürdigen Apps zu exportieren:

   a. Wählen Sie auf der Registerkarte **Untersuchungsausnahmen und vertrauenswürdige Programme** die Programme aus, die Sie exportieren möchten.

   b. Klicken Sie auf die drei Punkte und wählen Sie den Punkt **Export** aus.

   c. Bestätigen Sie, dass Sie nur die ausgewählten Programme exportieren möchten, oder exportieren Sie die gesamte Liste.

   Kaspersky Embedded Systems Security exportiert die Liste in die xml-Datei.
7. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf der Registerkarte **Untersuchungsausnahmen und vertrauenswürdige Programme** auf **Aus vorheriger Version importieren**, wenn Sie die Ausnahmeliste aus einer xml-Datei importieren möchten, die in der Programmversion 3.4 oder älter erstellt wurde.

   Wenn Sie Regeln aus einer xml-Datei importieren, die in Version 4.0 oder höher erstellt wurde, klicken Sie auf **Import**.

   b. Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.

   c. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   d. Klicken Sie auf **Import**.

8. Um eine Liste mit vertrauenswürdigen Apps zu importieren:

    a. Klicken Sie auf der Registerkarte **Untersuchungsausnahmen und vertrauenswürdige Programme** auf **Aus vorheriger Version importieren**, wenn Sie die Liste mit vertrauenswürdigen Programmen aus einer xml-Datei importieren möchten, die in der Programmversion 3.4 oder älter erstellt wurde.

    Wenn Sie vertrauenswürdige Programme aus einer xml-Datei importieren, die in Version 4.0 oder höher erstellt wurde, klicken Sie auf **Import**.

    b. Wenn es auf dem Computer bereits eine Liste mit vertrauenswürdigen Apps gibt, fragt Kaspersky Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

    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. Klicken Sie auf **Import**.

9. Speichern Sie die vorgenommenen Änderungen.

So exportieren oder importieren Sie die vertrauenswürdige Zone (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

    Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

2. So exportieren Sie die Liste der Ausnahmen oder vertrauenswürdigen Programme:

    a. Klicken Sie im Abschnitt **Ausnahmen** auf die Schaltfläche **Einstellungen** neben den Blöcken **Untersuchungsausnahmen** oder **Vertrauenswürdige Programme**.

    Daraufhin wird ein Fenster mit einer Liste von Untersuchungsausnahmen oder vertrauenswürdigen Programmen geöffnet.

    b. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

    c. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

        1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

        2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

    d. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

    Kaspersky Embedded Systems Security exportiert die Liste in die xml-Datei.

3. So importieren Sie eine Liste mit Ausnahmen oder vertrauenswürdigen Programmen:

    a. Klicken Sie im Abschnitt **Ausnahmen** auf die Schaltfläche **Einstellungen** neben den Blöcken **Untersuchungsausnahmen** oder **Vertrauenswürdige Programme**.

    b. Wählen Sie die Ausnahmen oder die vertrauenswürdigen Programme aus, die Sie importieren möchten.

    c. Klicken Sie auf das Ordnersymbol und wählen Sie **Import** aus.

d. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die xml-Datei aus, aus der Sie die Liste der Ausnahmen oder vertrauenswürdigen Programme importieren möchten.

e. Öffnen Sie die Datei.

Wenn es auf dem Computer bereits eine Liste mit Ausnahmen gibt, fragt Kaspersky Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.

4. Speichern Sie die vorgenommenen Änderungen.

Vertrauenswürdigen Zertifikatspeicher des Systems verwenden

Durch die Verwendung des Zertifikatspeichers des Systems können Programme, die eine vertrauenswürdige digitale Signatur besitzen, von der Untersuchung auf Viren ausgeschlossen werden. Kaspersky Embedded Systems Security weist solche Programme automatisch der Gruppe *Vertrauenswürdig* zu.

So konfigurieren Sie die Verwendung eines vertrauenswürdigen Zertifikatspeichers des Systems (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Zusätzlich → Vertrauenswürdige Zone** aus und klicken Sie auf **Einstellungen**.
4. Wählen Sie die Registerkarte **Vertrauenswürdiger Zertifikatspeicher des Systems** aus.
5. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigen Zertifikatspeicher des Systems verwenden** und wählen Sie in der Dropdown-Liste den Systemspeicher aus, den Kaspersky Embedded Systems Security als vertrauenswürdig einstufen soll.
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Verwendung eines vertrauenswürdigen Zertifikatspeichers des Systems (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Zusätzlich → Vertrauenswürdige Zone** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Wählen Sie die Registerkarte **Vertrauenswürdiger Zertifikatspeicher des Systems** aus.

6. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdigen Zertifikatspeicher des Systems verwenden** und wählen Sie in der Dropdown-Liste den Systemspeicher aus, den Kaspersky Embedded Systems Security als vertrauenswürdig einstufen soll.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Verwendung eines vertrauenswürdigen Zertifikatspeichers des Systems (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Knoten **Kaspersky Embedded Systems Security** aus und wählen Sie im Kontextmenü des Knotens den Punkt **Vertrauenswürdige Zone** aus.

   Das Fenster **Einstellungen der vertrauenswürdigen Zone konfigurieren** wird geöffnet.

2. Aktivieren Sie unter **Vertrauenswürdiger Zertifikatspeicher des Systems** das Kontrollkästchen **Vertrauenswürdigen Zertifikatspeicher des Systems verwenden** und wählen Sie in der Dropdown-Liste den Systemspeicher aus, den Kaspersky Embedded Systems Security als vertrauenswürdig einstufen soll.

3. Speichern Sie die vorgenommenen Änderungen.

Vordefinierte Untersuchungsausnahmen und vertrauenswürdige Programme

Mithilfe vordefinierter Untersuchungsausnahmen und vertrauenswürdiger Programme können Sie Prozesse und Dateien der folgenden Software schnell zur vertrauenswürdigen Zone hinzufügen:

- Microsoft Exchange Server
- Microsoft SQL Server
- Microsoft Hyper-V
- Der Datendeduplizierungsprozess in Microsoft Windows Server
- Microsoft System Center Configuration Manager

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
  - In der Befehlszeile.

Echtzeitschutz für Dateien

Die Kaspersky Embedded Systems Security-Komponente Echtzeitschutz für Dateien untersucht folgende Objekte des geschützten Geräts, wenn auf diese zugegriffen wird:

- Dateien
- Alternative NTFS-Datenströme
- Master Boot Records und Bootsektoren von lokalen Festplatten und externen Geräten
- Container-Dateien in Windows Server 2016 und Windows Server 2019.

Wenn eine Anwendung eine Datei auf dem geschützten Gerät schreibt oder liest, fängt Kaspersky Embedded Systems Security die Datei ab, untersucht sie auf Bedrohungen und führt, wenn eine Bedrohung erkannt wird, eine Standardaktion oder eine von Ihnen festgelegte Aktion aus: Desinfektion, Verschieben in die Quarantäne oder Löschen. Vor der Desinfektion oder dem Löschen speichert Kaspersky Embedded Systems Security eine verschlüsselte Kopie der Quelldatei im Backup-Ordner.

Kaspersky Embedded Systems Security fängt Dateivorgänge ab, die in Containern für Windows Server 2016 und Windows Server 2019 ausgeführt werden.

Ein *Container* ist eine isolierte Umgebung, in der Programme ohne direkte Interaktion mit dem Betriebssystem ausgeführt werden können. Wenn sich ein Container im Schutzbereich der Komponente befindet, untersucht Kaspersky Embedded Systems Security die Container-Dateien, auf die Benutzer zugreifen, auf Computerbedrohungen. Wenn eine Bedrohung erkannt wird, versucht das Programm, den Container zu desinfizieren. Bei erfolgreicher Desinfektion ist der Container weiterhin verfügbar. Schlägt die Desinfektion fehl, wird der Container deaktiviert.

Kaspersky Embedded Systems Security erkennt außerdem Schadsoftware für Prozesse, die unter Windows Subsystem for Linux® laufen. Bei solchen Prozessen wendet die Komponente Echtzeitschutz für Dateien die in der aktuellen Konfiguration festgelegte Aktion an.

Über den Schutzbereich von Aufgaben und Sicherheitseinstellungen

Die Komponente Echtzeitschutz für Dateien schützt standardmäßig alle Objekte im Dateisystem des Geräts. Verlangen die Sicherheitsanforderungen keinen Schutz für alle Objekte des Dateisystems, oder wenn Sie einige Objekte aus dem Gültigkeitsbereich der Aufgabe zum Echtzeitschutz ausschließen möchten, können Sie den Schutzbereich beschränken.

In der Anwendungskonsole wird der Schutzbereich als Liste jener Dateiressourcen des Geräts dargestellt, die von Kaspersky Embedded Systems Security überwacht werden können.

Parameter für Sicherheit

Die Sicherheitseinstellungen für Aufgaben können entweder als allgemeine Einstellungen für alle Knoten oder Elemente im Schutzbereich konfiguriert werden oder als individuelle Einstellungen für jeden Knoten bzw. jedes Element in der Liste der Dateiressourcen des Geräts.

Die Sicherheitseinstellungen, die für den ausgewählten übergeordneten Knoten konfiguriert wurden, werden automatisch für alle untergeordneten Node übernommen. Die Sicherheitseinstellungen des übergeordneten Knotens werden für untergeordnete Knoten, die gesondert konfiguriert werden, nicht übernommen.

Sie können die Parameter eines ausgewählten Schutzbereichs auf eine der folgenden Weisen anpassen:

- Wählen Sie eine der vordefinierten Sicherheitsstufen aus.
- Konfigurieren Sie die Sicherheitseinstellungen manuell für die ausgewählten Knoten oder Elemente in der Liste der Dateiressourcen (die Sicherheitsstufe ändert sich in **Benutzerdefiniert**).

Vordefinierte Schutzbereiche

Die Liste der Dateiressourcen enthält die Knoten, für die Sie gemäß den Microsoft Windows-Sicherheitseinstellungen über Leserechte verfügen.

Kaspersky Embedded Systems Security deckt die folgenden vordefinierten Schutzbereiche ab:

- **Lokale Festplatten**. Kaspersky Embedded Systems Security schützt Dateien auf den Festplatten des Geräts.
- **Wechseldatenträger**. Kaspersky Embedded Systems Security schützt Dateien auf externen Geräten, z. B. auf CDs oder Wechseldatenträger. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Schutzbereich aufnehmen oder aus diesem ausschließen.
- **Netzwerk**. Kaspersky Embedded Systems Security schützt die Dateien, die in Netzwerkordnern gespeichert sind oder aus diesen von auf dem Gerät laufenden Programmen abgefragt werden. Kaspersky Embedded Systems Security schützt Dateien in Netzwerkordnern nicht, wenn Programme von anderen geschützten Geräten aus darauf zugreifen.

Die vordefinierten Schutzbereiche werden standardmäßig in der Liste mit den Bereichen angezeigt, können dort angepasst werden und sind zum Hinzufügen in die Liste bei ihrer Erstellung in den Schutzbereichseinstellungen verfügbar.

Verbundene Netzlaufwerke werden auch nicht in der Dateiressourcenliste des geschützten Geräts angezeigt. Um Objekte auf einem Netzwerk-Datenträger in den Schutzbereich aufzunehmen, geben Sie den Pfad des Ordners an, der diesem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

Über vordefinierte Sicherheitsstufen

Für in der Struktur oder Liste der Dateiressourcen des geschützten Geräts ausgewählte Knoten können Sie eine der folgenden vordefinierten Sicherheitsstufen festlegen: **Maximale Leistung**, **Empfohlen**, **Maximaler Schutz** oder **Informieren**. Jede dieser Stufen besitzt eine eigene Auswahl von Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird empfohlen, wenn Ihr Netzwerk über zusätzliche Sicherheitsmaßnahmen verfügt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien, die über die Verwendung von Kaspersky Embedded Systems Security auf geschützten Geräten und Workstations hinausgehen.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Geräte. Die Experten von Kaspersky empfehlen diese Stufe als ausreichenden Schutz von Geräten in den meisten Unternehmensnetzwerken. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximaler Schutz

Die Sicherheitsstufe **Maximaler Schutz** wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Gerätesicherheit hat.

Informieren

Die Sicherheitsstufe **Informieren** wird empfohlen, wenn sich im Unternehmensnetzwerk möglicherweise viele infizierte Computer befinden und deren Blockierung den Betrieb des Unternehmens erheblich stören könnte.

Vordefinierte Sicherheitsstufen und entsprechende Einstellungswerte

Einstellungen	Sicherheitsstufe			
	Maximale Leistung	Empfohlen	Maximaler Schutz	Informieren
Schutz von Objekten	Untersuchte Objekte gemäß der Liste der Erweiterungen, die in der Antiviren-Datenbank angegeben sind	Objekte, die nach Format untersucht werden	Objekte, die nach Format untersucht werden	Objekte, die nach Format untersucht werden
Scan only new and modified files	Aktiviert	Aktiviert	Deaktiviert	Aktiviert
Scan of compound files	Deaktiviert	Dateien in Microsoft Office-Formaten untersuchen	Dateien in Microsoft Office-Formaten untersuchen	Dateien in Microsoft Office-Formaten untersuchen

Einstellungen	Sicherheitsstufe			
	Maximale Leistung	Empfohlen	Maximaler Schutz	Informieren
Aktion für infizierte und andere Objekte	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen.	Zugriff verweigern und von Kaspersky-Experten empfohlene Aktion ausführen	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen.	Informieren
Aktion auf die ausgewählten Objekttypen anwenden	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann	Deaktiviert	Deaktiviert	Aktiviert	Deaktiviert
Systemkritische Objekte sind Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Embedded Systems Security erforderlich sind. Diese Dateien können nicht gelöscht werden. Prozesse, die mit solchen Objekten verknüpft sind, können nicht beendet werden.				
Unpack in the background compound files larger than (MB)				
Stop scanning if it takes longer than (sec)	60 Sek.	60 Sek.	60 Sek.	60 Sek.
Do not scan compound objects larger than (MB)	8 MB	8 MB	Nicht konfiguriert.	8 MB
iSwift-Technologie verwenden	Aktiviert	Aktiviert	Aktiviert	Aktiviert
iChecker-Technologie verwenden	Aktiviert	Aktiviert	Aktiviert	Aktiviert

Dateierweiterungen, die von der Komponente Echtzeitschutz für Dateien standardmäßig untersucht werden

In der Grundeinstellung untersucht Kaspersky Embedded Systems Security Dateien mit den folgenden Erweiterungen:

- *386*
- *acm*
- *ade, adp*
- *asp*
- *asx*
- *ax*
- *bas*
- *bat*
- *bin*

- *chm*
- *cla, clas**
- *cmd*
- *com*
- *cpl*
- *crt*
- *dll*
- *dpl*
- *drv*
- *dvb*
- *dwg*
- *efi*
- *emf*
- *eml*
- *.exe*
- *fon*
- *fpm*
- *hlp*
- *hta*
- *htm, html**
- *htt*
- *ico*
- *inf*
- *ini*
- *ins*
- *isp*
- *jpg, jpe*
- *js, jse*

- *lnk*
- *mbx*
- *msc*
- *msg*
- *msi*
- *msp*
- *mst*
- *nws*
- *ocx*
- *oft*
- *otm*
- *pcd*
- *pdf*
- *php*
- *pht*
- *phtm**
- *pif*
- *plg*
- *png*
- *pot*
- *prf*
- *prg*
- *reg*
- *rsc*
- *rtf*
- *scf*
- *scr*
- *sct*

- *shb*
- *shs*
- *sht*
- *shtm**
- *swf*
- *sys*
- *the*
- *them**
- *tsp*
- *url*
- *vb*
- *vbe*
- *vbs*
- *vxd*
- *wma*
- *wmf*
- *wmv*
- *wsc*
- *wsf*
- *wsh*
- *do?*
- *md?*
- *mp?*
- *ov?*
- *pp?*
- *vs?*
- *xl?*

Komponente Echtzeitschutz für Dateien konfigurieren

Die Komponente Echtzeitschutz für Dateien verwendet standardmäßig die unten in der Tabelle beschriebenen Einstellungen. Sie können die Werte dieser Parameter ändern.

Standardeinstellungen der Komponente Echtzeitschutz für Dateien

Einstellung	Standardwert	Beschreibung
Schutzbereich	Gesamtes geschütztes Gerät ohne virtuelle Festplatten.	Mit dieser Option können Sie den Schutzbereich ändern.
Parameter für Sicherheit	Einheitlich für den gesamten Schutzbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Sie können für die ausgewählten Knoten in der Struktur oder Liste der Dateiressourcen des geschützten Geräts folgende Aktionen ausführen: • eine andere vordefinierte Sicherheitsstufe auswählen • die Sicherheitseinstellungen manuell ändern Sie können eine Gruppe von Sicherheitsparametern für den ausgewählten Knoten in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen.
Schutzmodus für Objekte	**Intelligenter Modus**.	Mit dieser Option wählen Sie den Schutzmodus aus, d. h. Sie legen fest, auf welche Art von Zugriffsversuchen Kaspersky Embedded Systems Security die Objekte untersucht.
Heuristische Analyse	Es wird die Sicherheitsstufe **Mittel** angewendet.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
Block access to network shared resources for the sessions that show malicious activity	Wird nicht verwendet.	Mit dieser Option können Sie die aktuelle Sitzung blockieren und die Host-IP oder Host-LUID, für die bösartige Aktivitäten erkannt wurden, im Abschnitt "Speicher der blockierten Hosts" hinzufügen.
Untersuchung wichtiger Bereiche starten, wenn aktive Infektion erkannt wird	Wird verwendet	Wenn eine aktive Infektion erkannt wird, erstellt Kaspersky Embedded Systems Security eine Aufgabe zur Untersuchung wichtiger Bereiche und startet sie.
Container anhalten, wenn Desinfektion fehlschlägt	Wird verwendet	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	Wird verwendet	Ist das Kontrollkästchen aktiviert, untersucht das Programm den Container nur beim Start des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.

So aktivieren Sie die Virenuntersuchung von Dateien (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Einstellungen für den Echtzeitschutz von Dateien** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Echtzeitschutz für Dateien**.

6. Wählen Sie im Block **Schutzmodus für Objekte** auf der Registerkarte **Allgemein** den Funktionsmodus für den Echtzeitschutz für Dateien aus:

   - **Intelligenter Modus**. Kaspersky Embedded Systems Security wählt die Objekte für die Untersuchung selbstständig aus. Ein Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn durch den Prozess mehrere Male auf das Objekt zugegriffen und von ihm verändert wird, untersucht Kaspersky Embedded Systems Security das Objekt nur nachdem das Objekt zum letzten Mal von dem Prozess gespeichert wurde.

   - **Bei Zugriff und Veränderungen**. Kaspersky Embedded Systems Security untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern. Dieser Status gilt als Standard.

   - **Bei Zugriff**. Kaspersky Embedded Systems Security untersucht alle Objekte, wenn diese zum Lesen, Ausführen oder Ändern geöffnet werden.

   - **Bei Ausführung**. Kaspersky Embedded Systems Security untersucht eine Datei nur beim Öffnen zum Ausführen.

7. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.

8. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Block access to network shared resources for the sessions that show malicious activity**.

9. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Launch critical areas scan when active infection is detected**.

   Ist das Kontrollkästchen aktiviert, führt Kaspersky Embedded Systems Security beim Fund einer aktiven Infektion die vordefinierte Aufgabe *Untersuchung wichtiger Bereiche* aus. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

10. Legen Sie die Einstellungen für die Untersuchung von Dateivorgängen fest, die in Windows-Containern ausgeführt werden.

11. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Virenuntersuchung von Dateien (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Aktivieren Sie das Kontrollkästchen **Echtzeitschutz für Dateien aktivieren**.

6. Wählen Sie im Block **Schutzmodus für Objekte** auf der Registerkarte **Allgemein** den Funktionsmodus für den Echtzeitschutz für Dateien aus:

   - **Intelligenter Modus**. Kaspersky Embedded Systems Security wählt die Objekte für die Untersuchung selbstständig aus. Ein Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn durch den Prozess mehrere Male auf das Objekt zugegriffen und von ihm verändert wird, untersucht Kaspersky Embedded Systems Security das Objekt nur nachdem das Objekt zum letzten Mal von dem Prozess gespeichert wurde.

   - **Bei Zugriff und Veränderungen**. Kaspersky Embedded Systems Security untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern. Dieser Status gilt als Standard.

   - **Bei Zugriff**. Kaspersky Embedded Systems Security untersucht alle Objekte, wenn diese zum Lesen, Ausführen oder Ändern geöffnet werden.

   - **Bei Ausführung**. Kaspersky Embedded Systems Security untersucht eine Datei nur beim Öffnen zum Ausführen.

7. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.

8. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Zugriff auf freigegebene Netzwerkressourcen blockieren für Netzwerksitzungen, die bösartige Aktivität zeigen**.

9. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Untersuchung wichtiger Bereiche starten, wenn aktive Infektion erkannt wird**.

   Ist das Kontrollkästchen aktiviert, führt Kaspersky Embedded Systems Security beim Fund einer aktiven Infektion die vordefinierte Aufgabe *Untersuchung wichtiger Bereiche* aus. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

10. Legen Sie die Einstellungen für die Untersuchung von Dateivorgängen fest, die in Windows-Containern ausgeführt werden.

11. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Virenuntersuchung von Dateien (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Echtzeitschutz für Dateien** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Echtzeitschutz für Dateien** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Echtzeitschutz für Dateien**.

4. Wählen Sie im Block **Schutzmodus für Objekte** auf der Registerkarte **Allgemein** den Funktionsmodus für den Echtzeitschutz für Dateien aus:

   - **Intelligenter Modus**. Kaspersky Embedded Systems Security wählt die Objekte für die Untersuchung selbstständig aus. Ein Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn durch den Prozess mehrere Male auf das Objekt zugegriffen und von ihm verändert wird, untersucht Kaspersky Embedded Systems Security das Objekt nur nachdem das Objekt zum letzten Mal von dem Prozess gespeichert wurde.

   - **Bei Zugriff und Veränderungen**. Kaspersky Embedded Systems Security untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern. Dieser Status gilt als Standard.

- **Bei Zugriff**. Kaspersky Embedded Systems Security untersucht alle Objekte, wenn diese zum Lesen, Ausführen oder Ändern geöffnet werden.
- **Bei Ausführung**. Kaspersky Embedded Systems Security untersucht eine Datei nur beim Öffnen zum Ausführen.

5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.
6. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Block access to network shared resources for the sessions that show malicious activity**.
7. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Launch critical areas scan when active infection is detected**.

   Ist das Kontrollkästchen aktiviert, führt Kaspersky Embedded Systems Security beim Fund einer aktiven Infektion die vordefinierte Aufgabe *Untersuchung wichtiger Bereiche* aus. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
8. Legen Sie die Einstellungen für die Untersuchung von Dateivorgängen fest, die in Windows-Containern ausgeführt werden.
9. Speichern Sie die vorgenommenen Änderungen.

Schutzbereich für die Komponente Echtzeitschutz für Dateien konfigurieren

Für die Komponente Echtzeitschutz für Dateien werden standardmäßig die gleichen Sicherheitseinstellungen verwendet wie für den gesamten Schutzbereich. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**.

Sie können die Standardwerte der Sicherheitseinstellungen ändern. Legen Sie dazu entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für einzelne Elemente in der Liste der Dateiressourcen des Geräts fest.

Wenn dasselbe Objekt in mehreren Schutzbereichseinträgen enthalten ist und diese Einträge unterschiedliche Sicherheitsstufen haben, ist die letzte Regel in der Liste vorrangig. Stellen Sie sich beispielsweise einen Schutzbereich vor, der zwei Einträge enthält: **Alle Festplatten** (Sicherheitsstufe **Inform**) und `*\Users\*\Downloads\*` (Sicherheitsstufe **Custom**). Das Programm untersucht Festplatten mit der Stufe „Informieren“, unter Ausnahme des Ordners `Downloads`. Das Programm untersucht den Ordner `Downloads` nach den manuell festgelegten Einstellungen, da dieser Eintrag in der Liste der Schutzbereiche an letzter Stelle steht.

So konfigurieren Sie den Schutzbereich für den Echtzeitschutz für Dateien (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.

4. Klicken Sie im Abschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**.

5. Wählen Sie die Registerkarte **Schutzbereich** aus.

6. Wählen Sie in der Liste der Dateiressourcen des geschützten Geräts die Elemente aus, für die Sie eine vordefinierte Sicherheitsstufe festlegen möchten.

7. Wenn die Dateifreigabe nicht in der Liste enthalten ist, fügen Sie sie manuell hinzu:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie in der Ordnerstruktur den Pfad des erforderlichen Objekts an oder geben Sie im Feld **Objekt** den Pfad an.

   Verwenden Sie bei Bedarf Sonderzeichen, um die Maske des Objektpfads einzugeben:

   - 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.

   Das Objekt **Dieser PC** in der Liste der Dateiressourcen des Computers enthält die folgenden Objekte: **Alle Festplatten**, **Alle Netzlaufwerke** und **Alle Wechseldatenträger**.

   c. Klicken Sie auf **OK**.

8. Vergewissern Sie sich, dass die ausgewählte Dateiressource zum Schutzbereich gehört.

9. Legen Sie eine vordefinierte Sicherheitsstufe für den ausgewählten Schutzbereich fest, indem Sie auf **Konfigurieren** klicken. Standardmäßig werden auf den gesamten Schutzbereich identische Sicherheitseinstellungen angewendet. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**. Sie können die standardmäßigen Sicherheitseinstellungen bearbeiten.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Schutzbereich für den Echtzeitschutz für Dateien (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Wählen Sie die Registerkarte **Schutzbereich** aus.

6. Wählen Sie in der Liste der Dateiressourcen des geschützten Geräts die Elemente aus, für die Sie eine vordefinierte Sicherheitsstufe festlegen möchten.

7. Wenn die Dateifreigabe nicht in der Liste enthalten ist, fügen Sie sie manuell hinzu:

   a. Klicken Sie auf **Hinzufügen**.

   b. Wählen Sie in der Liste **Typ des Objekts** eine Option aus:

   Verwenden Sie Sonderzeichen für die Option **Maske**, um die Maske des Objektpfads einzugeben:

   - 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.

   Das Objekt **Dieser PC** in der Liste der Dateiressourcen des Computers enthält die folgenden Objekte: **Alle Festplatten**, **Alle Netzlaufwerke** und **Alle Wechseldatenträger**.

   c. Klicken Sie auf **OK**.

8. Stellen Sie sicher, dass die ausgewählte Dateiressource zum Schutzbereich gehört. Verwenden Sie gegebenenfalls den Schalter neben dem Listenelement.

9. Legen Sie eine vordefinierte Sicherheitsstufe für den ausgewählten Schutzbereich fest, indem Sie auf **Ändern** klicken. Standardmäßig werden auf den gesamten Schutzbereich identische Sicherheitseinstellungen angewendet. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**. Sie können die standardmäßigen Sicherheitseinstellungen bearbeiten.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie den Schutzbereich für den Echtzeitschutz für Dateien (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Echtzeitschutz für Dateien** auf **Schutzbereich konfigurieren**.

   Das Fenster **Eigenschaften: Echtzeitschutz für Dateien** wird geöffnet.

3. Wählen Sie in der Liste der Dateiressourcen des geschützten Geräts die Elemente aus, für die Sie eine vordefinierte Sicherheitsstufe festlegen möchten.

4. Wenn die Dateifreigabe nicht in der Liste enthalten ist, fügen Sie sie manuell hinzu:

   a. Klicken Sie auf **Hinzufügen**.

   b. Geben Sie in der Ordnerstruktur den Pfad des erforderlichen Objekts an oder geben Sie im Feld **Objekt** den Pfad an.

   Verwenden Sie bei Bedarf Sonderzeichen, um die Maske des Objektpfads einzugeben:

   - 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.

   Das Objekt **Dieser PC** in der Liste der Dateiressourcen des Computers enthält die folgenden Objekte: **Alle Festplatten**, **Alle Netzlaufwerke** und **Alle Wechseldatenträger**.

   c. Klicken Sie auf **OK**.

5. Vergewissern Sie sich, dass die ausgewählte Dateiressource zum Schutzbereich gehört.

6. Legen Sie eine vordefinierte Sicherheitsstufe für den ausgewählten Schutzbereich fest, indem Sie auf **Konfigurieren** klicken. Standardmäßig werden auf den gesamten Schutzbereich identische Sicherheitseinstellungen angewendet. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**. Sie können die standardmäßigen Sicherheitseinstellungen bearbeiten.

7. Speichern Sie die vorgenommenen Änderungen.

Sicherheitseinstellungen manuell anpassen

Standardmäßig werden in den Aufgaben zum Echtzeit-Computerschutz die gleichen Sicherheitseinstellungen verwendet wie für den gesamten Schutzbereich. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**.

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für einzelne Elemente in der Liste der Dateiressourcen des Geräts oder den Nodes in der Struktur festlegen.

Bei der Arbeit mit der Struktur der Dateiressourcen auf dem geschützten Gerät werden die Sicherheitseinstellungen, die für den ausgewählten übergeordneten Knoten konfiguriert wurden, automatisch für alle untergeordneten Knoten übernommen. Die Sicherheitseinstellungen des übergeordneten Knotens werden für untergeordnete Knoten, die gesondert konfiguriert werden, nicht übernommen.

So konfigurieren Sie die Sicherheitseinstellungen manuell (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**.
5. Gehen Sie im Fenster **Echtzeitschutz für Dateien** auf die Registerkarte **Schutzbereich**.
6. Wählen Sie die Ressource aus, deren Sicherheitseinstellungen Sie konfigurieren möchten.
7. Klicken Sie auf **Konfigurieren**.
8. Wählen Sie im folgenden Fenster die erforderliche Sicherheitsstufe aus und klicken Sie auf **Einstellungen**.
9. Nehmen Sie im Abschnitt auf der Registerkarte **Allgemein** die folgenden Einstellungen vor:
    - Objekte, die in den Schutzbereich aufgenommen werden sollen:
        - **Alle Objekte**. Kaspersky Embedded Systems Security untersucht alle Objekte.
        - **Objekte nach Format untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats. Die Liste der Dateiformate wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
        - **Objekte nach Erweiterungsliste der Antiviren-Datenbanken untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Erweiterungsliste wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
        - **Objekte nach angegebener Erweiterungsliste untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Liste der Erweiterungen wird vom Benutzer manuell angegeben.
    - Aktivieren oder deaktivieren Sie im Block **Optimierung** das Kontrollkästchen **Scan only new and modified files**.
    - Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:
        - **Archive untersuchen**
        - **Programmpakete untersuchen**
        - **Dateien in Microsoft Office-Formaten untersuchen**

- Dateien in E-Mail-Formaten untersuchen

10. Nehmen Sie im Abschnitt auf der Registerkarte **Aktionen** die folgenden Einstellungen vor:
    - Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
        - Informieren
        - Blockieren
        - **Zusätzliche Aktion ausführen**

          Wählen Sie in der Dropdown-Liste die Aktion:
            - **Desinfizieren**
            - **Disinfect. Delete if disinfection fails**
            - Löschen
            - Empfohlen
    - Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
        a. Deaktivieren oder aktivieren Sie das Kontrollkästchen Aktion auf die ausgewählten Objekttypen anwenden.
        b. Klicken Sie auf **Einstellungen** und wählen Sie die zu erkennenden Objekttypen aus.
    - Konfigurieren Sie die Aktionen für zusammengesetzte Dateien, die nicht geändert werden können: Deaktivieren oder aktivieren Sie das Kontrollkästchen Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann.
11. Nehmen Sie im Abschnitt auf der Registerkarte **Optimierung** die folgenden Einstellungen vor:
    - Unpack in the background compound files larger than (MB)
    - Untersuchung beenden, wenn sie länger dauert als (Sek.)
    - Limit für Untersuchung zusammengesetzter Objekte (MB)
    - iSwift-Technologie verwenden
    - iChecker-Technologie verwenden
12. Speichern Sie die neuen Sicherheitseinstellungen.

So konfigurieren Sie die Sicherheitseinstellungen manuell (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Echtzeit-Computerschutz** → **Echtzeitschutz für Dateien** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Wählen Sie die Registerkarte **Schutzbereich** aus.

6. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel hinzuzufügen und die Sicherheitseinstellungen dafür festzulegen.

   - Wählen Sie eine bestehende Regel aus und klicken Sie auf die Schaltfläche **Bearbeiten**.

   Das Fenster **Bereich bearbeiten** wird geöffnet.

7. Setzen Sie den Schalter **Aktiv**.

8. Wählen Sie eine Sicherheitsstufe aus und geben Sie die passenden Sicherheitseinstellungen an.

9. Wählen Sie im Abschnitt **Schutzmodus für Objekte** den Type des Objekts aus, das Sie in den Untersuchungsbereich aufnehmen möchten:

   - Objekte, die in den Schutzbereich aufgenommen werden sollen:

     - **Alle Objekte**. Kaspersky Embedded Systems Security untersucht alle Objekte.

     - **Objekte nach Format untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats. Die Liste der Dateiformate wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.

     - **Objekte nach Erweiterungsliste der Antiviren-Datenbanken untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Erweiterungsliste wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.

     - **Objekte nach angegebener Erweiterungsliste untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Liste der Erweiterungen wird vom Benutzer manuell angegeben.

10. Aktivieren oder deaktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien schützen**.

11. Geben Sie im Abschnitt **Schutz von zusammengesetzten Objekten** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

    - **Archive untersuchen**
    - **Programmpakete untersuchen**
    - **Dateien in Microsoft Office-Formaten untersuchen**
    - **Dateien in E-Mail-Formaten untersuchen**

12. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:

    - **Informieren**
    - **Blockieren**
    - **Zusätzliche Aktion ausführen**

      Wählen Sie in der Dropdown-Liste die Aktion:

      - **Desinfizieren**
      - **Desinfizieren – Löschen, wenn Desinfektion fehlschlägt**
      - **Löschen**
      - **Empfohlen**

13. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

    a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Aktion auf die ausgewählten Objekttypen anwenden**.

    b. Wenn das Kontrollkästchen aktiviert ist, klicken Sie auf **Einstellungen** und wählen Sie die zu erkennenden Objekttypen aus.

14. Konfigurieren Sie die Aktionen für zusammengesetzte Dateien, die nicht geändert werden können: Deaktivieren oder aktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann**.

15. Konfigurieren Sie im Abschnitt **Optimierung** die folgenden Einstellungen:

    - **Zusammengesetzte Dateien im Hintergrund entpacken**
    - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
    - **Limit für Untersuchung zusammengesetzter Objekte (MB)**
    - **iSwift-Technologie verwenden**
    - **iChecker-Technologie verwenden**

16. Speichern Sie die neuen Sicherheitseinstellungen.

So konfigurieren Sie die Sicherheitseinstellungen manuell (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Echtzeitschutz für Dateien** auf **Schutzbereich konfigurieren**.

   Das Fenster **Eigenschaften: Echtzeitschutz für Dateien** wird geöffnet.

3. Wählen Sie die Ressource aus, deren Sicherheitseinstellungen Sie konfigurieren möchten.

4. Klicken Sie auf **Konfigurieren**.

5. Wählen Sie im folgenden Fenster die erforderliche Sicherheitsstufe aus und klicken Sie auf **Einstellungen**.

6. Nehmen Sie im Abschnitt auf der Registerkarte **Allgemein** die folgenden Einstellungen vor:

- Objekte, die in den Schutzbereich aufgenommen werden sollen:
  - **Alle Objekte**. Kaspersky Embedded Systems Security untersucht alle Objekte.
  - **Objekte nach Format untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats. Die Liste der Dateiformate wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
  - **Objekte nach Erweiterungsliste der Antiviren-Datenbanken untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Erweiterungsliste wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
  - **Objekte nach angegebener Erweiterungsliste untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Liste der Erweiterungen wird vom Benutzer manuell angegeben.
- Aktivieren oder deaktivieren Sie im Block **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien schützen**.
- Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:
  - **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 der Programmpakete von Drittherstellern.
  - **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 Kaspersky Embedded Systems Security untersucht.
  - **Dateien in E-Mail-Formaten untersuchen**.

7. Nehmen Sie im Abschnitt auf der Registerkarte **Aktionen** die folgenden Einstellungen vor:

- Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
  - **Informieren**
  - **Blockieren**
  - **Zusätzliche Aktion ausführen**.

    Wählen Sie in der Dropdown-Liste die Aktion:
    - **Desinfizieren**
    - **Disinfect. Delete if disinfection fails**

- **Löschen**
- **Empfohlen**

- Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

  a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Aktion auf die ausgewählten Objekttypen anwenden**.

  b. Klicken Sie auf **Einstellungen** und wählen Sie die zu erkennenden Objekttypen aus.

- Konfigurieren Sie die Aktionen für zusammengesetzte Dateien, die nicht geändert werden können: Deaktivieren oder aktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann**.

8. Nehmen Sie im Abschnitt auf der Registerkarte **Optimierung** die folgenden Einstellungen vor:

   - **Unpack in the background compound files larger than (MB)**
   - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
   - **Limit für Untersuchung zusammengesetzter Objekte (MB)**
   - **iSwift-Technologie verwenden**
   - **iChecker-Technologie verwenden**

9. Speichern Sie die neuen Sicherheitseinstellungen.

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 Embedded Systems Security ist 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 Embedded Systems Security innerhalb des Containers wird nicht unterstützt.

Kaspersky Embedded Systems Security bietet Sicherheit für Container. Außerdem ermöglicht die Komponente Kontrolle des Programmstarts die Verwaltung von Programmen in Containern. Die Komponente Kontrolle des Programmstarts wird für Container genauso konfiguriert wie für Anwendungen, die auf dem Computer installiert sind. Die Komponente 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.
- Die Untersuchung von Containern, die im WSL2-Modus (Windows Subsystem for Linux v2) (Docker Wine) wird 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 Echtzeitschutz für 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). Wenn die Desinfektion des gefundenen Objekts fehlschlägt, kann Kaspersky Embedded Systems Security den Container anhalten. Das Anhalten von Containern standardmäßig aktiviert.

So konfigurieren Sie die Untersuchung von Containern (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**.
5. 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**. Ist das Kontrollkästchen aktiviert, untersucht das Programm den Container nur beim Start des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.
6. Speichern Sie die neuen Sicherheitseinstellungen.

So konfigurieren Sie die Untersuchung von Containern (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** und klicken Sie auf die Schaltfläche **Anpassen**.
5. 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**. Ist das Kontrollkästchen aktiviert, untersucht das Programm den Container nur beim Start des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.
6. Speichern Sie die neuen Sicherheitseinstellungen.

So konfigurieren Sie die Untersuchung von Containern (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Echtzeitschutz für Dateien** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Echtzeitschutz für Dateien** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Echtzeitschutz für Dateien** wird geöffnet.
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**. Ist das Kontrollkästchen aktiviert, untersucht das Programm den Container nur beim Start des Containers. Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm den Container kontinuierlich in Echtzeit.
4. Speichern Sie die vorgenommenen Änderungen.

Verwendung von KSN

Um Benutzercomputer effektiver zu schützen, verwendet Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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

So aktivieren Sie die Verwendung von Kaspersky Security Network (in der Kaspersky Security Center-Verwaltungskonsole)

1. Wählen Sie in der Struktur der Kaspersky Security Network-Verwaltungskonsole den Ordner **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie von Kaspersky Embedded Systems Security aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster in der Liste den Abschnitt **Echtzeit-Computerschutz → KSN-Nutzung** aus.
4. Klicken Sie auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Kaspersky Security Network**, um die Komponente zu aktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Embedded Systems 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.

   Kaspersky Embedded Systems Security verwendet standardmäßig den erweiterten Modus von Kaspersky Security Network. Im erweiterten Modus von Kaspersky Security Network überträgt Kaspersky Embedded Systems Security zusätzliche Daten an Kaspersky.
6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Erweiterten KSN-Modus aktivieren**.
7. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verwendung von Kaspersky Security Network aktiviert ist, verwendet Kaspersky Embedded Systems Security die Informationen über die Reputation von Dateien, Webressourcen und Programmen, die aus Kaspersky Security Network empfangen werden.

So aktivieren Sie die Verwendung von Kaspersky Security Network (in der Konsole für Kaspersky Embedded Systems Security)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Kaspersky Security Network** aus.
3. Klicken Sie im Programmhauptfenster auf **Eigenschaften**.
4. Aktivieren Sie das Kontrollkästchen **Kaspersky Security Network**, um die Komponente zu aktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Embedded Systems 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.

   Kaspersky Embedded Systems Security verwendet standardmäßig den erweiterten Modus von Kaspersky Security Network. Im erweiterten Modus von Kaspersky Security Network überträgt Kaspersky Embedded Systems Security zusätzliche Daten an Kaspersky.
5. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Erweiterten KSN-Modus aktivieren**.
6. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verwendung von Kaspersky Security Network aktiviert ist, verwendet Kaspersky Embedded Systems Security die Informationen über die Reputation von Dateien, Webressourcen und Programmen, die aus Kaspersky Security Network empfangen werden.

So aktivieren Sie die Verwendung von Kaspersky Security Network (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zum Abschnitt **Echtzeit-Computerschutz → KSN-Nutzung** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Kaspersky Security Network aktivieren**, um die Komponente zu aktivieren.

   Wenn Sie die Verwendung von KSN aktiviert haben, zeigt Kaspersky Embedded Systems Security die Erklärung zu Kaspersky Security Network an. Wenn Sie damit einverstanden sind, akzeptieren Sie die Nutzungsbedingungen von Kaspersky Security Network.

   Kaspersky Embedded Systems Security verwendet standardmäßig den erweiterten Modus von Kaspersky Security Network. Im erweiterten Modus von Kaspersky Security Network überträgt Kaspersky Embedded Systems Security zusätzliche Daten an Kaspersky.
6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Erweiterten KSN-Modus aktivieren**.
7. Speichern Sie die vorgenommenen Änderungen.

Wenn die Verwendung von Kaspersky Security Network aktiviert ist, hat dies hat zur Folge, dass Kaspersky Embedded Systems Security die Informationen über die Reputation von Dateien, Webressourcen und Programmen verwendet, die aus Kaspersky Security Network empfangen werden.

Status der Verwendung von Kaspersky Security Network

Während die Aufgabe *KSN-Nutzung* ausgeführt wird, können Sie Echtzeit-Informationen über die Anzahl der von Kaspersky Embedded Systems Security verarbeiteten Objekte anzeigen (ab dem Aufgabenstart bis zum aktuellen Zeitpunkt).

So zeigen Sie eine Statistik zur KSN-Nutzung an:

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Echtzeit-Computerschutz** aus.
2. Wählen Sie den untergeordneten Knoten **Kaspersky Security Network** aus.

   Im Ergebnisbereich im Abschnitt **Statistik** wird die Aufgabenstatistik angezeigt (siehe folgende Tabelle).

KSN-Statistik

Feld	Beschreibung
Dateianfragen gesendet	Anzahl der von Kaspersky Embedded Systems Security an KSN gesendeten Reputationabfragen für Objekte.
Nicht vertrauenswürdige Dateien in KSN	Anzahl der Objekte mit nicht vertrauenswürdiger Reputation, die von KSN zugewiesen wurde.

Feld	Beschreibung
Fehler beim Senden von Anfragen	Anzahl der fehlerhaft verarbeiteten KSN-Anfragen.
Statistik erstellt	Anzahl der erstellten Statistikpakete, die an KSN gesendet wurden.
Entfernte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security erfolgreich gelöscht wurden.
Nicht entfernte Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos zu entfernen versucht hat, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Ins Backup verschoben	Anzahl der Objekte, die von Kaspersky Embedded Systems Security erfolgreich ins Backup kopiert wurden.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security nicht ins Backup kopieren konnte (z. B. da zu wenig Speicherplatz auf der Festplatte vorhanden war). Dateien, die nicht in den Backup verschoben werden konnten, werden durch das Programm weder desinfiziert noch gelöscht.
Eingeschränkter Modus	Der Status gibt an, ob die Anwendung Datei-Reputationsanforderungen in einem begrenzten Modus sendet. Im begrenzten Modus sendet Kaspersky Embedded Systems Security gemäß den Empfehlungen der Spezialisten von Kaspersky nur einen Teil der Datei-Reputationsanforderungen.

Die Werte der Felder **Entfernte Objekte**, **Nicht entfernte Objekte**, **Ins Backup verschoben**, **Nicht ins Backup verschobene Objekte** werden aus der Statistik der Komponente Echtzeitschutz für Dateien generiert.

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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security die Datei als *Nicht vertrauenswürdig* und führt die für erkannte Bedrohungen vorgesehene Aktion aus.

In einigen Fällen fordert Kaspersky Embedded Systems Security jedoch möglicherweise nicht die Reputation eines Objekts im KSN/KPSN an. Wenn dies der Fall ist, empfängt Kaspersky Embedded Systems Security keine Daten aus der lokalen Reputationsdatenbank von KPSN. Kaspersky Embedded Systems 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 die Reputationsanforderungen an KSN/KPSN in einem Cache. 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.

KSN Proxy-Einstellungen

Benutzercomputer, die vom Administrationsserver für Kaspersky Security Center verwaltet werden, können zur Interaktion mit KSN den Dienst KSN Proxy verwenden.

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 Dienst KSN Proxy 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. Wenn KSN Proxy nicht verfügbar ist, müssen Sie überprüfen, ob das Gerät als KSN-Proxyserver funktioniert. Überprüfen Sie dazu Folgendes:

- 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 zur Konfiguration von KSN Proxy finden Sie in der Hilfe zu Kaspersky Security Center. Außerdem können Sie KSN Proxy für bestimmte Computer über die Kaspersky Embedded Systems Security-Richtlinie aktivieren oder deaktivieren.

So aktivieren Sie KSN Proxy (in der Kaspersky Security Center-Verwaltungskonsole)

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

2. Wählen Sie die gewünschte Richtlinie von Kaspersky Embedded Systems Security aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster in der Liste den Abschnitt **Echtzeit-Computerschutz** → KSN-Nutzung aus.

4. Klicken Sie auf **Einstellungen**.

5. Verwenden Sie im Block **KSN Proxy-Einstellungen** 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 Embedded Systems Security die KSN-Server, wenn der Dienst KSN Proxy nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird).

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie KSN Proxy (in der Konsole für Kaspersky Embedded Systems Security)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Kaspersky Security Network** aus.
3. Klicken Sie im Programmhauptfenster auf **Eigenschaften**.
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 Embedded Systems Security die KSN-Server, wenn der Dienst KSN Proxy nicht verfügbar ist. Die KSN-Server können sich sowohl bei Kaspersky als auch bei Drittanbietern befinden (wenn Kaspersky Private Security Network verwendet wird).

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie KSN Proxy (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz** → **KSN-Nutzung** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Administrationsserver als KSN-Proxyserver verwenden**, um KSN Proxy zu aktivieren bzw. 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 Embedded Systems 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).

7. Speichern Sie die vorgenommenen 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.

Exploit-Prävention

Kaspersky Embedded Systems Security bietet eine Möglichkeit zum Schutz des Prozess-Speichers vor Exploits. Diese Funktionalität wird durch die Komponente Exploit-Prävention implementiert. Mit ihr können Sie den Aktivitätsstatus der Komponente ändern und den Schutz von Prozessen vor Exploits konfigurieren.

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 Embedded Systems Security den Start dieser Datei oder informiert den Benutzer. Die Komponente schützt den Prozess-Speicher vor Exploits. Dazu wird ein externer Prozess-Schutzagent (Protection Agent) in den geschützten Prozess eingefügt.

Der *Prozess-Schutzagent* (im Folgenden *Agent* genannt) ist ein dynamisch ladendes Modul von Kaspersky Embedded Systems Security, das in die geschützten Prozesse eingefügt wird, um ihre Integrität zu überwachen und die Risiken einer Ausnutzung von Schwachstellen zu mindern.

Das Funktionieren des Agenten innerhalb des geschützten Prozesses ist abhängig vom Start und Beenden dieses Prozesses: Der Agent kann nur bei einem Neustart des Prozesses, der zur Liste der geschützten Prozesse hinzugefügt wurde, erstmals in den Prozess geladen werden. Auch das Entladen des Agenten aus dem Prozess nach seiner Entfernung aus der Liste der geschützten Prozesse ist nur nach einem Neustart des Prozesses möglich.

Das Entladen des Agenten aus den geschützten Prozessen setzt voraus, dass die Prozesse beendet werden: Beim Entfernen der Komponente „Exploit-Prävention“ friert das Programm die Umgebung ein und erzwingt das Entladen des Agenten aus den geschützten Prozessen. Wenn der Agent während der Deinstallation der Komponente in einen der geschützten Prozesse eingeschleust wird, müssen Sie den betroffenen Prozess beenden. Möglicherweise muss das geschützte Gerät neu gestartet werden (z. B. wenn der Systemprozess geschützt ist).

Wenn Anzeichen für einen Exploit-Angriff auf den geschützten Prozess gefunden werden, führt Kaspersky Embedded Systems Security eine der folgenden Aktionen aus:

- Prozess wird bei einem Exploit-Versuch beendet
- Benachrichtigung über die Ausnutzung einer Schwachstelle im Prozess wird ausgelöst

Sie können den Schutz von Prozessen auf eine der folgenden Weisen beenden:

- Komponente deinstallieren
- Prozess aus der Liste der geschützten Prozesse entfernen und neu starten

Modus der Exploit-Prävention

Sie können die getroffenen Aktionen zur Minderung der Risiken einer Ausnutzung von Schwachstellen in geschützten Prozessen anpassen, indem Sie einen von zwei Modi auswählen:

- **Verbieten**. In diesem Modus beendet Kaspersky Embedded Systems Security einen geschützten Prozess beim Fund eines Exploit-Versuchs, wenn ein aktives Verfahren zur Risikominderung angewendet wird.

  Wenn eine versuchte Ausnutzung einer Schwachstelle in einem geschützten Prozess gefunden wird, die im Betriebssystem als kritisch eingestuft ist, beendet Kaspersky Embedded Systems Security den Prozess nicht – unabhängig vom Modus, der in den Einstellungen der Komponente „Exploit-Prävention“ angegeben ist.

- **Informieren** (bei der Arbeit in der Kaspersky Security Center Web Console – **Informieren**). Wenden Sie diesen Modus an, um mithilfe von Ereignissen im Sicherheitsprotokoll Daten über Exploits in geschützten Prozessen zu erhalten. Der missbräuchlich verwendete Prozess wird auch weiterhin ausgeführt.

  Wenn dieser Modus ausgewählt ist, erstellt Kaspersky Embedded Systems Security Ereignisse, um alle Versuche zu protokollieren, mit denen Schwachstellen aufgedeckt werden sollen. Standardmäßig ausgewählt.

Exploit-Prävention aktivieren und deaktivieren

Kaspersky Embedded Systems Security kann ausführbare Dateien überwachen, die von verwundbaren Programmen ausgeführt werden. Wenn Kaspersky Embedded Systems Security erkennt, dass eine ausführbare Datei aus einem verwundbaren Programm nicht vom Benutzer gestartet wurde, führt Kaspersky Embedded Systems Security die ausgewählte Aktion aus (beispielsweise wird der Vorgang blockiert).

So aktivieren oder deaktivieren Sie die Exploit-Prävention (in der Kaspersky Security Center-Verwaltungskonsole)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie von Kaspersky Embedded Systems Security aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster in der Liste den Abschnitt **Echtzeit-Computerschutz** → **Exploit-Prävention** aus.
4. Klicken Sie auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Exploit-Prävention**, um die Komponente zu aktivieren.
6. Wählen Sie auf der Registerkarte **Allgemein** einen Modus für die Exploit-Prävention aus: **Verbieten** oder **Informieren**.
7. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Exploit-Prävention**, um die Komponente zu deaktivieren.
8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Exploit-Prävention (in der Konsole für Kaspersky Embedded Systems Security)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Exploit-Prävention** aus.
3. Klicken Sie im Programmhauptfenster auf **Eigenschaften**.
4. Aktivieren Sie das Kontrollkästchen **Exploit-Prävention**, um die Komponente zu aktivieren.
5. Wählen Sie auf der Registerkarte **Allgemein** einen Modus für die Exploit-Prävention aus: **Verbieten** oder **Informieren**.
6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Exploit-Prävention**, um die Komponente zu deaktivieren.
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Exploit-Prävention (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz** → **Exploit-Prävention** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Dadurch wird ein Fenster geöffnet. Aktivieren Sie in diesem Fenster unter **Modus der Exploit-Prävention** das Kontrollkästchen **Exploit von anfälligen Prozessen verhindern**, um die Komponente zu aktivieren.
6. Wählen Sie einen Modus für die Exploit-Prävention aus: **Blockieren** oder **Informieren**.
7. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Exploit von anfälligen Prozessen verhindern**, um die Komponente zu deaktivieren.
8. Speichern Sie die vorgenommenen Änderungen.

Schutz des Arbeitsspeichers aktivieren und deaktivieren

Kaspersky Embedded Systems Security blockiert externe Prozesse, die versuchen, Zugriff auf Systemprozesse zu erhalten. Der Schutz für den Arbeitsspeicher von Systemprozessen ist standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie den Schutz des Arbeitsspeichers (in der Kaspersky Security Center-Verwaltungskonsole)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie von Kaspersky Embedded Systems Security aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.

3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster in der Liste den Abschnitt **Echtzeit-Computerschutz → Exploit-Prävention** aus.

4. Klicken Sie auf **Einstellungen**.

5. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**.

6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie den Schutz des Arbeitsspeichers (in der Konsole für Kaspersky Embedded Systems Security)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.

2. Wählen Sie den untergeordneten Knoten **Exploit-Prävention** aus.

3. Klicken Sie im Programmhauptfenster auf **Eigenschaften**.

4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**.

5. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen aktivieren**.

6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie den Schutz des Arbeitsspeichers (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Echtzeit-Computerschutz → Exploit-Prävention** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Aktivieren Sie im folgenden Fenster im Block **Schutz für den Arbeitsspeicher von Systemprozessen** das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen**.

6. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Schutz für den Arbeitsspeicher von Systemprozessen**, um den Schutz für den Arbeitsspeicher von Systemprozessen zu deaktivieren.

7. Speichern Sie die vorgenommenen Änderungen.

Liste der geschützten Prozesse erstellen

Die Komponente Exploit-Prävention schützt standardmäßig mehrere Prozesse. Das Programm kann automatisch eine Liste der geschützten Prozesse erstellen. Außerdem können Sie Prozesse manuell hinzufügen oder entfernen.

So verwalten Sie die Liste der geschützten Prozesse (in der Kaspersky Security Center-Verwaltungskonsole)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Richtlinien** aus.
2. Wählen Sie die gewünschte Richtlinie von Kaspersky Embedded Systems Security aus und öffnen Sie mit einem Doppelklick das Fenster mit den Richtlinieneigenschaften.
3. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster in der Liste den Abschnitt **Echtzeit-Computerschutz** → **Exploit-Prävention** aus.
4. Klicken Sie auf **Einstellungen**.
5. Wählen Sie auf der Registerkarte **Geschützte Prozesse** eine der folgenden Optionen aus, um Prozesse vor dem Einschleusen bösartigen Codes zu schützen:
   - **Geschützte Prozesse automatisch erkennen**. Wenn Sie diese Option auswählen, erstellt das Programm automatisch eine Liste der geschützten Prozesse.
   - **Nur Prozesse aus der unten stehenden Liste schützen**. Wenn Sie diese Option auswählen, können Sie die zu schützenden Prozesse auswählen.
6. Wenn Sie **Nur Prozesse aus der unten stehenden Liste schützen** ausgewählt haben, können Sie die Liste der geschützten Prozesse wie folgt bearbeiten:
   - Klicken Sie bei Bedarf auf **Hinzufügen** und wählen Sie einen Prozess aus, den Sie zur Liste der geschützten Prozesse hinzufügen möchten.
   - Wenn Sie einen Prozess aus der Liste der geschützten Prozesse löschen möchten, wählen Sie den Prozess in der Liste aus und klicken Sie auf **Löschen**.

     Die Schaltfläche **Löschen** wird verfügbar, nachdem Sie einen oder mehrere Prozesse in der Liste ausgewählt haben.
7. Speichern Sie die vorgenommenen Änderungen.

So verwalten Sie die Liste der geschützten Prozesse (in der Konsole für Kaspersky Embedded Systems Security)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Exploit-Prävention** aus.
3. Klicken Sie im Programmhauptfenster auf **Eigenschaften**.
4. Wählen Sie auf der Registerkarte **Geschützte Prozesse** eine der folgenden Optionen aus, um Prozesse vor dem Einschleusen bösartigen Codes zu schützen:
   - **Geschützte Prozesse automatisch erkennen**. Wenn Sie diese Option auswählen, erstellt das Programm automatisch eine Liste der geschützten Prozesse.
   - **Nur Prozesse aus der unten stehenden Liste schützen**. Wenn Sie diese Option auswählen, können Sie die zu schützenden Prozesse auswählen.

5. Wenn Sie **Nur Prozesse aus der unten stehenden Liste schützen** ausgewählt haben, können Sie die Liste der geschützten Prozesse wie folgt bearbeiten:

   - Klicken Sie bei Bedarf auf **Hinzufügen** und wählen Sie einen Prozess aus, den Sie zur Liste der geschützten Prozesse hinzufügen möchten.

   - Wenn Sie einen Prozess aus der Liste der geschützten Prozesse löschen möchten, wählen Sie den Prozess in der Liste aus und klicken Sie auf **Löschen**.

     Die Schaltfläche **Löschen** wird verfügbar, nachdem Sie einen oder mehrere Prozesse in der Liste ausgewählt haben.

6. Speichern Sie die vorgenommenen Änderungen.

So verwalten Sie die Liste der geschützten Prozesse (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zum Abschnitt **Echtzeit-Computerschutz → Exploit-Prävention** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Wählen Sie unter **Liste mit geschützten Prozessen** eine der folgenden Optionen aus, um Prozesse vor dem Einschleusen bösartigen Codes zu schützen:

   - **Geschützte Prozesse automatisch erkennen**. Wenn Sie diese Option auswählen, erstellt das Programm automatisch eine Liste der geschützten Prozesse.

   - **Nur Prozesse aus der unten stehenden Liste schützen**. Wenn Sie diese Option auswählen, können Sie zu schützende Prozesse hinzufügen, bearbeiten und entfernen.

6. Wenn Sie **Nur Prozesse aus der unten stehenden Liste schützen** ausgewählt haben, führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf **Hinzufügen**, um das Fenster **Geschützter Prozess** zu öffnen und gehen Sie in diesem Fenster wie folgt vor:

     a. Aktivieren Sie das Kontrollkästchen **Geschützter Prozess**.

     b. Tragen Sie im Feld **Prozessname** den Namen des Prozesses ein.

     c. Speichern Sie die vorgenommenen Änderungen.

   - Bearbeiten Sie bei Bedarf die Einstellungen für den Prozess in der Liste der geschützten Prozesse. Gehen Sie hierzu wie folgt vor:

     a. Wählen Sie einen Prozess aus der Liste der geschützten Prozessen aus.

     b. Klicken Sie auf **Ändern**. Die Schaltfläche **Ändern** wird verfügbar, nachdem Sie einen oder mehrere Prozesse in der Liste ausgewählt haben.

     c. Aktivieren oder deaktivieren Sie im Fenster **Geschützter Prozess** das Kontrollkästchen **Geschützter Prozess**.

d. Ändern Sie bei Bedarf den Namen des Prozesses im Feld **Prozessname**.

e. Speichern Sie die vorgenommenen Änderungen.

- Bei Bedarf können Sie einen Prozess aus der Liste der geschützten Prozesse entfernen. Gehen Sie hierzu wie folgt vor:

  a. Wählen Sie einen oder mehrere Prozesse aus der Liste der geschützten Prozesse aus.

  b. Klicken Sie auf **Löschen**. Die Schaltfläche **Löschen** wird verfügbar, nachdem Sie einen oder mehrere Prozesse in der Liste ausgewählt haben.

7. Speichern Sie die vorgenommenen Änderungen.

Rollback von schädlichen Aktionen

Mithilfe der Komponente „Rollback von schädlichen Aktionen“ kann Kaspersky Embedded Systems Security Aktionen rückgängig machen, die von schädlichen Programmen im Betriebssystem ausgeführt wurden.

Beim Rollback von Schadsoftware-Aktionen im Betriebssystem führt Kaspersky Embedded Systems Security die folgenden Aktionen aus:

- **Dateiaktivität**
  - Löschen von ausführbaren 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**.
  - Das Programm stellt Dateien nur auf Geräten mit dem Dateisystem NTFS und FAT32 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.
  - Veränderungen von Dateien, die über eine Netzwerkschnittstelle ausgeführt wurden, werden vom Programm nicht kontrolliert. (Beispiel: Eine Datei wurde in einen gemeinsamen Ordner verschoben und der Prozess wurde per Fernzugriff von einem anderen Computer gestartet.)
- **Aktivität der Registrierung**
  - löscht Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden.

  Kaspersky Embedded Systems Security stellt Partitionen und Registrierungsschlüssel, die von Schadsoftware erstellt wurden, nicht wieder her.
- **Systemaktivität**
  - beendet Prozesse, die von Schadsoftware gestartet wurden.
  - beendet Prozesse, in die Schadsoftware eingedrungen ist.

Kaspersky Embedded Systems Security setzt Prozesse, die von Schadsoftware beendet wurden, nicht fort.

- **Netzwerkaktivität**
  - verbietet die Netzwerkaktivität von Schadsoftware.
  - verbietet die Netzwerkaktivität von Prozessen, in die Schadsoftware eingedrungen ist.

Ein Rollback der Aktionen eines schädlichen Programms kann von der Komponente Echtzeitschutz für Dateien oder während einer Untersuchung auf Befehl initiiert 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 oder deaktivieren Sie die Komponente Rollback von schädlichen Aktionen (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Echtzeit-Computerschutz**.
4. Klicken Sie im Block **Rollback von schädlichen Aktionen** auf **Einstellungen**.
5. Das Fenster **Rollback von schädlichen Aktionen** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
6. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, wenn Sie das Rollback von schädlichen Aktionen aktivieren möchten.
   - Deaktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, wenn Sie das Rollback von schädlichen Aktionen deaktivieren möchten.
7. Klicken Sie im Fenster **Rollback von schädlichen Aktionen** auf **OK**.
8. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

So aktivieren oder deaktivieren Sie die Komponente Rollback von schädlichen Aktionen (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie den Abschnitt **Echtzeit-Computerschutz** aus.

5. Klicken Sie im Block **Rollback von schädlichen Aktionen** auf **Anpassen**.

6. Das Fenster **Rollback von schädlichen Aktionen** wird geöffnet.

7. Führen Sie einen der folgenden Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, wenn Sie das Rollback von schädlichen Aktionen aktivieren möchten.

   - Deaktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, wenn Sie das Rollback von schädlichen Aktionen deaktivieren möchten.

8. Klicken Sie im Fenster **Rollback von schädlichen Aktionen** auf **OK**.

9. Klicken Sie im Fenster **<Name der Richtlinie>** auf **Speichern**.

So aktivieren oder deaktivieren Sie die Komponente Rollback von schädlichen Aktionen (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Echtzeit-Computerschutz → Rollback von schädlichen Aktionen** aus.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Rollback von schädlichen Aktionen** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

3. Führen Sie einen der folgenden Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, wenn Sie das Rollback von schädlichen Aktionen aktivieren möchten.

   - Deaktivieren Sie das Kontrollkästchen **Rollback von schädlichen Aktionen**, wenn Sie das Rollback von schädlichen Aktionen deaktivieren möchten.

4. Klicken Sie im Fenster **Rollback von schädlichen Aktionen** auf **OK**.

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 Embedded Systems Security die ausgewählte Reaktion aus. Diese Funktionalität von Kaspersky Embedded Systems Security, die auf Vorlagen für gefährliches Verhalten beruht, bietet einen proaktiven Computerschutz.

Verschlüsselungsschutz für lokale Ordner aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Komponente Verhaltensanalyse (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Allgemein**.
7. Verwenden Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung lokaler Ordner aktivieren**, um die Option zu aktivieren oder deaktivieren. Ist dieses Kontrollkästchen aktiviert, so führt Kaspersky Embedded Systems Security bei schädlicher Aktivität die unten angegebene Aktion aus.
8. 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 Embedded Systems Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.
   - **Blockieren**. Wenn dieses Element gewählt wird, beendet Kaspersky Embedded Systems Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.
   - **Informieren**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Embedded Systems Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren oder deaktivieren Sie die Komponente Verhaltensanalyse (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz** → **Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Verhaltensanalyse** wird geöffnet.
5. Verwenden Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Allgemein**.
7. Verwenden Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung lokaler Ordner aktivieren**, um die Option zu aktivieren oder deaktivieren. Ist dieses Kontrollkästchen aktiviert, so führt Kaspersky Embedded Systems Security bei schädlicher Aktivität die unten angegebene Aktion aus.
8. Wählen Sie die entsprechende Aktion im Block **Wenn eine externe Verschlüsselung freigegebener Ordner erkannt wird**:

   - **Löschen**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Embedded Systems Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.
   - **Blockieren**. Wenn dieses Element gewählt wird, beendet Kaspersky Embedded Systems Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.
   - **Informieren**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Embedded Systems Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren oder deaktivieren Sie die Komponente Verhaltensanalyse (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz** → **Verhaltenserkennung** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Verhaltensanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Verhaltensanalyse** geöffnet.
3. Aktivieren Sie das Kontrollkästchen **Verhaltensanalyse**.
4. Gehen Sie auf die Registerkarte **Allgemein**.
5. Verwenden Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung lokaler Ordner aktivieren**, um die Option zu aktivieren oder deaktivieren. Ist dieses Kontrollkästchen aktiviert, so führt Kaspersky Embedded Systems Security bei schädlicher Aktivität die unten angegebene Aktion aus.

6. Wählen Sie die entsprechende Aktion im Block **Wenn eine externe Verschlüsselung freigegebener Ordner erkannt wird**:

   - **Löschen**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so löscht Kaspersky Embedded Systems Security die ausführbare Datei der Schadsoftware und legt eine Backup-Kopie der Datei an.

   - **Blockieren**. Wenn dieses Element gewählt wird, beendet Kaspersky Embedded Systems Security beim Auffinden einer schädlichen Programmaktivität die betreffende Anwendung.

   - **Informieren**. Ist dieses Element ausgewählt und es wird eine schädliche Programmaktivität erkannt, so fügt Kaspersky Embedded Systems Security Informationen über die schädliche Aktivität dieses Programms zur Liste der aktiven Bedrohungen hinzu.

7. Speichern Sie die vorgenommenen Änderungen.

Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern

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 Funktion zum Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern gewährleistet die Analyse von Aktivitäten in gemeinsamen Ordnern. Falls die Aktivität mit einer Vorlage für gefährliches Verhalten übereinstimmt, das für eine externe Verschlüsselung charakteristisch ist, so führt Kaspersky Embedded Systems Security die ausgewählte Aktion aus.

Wenn ein Versuch erkannt wird, Dateien in freigegebenen Ordnern zu ändern, führt Kaspersky Embedded Systems Security 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.

- Es wird ein Eintrag zu den Berichten der lokalen Programmoberfläche hinzugefügt und Informationen über erkannte schädliche Aktivitäten werden an Kaspersky Security Center gesendet.

- 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 zur externen Verschlüsselung von Dateien in freigegebenen Ordnern erkannt wird, blockiert Kaspersky Embedded Systems Security die Sitzung des Remote-Benutzers für eine Stunde (Standardwert).

Die Funktion für den Schutz vor der externen Verschlüsselung von gemeinsamen Ordnern ist nach der Installation von Kaspersky Embedded Systems Security bis zum Neustart des Computers beschränkt.

So aktivieren oder deaktivieren Sie den Schutz vor der externen Verschlüsselung freigegebener Ordner in der (Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. Verwenden Sie das Kontrollkästchen **Freigegebene Ordner schützen**, um die Option zu aktivieren oder deaktivieren.
8. Wählen Sie die entsprechende Aktion im Block **Schutz vor der externen Verschlüsselung freigegebener Ordner**:

   - **Verbindung blockieren für n Minuten**. Ist diese Option ausgewählt und Kaspersky Embedded Systems Security erkennt einen Versuch, Dateien in gemeinsamen Ordnern zu ändern, so blockiert die App den Zugriff auf die Dateiänderung (schreibgeschützt) 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 ein Versuch zur Änderung von Dateien in freigegebenen Ordnern erkannt wird, fügt Kaspersky Embedded Systems Security Informationen über diesen Änderungsversuch von Dateien in freigegebenen Ordnern zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über den Fund schädlicher Aktivitäten an Kaspersky Security Center.

9. Erstellen Sie bei Bedarf einen Schutzbereich und konfigurieren Sie die Ausnahmen.

10. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So aktivieren oder deaktivieren Sie den Schutz vor der externen Verschlüsselung freigegebener Ordner (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Echtzeit-Computerschutz** → **Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Verhaltensanalyse** wird geöffnet.

5. Verwenden Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.

7. Verwenden Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung freigegebener Ordner aktivieren**, um die Option zu aktivieren oder deaktivieren.

8. Wählen Sie die entsprechende Aktion im Block **Erkennung von externer Verschlüsselung**:

   - **Verbindung blockieren**. Ist diese Option ausgewählt und Kaspersky Embedded Systems Security erkennt einen Versuch, Dateien in freigegebenen Ordnern zu ändern, so blockiert das Programm den Zugriff auf die Dateiänderung (schreibgeschützt) für die Sitzung, die die schädliche Aktivität initiiert hat, und legt Backup-Kopien für die veränderten Dateien an.

     Ist die Komponente „Rollback von schädlichen Aktionen" aktiviert und die Option **Verbindung blockieren** ausgewählt, so werden veränderte Dateien aus den Backup-Kopien wiederhergestellt.

   - **Informieren**. Wenn diese Option ausgewählt ist und ein Versuch zur Änderung von Dateien in freigegebenen Ordnern erkannt wird, fügt Kaspersky Embedded Systems Security Informationen über diesen Änderungsversuch von Dateien in freigegebenen Ordnern zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über den Fund schädlicher Aktivitäten an Kaspersky Security Center.

9. Erstellen Sie bei Bedarf einen Schutzbereich und konfigurieren Sie die Ausnahmen.

10. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So aktivieren oder deaktivieren Sie den Schutz von freigegebenen Ordnern vor externer Verschlüsselung (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Verhaltenserkennung** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Verhaltensanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Verhaltensanalyse** geöffnet.
3. Aktivieren Sie das Kontrollkästchen **Verhaltensanalyse**.
4. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
5. Verwenden Sie das Kontrollkästchen **Freigegebene Ordner schützen**, um die Option zu aktivieren oder deaktivieren.
6. Wählen Sie die entsprechende Aktion im Block **Schutz vor der externen Verschlüsselung freigegebener Ordner**:

   - **Verbindung blockieren für n Minuten**. Ist diese Option ausgewählt und Kaspersky Embedded Systems Security erkennt einen Versuch, Dateien in gemeinsamen Ordnern zu ändern, so blockiert die App den Zugriff auf die Dateiänderung (schreibgeschützt) für die Sitzung, die die schädliche Aktivität initiiert hat, und erstellt Backup-Kopien der veränderten Dateien.

     Wenn die Komponente Rollback von schädlichen Aktionen aktiviert ist und die Option **Verbindung blockieren für n Minuten** ausgewählt ist, werden die veränderten Dateien aus Backup-Kopien wiederhergestellt.

   - **Informieren**. Wenn diese Option ausgewählt ist und ein Versuch zur Änderung von Dateien in freigegebenen Ordnern erkannt wird, fügt Kaspersky Embedded Systems Security Informationen über diesen Änderungsversuch von Dateien in freigegebenen Ordnern zur Liste der aktiven Bedrohungen hinzu, fügt den Berichten der lokalen Programmoberfläche einen Eintrag hinzu und sendet Informationen über den Fund schädlicher Aktivitäten an Kaspersky Security Center.
7. Erstellen Sie bei Bedarf einen Schutzbereich und konfigurieren Sie die Ausnahmen.
8. Speichern Sie die vorgenommenen Änderungen.

Schutzbereich bearbeiten

Ein *Schutzbereich* ist eine Liste mit Pfaden zu freigegebenen Ordnern, in denen Kaspersky Embedded Systems Security die Dateiaktivität überwacht. Kaspersky Embedded Systems Security unterstützt bei der Eingabe einer Maske sowohl Umgebungsvariablen als auch die Zeichen `*` und `?`: Standardmäßig identifiziert das Programm freigegebene Ordner automatisch und überwacht die Dateiaktivität in allen Ordnern.

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. Fehlalarme können beispielsweise durch die Komponente Verhaltensanalyse ausgelöst werden, wenn der Benutzer in einem freigegebenen 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 freigegebenen Ordner ablegen, fügen Sie diesen Ordner den Ausnahmen hinzu.

Sie können auch Computer ausschließen, wenn Sie möchten, dass Versuche zur externen Verschlüsselung, die von diesen Computern stammen, ignoriert werden.

So konfigurieren Sie den Schutzbereich (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. Klicken Sie im Block **Schutzbereich** auf **Konfigurieren**.
8. Wählen Sie im folgenden Fenster den Modus **Nur die angegebenen freigegebenen Ordner** aus.
9. Klicken Sie auf **Hinzufügen**.
10. 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.

11. Klicken Sie auf **OK**.
12. Legen Sie bei Bedarf Ausnahmen für den Schutzbereich fest:

    a. Klicken Sie im Block **Ausnahmen** auf **Konfigurieren**.

    b. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

    c. Geben Sie im folgenden Fenster 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 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.

13. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie den Schutzbereich (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz** → **Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Verhaltensanalyse** wird geöffnet.
5. Verwenden Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. Wählen Sie unter **Schutzbereich** den Modus **Nur die angegebenen freigegebenen Ordner** aus.
8. Klicken Sie auf **Hinzufügen**.
9. 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.
10. Klicken Sie auf **OK**.

11. Legen Sie bei Bedarf Ausnahmen für den Schutzbereich fest:

    a. Klicken Sie im Block **Auszuschließendes Objekt** auf **Hinzufügen**.

    b. Geben Sie im folgenden Fenster 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 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.

12. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So konfigurieren Sie den Schutzbereich (in der Anwendungskonsole)

1. Wählen Sie im Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
2. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.
3. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Verhaltenserkennung** aus.
4. Klicken Sie im Ergebnisbereich des Knotens **Verhaltensanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Verhaltensanalyse** geöffnet.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. Klicken Sie im Block **Schutzbereich** auf **Konfigurieren**.
8. Wählen Sie im folgenden Fenster den Modus **Nur die angegebenen freigegebenen Ordner** aus.
9. Klicken Sie im Block **Schutzbereich** auf **Hinzufügen**.

10. 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.

11. Klicken Sie auf **OK**.

12. Legen Sie bei Bedarf Ausnahmen für den Schutzbereich fest:

    a. Klicken Sie im Block **Ausnahmen** auf **Einstellungen**.

    b. Klicken Sie im folgenden Fenster **Ausnahmen nach Maske** auf die Schaltfläche **Hinzufügen**.

    c. Geben Sie im folgenden Fenster 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 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.

13. 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. Kaspersky Embedded Systems Security überwacht die Datenverschlüsselung von vertrauenswürdigen Computern nicht.

Auf geschützten Geräten mit Windows XP oder Windows Server 2003 überwacht Kaspersky Embedded Systems Security Versuche, freigegebene Ordner zu verschlüsseln, selbst wenn Sie einen Remote-Computer zur Liste der vertrauenswürdigen Computer hinzufügen.

Damit die Funktionalität, mit der bestimmte Adressen aus dem Schutz vor der externen Verschlüsselung von freigegebenen 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 Embedded Systems Security eingeschaltet war. Sie können diesen Remote-Computer nach dem Start von Kaspersky Embedded Systems 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 einen vertrauenswürdigen Computer für die externe Datenverschlüsselung hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.
5. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
6. Klicken Sie im Block **Ausnahmen für IP-Adressen** auf **Konfigurieren**.
7. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
8. Geben Sie die IP-Adresse oder den Namen des Computers ein, dessen Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So fügen Sie einen vertrauenswürdigen Computer für die externe Datenverschlüsselung hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz** → **Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Verhaltensanalyse** wird geöffnet.
5. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
6. Klicken Sie im Block **Ausnahmen** auf **Hinzufügen**.
7. Geben Sie die IP-Adresse oder den Namen des Computers ein, dessen Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.
8. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So fügen Sie einen vertrauenswürdigen Computer für die externe Datenverschlüsselung hinzu (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz** → **Verhaltenserkennung** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Verhaltensanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Verhaltensanalyse** geöffnet.
3. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
4. Klicken Sie im Block **Ausnahmen für IP-Adressen** auf **Konfigurieren**.
5. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.
6. Geben Sie die IP-Adresse oder den Namen des Computers ein, dessen Versuche zur externen Verschlüsselung nicht verarbeitet werden sollen.
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. Standardmäßig blockiert Kaspersky Embedded Systems Security die Sitzung eines Remote-Benutzers für eine Stunde. Nach Ablauf der Sperrdauer entfernt Kaspersky Embedded Systems 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 Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.
4. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.
5. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Verhaltensanalyse**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. Konfigurieren Sie unter **Wenn eine externe Verschlüsselung freigegebener Ordner erkannt wird** die Sperrdauer für einen nicht vertrauenswürdigen Computer, der bösartige Aktivitäten ausführt oder Daten verschlüsselt.
8. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz → Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Verhaltensanalyse** wird geöffnet.
5. Verwenden Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. Konfigurieren Sie unter **Erkennung von externer Verschlüsselung** die Sperrdauer für einen nicht vertrauenswürdigen Computer, der bösartige Aktivitäten ausführt oder Daten verschlüsselt.
8. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Sperrdauer für einen nicht vertrauenswürdigen Computer (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Verhaltenserkennung** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Verhaltensanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Verhaltensanalyse** geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Verhaltensanalyse**.

4. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.

5. Konfigurieren Sie unter **Schutz vor der externen Verschlüsselung freigegebener Ordner** die Sperrdauer für einen nicht vertrauenswürdigen Computer, der bösartige Aktivitäten ausführt oder Daten verschlüsselt.

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 Ausnahmen anzulegen oder die Listen auf einen anderen Server zu migrieren.

So exportieren und importieren Sie eine Liste der Ausnahmen (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Echtzeit-Computerschutz** aus.

4. Klicken Sie im Abschnitt **Verhaltensanalyse** auf **Einstellungen**.

5. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.

6. Klicken Sie im Block **Ausnahmen für IP-Adressen** auf **Konfigurieren**.

7. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie bei Bedarf die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche und wählen Sie den Exportmodus aus: Exportieren Sie die gesamte Ausnahmeliste oder nur ausgewählte Ausnahmen.

   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 Embedded Systems Security exportiert die Ausnahmeliste in die xlm-Datei.

8. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf die Schaltfläche → **Import**.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

b. Öffnen Sie die Datei.

Kaspersky Embedded Systems Security importiert die Ausnahmen.

9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So exportieren und importieren Sie eine Liste der Ausnahmen (in der Web Console)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz** → **Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Verhaltensanalyse** wird geöffnet.
5. Verwenden Sie das Kontrollkästchen **Verhaltensanalyse aktivieren**, um die Komponente zu aktivieren oder zu deaktivieren.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner**.
7. So exportieren Sie die Liste der Ausnahmen im Block **Ausnahmen**:

   a. Wählen Sie bei Bedarf die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche **Export** und wählen Sie den Exportmodus aus: die gesamte Ausnahmeliste oder nur ausgewählte Ausnahmen exportieren.

   c. Speichern Sie die Datei.

   Kaspersky Embedded Systems Security exportiert die Ausnahmeliste in die xlm-Datei.
8. So importieren Sie die Ausnahmeliste im Block **Ausnahmen**:

   a. Klicken Sie auf die Schaltfläche **Import** und wählen Sie einen Importmodus aus: Hinzufügen oder Ersetzen.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   c. Öffnen Sie die Datei.

   Kaspersky Embedded Systems Security importiert die Ausnahmen im ausgewählten Modus.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

Schutz vor Netzwerkbedrohungen

Die Komponente Schutz vor Netzwerkbedrohungen untersucht den eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind. Wird ein versuchter Netzwerkangriff erkannt, der auf den Computer abzielt, blockiert Kaspersky Embedded Systems Security die Netzwerkaktivitäten vom 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.

Die Aufgabe *Schutz vor Netzwerkbedrohungen* wird standardmäßig im Modus **Blockieren** ausgeführt. In diesem Modus blockiert Kaspersky Embedded Systems Security die Verbindung mit Computern, die eine für Netzwerkangriffe typische Aktivität aufweisen, und fügt in einigen Fällen die IP-Adressen dieser Computer zur Liste der blockierten Netzwerksitzungen hinzu.

Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

Kaspersky Embedded Systems Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ geändert werden.

Sie können den Zugriff auf blockierte Hosts wiederherstellen und die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen. Konfigurieren Sie dazu die Einstellungen für blockierte Hosts.

Die IP-Adressen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, werden in den folgenden Fällen aus der Liste der blockierten Hosts gelöscht:

- Kaspersky Embedded Systems Security wird deinstalliert.
- Die IP-Adresse wurde manuell aus der Liste der blockierten Hosts gelöscht.
- Die Blockierdauer des Hosts ist abgelaufen.
- Der Modus **Blockieren** wurde deaktiviert.

Schutz vor Netzwerkbedrohungen aktivieren und konfigurieren

So aktivieren und konfigurieren Sie den Schutz vor Netzwerkbedrohungen (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der Netzwerkaktivität**.
4. Klicken Sie im Block **Schutz vor Netzwerkbedrohungen** auf **Einstellungen**.

5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Schutz vor Netzwerkbedrohungen**.

6. Wählen Sie den Aufgabenmodus im Abschnitt **Operating mode**.

   - **Blockieren**. Wenn dieser Modus ausgewählt ist, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind, blockiert die Verbindung mit Computern, die eine solche Aktivität aufweisen, und fügt in einigen Fällen die IP-Adressen von Computern zur Liste der blockierten Netzwerksitzungen hinzu. Außerdem protokolliert das Programm Ereignisse über erkannte Aktivitäten, die für Netzwerkangriffe typisch sind, im Komponentenprotokoll.

   - **Inform**. Wenn dieser Modus ausgewählt ist, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind, blockiert jedoch nicht die Verbindung zu Computern, die eine solche Aktivität aufweisen, und fügt die IP-Adressen von Computern nicht zur Liste der blockierten Netzwerksitzungen hinzu. Das Programm protokolliert Ereignisse über erkannte Aktivitäten, die für Netzwerkangriffe typisch sind, im Komponentenprotokoll.

7. Mit dem Kontrollkästchen **Port-Scanning und Netzwerk-Flooding als Angriffe betrachten** können Sie die Erkennung der entsprechenden Angriffe aktivieren oder deaktivieren.

8. Aktivieren Sie bei Bedarf das Kontrollkästchen **Block attacking devices for n Min**.

9. Aktivieren oder deaktivieren Sie im Block **MAC spoofing protection** das Kontrollkästchen **Enable protection against MAC spoofing attacks**.

10. Bei Bedarf können Sie Ausnahmen hinzufügen, für die keine Sperrung erfolgen soll.

11. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder konfigurieren Sie den Schutz vor Netzwerkbedrohungen (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie die Option **Kontrolle der Netzwerkaktivität** → **Schutz vor Netzwerkbedrohungen** aus.

5. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**.

6. Wählen Sie den Funktionsmodus der Aufgabe aus:

   - **Blockieren**. Wenn dieser Modus ausgewählt ist, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind, blockiert die Verbindung mit Computern, die eine solche Aktivität aufweisen, und fügt in einigen Fällen die IP-Adressen von Computern zur Liste der blockierten Netzwerksitzungen hinzu. Außerdem protokolliert das Programm Ereignisse über erkannte Aktivitäten, die für Netzwerkangriffe typisch sind, im Komponentenprotokoll.

   - **Informieren**. Wenn dieser Modus ausgewählt ist, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind, blockiert jedoch nicht die Verbindung zu Computern, die eine solche Aktivität aufweisen, und fügt die IP-Adressen von Computern nicht zur Liste der blockierten Netzwerksitzungen hinzu. Das Programm protokolliert Ereignisse über erkannte Aktivitäten, die für Netzwerkangriffe typisch sind, im Komponentenprotokoll.

7. Mit dem Kontrollkästchen **Port-Scanning und Netzwerk-Flooding als Angriffe betrachten** können Sie die Erkennung der entsprechenden Angriffe aktivieren oder deaktivieren.

8. Aktivieren Sie bei Bedarf das Kontrollkästchen **Angreifende Geräte sperren für n Min**.

9. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Schutz vor MAC-Spoofing-Angriffen aktivieren**.

10. Bei Bedarf können Sie Ausnahmen hinzufügen, für die keine Sperrung erfolgen soll.

11. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und konfigurieren Sie den Schutz vor Netzwerkbedrohungen (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Echtzeit-Computerschutz → Schutz vor Netzwerkbedrohungen**.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Eigenschaften: Schutz vor Netzwerkbedrohungen** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Schutz vor Netzwerkbedrohungen**.

4. Wählen Sie den Aufgabenmodus im Abschnitt **Funktionsmodus**.

   - **Verbieten**. Wenn dieser Modus ausgewählt ist, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind, blockiert die Verbindung mit Computern, die eine solche Aktivität aufweisen, und fügt in einigen Fällen die IP-Adressen von Computern zur Liste der blockierten Netzwerksitzungen hinzu. Außerdem protokolliert das Programm Ereignisse über erkannte Aktivitäten, die für Netzwerkangriffe typisch sind, im Komponentenprotokoll.

   - **Informieren**. Wenn dieser Modus ausgewählt ist, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die für Netzwerkangriffe typisch sind, blockiert jedoch nicht die Verbindung zu Computern, die eine solche Aktivität aufweisen, und fügt die IP-Adressen von Computern nicht zur Liste der blockierten Netzwerksitzungen hinzu. Das Programm protokolliert Ereignisse über erkannte Aktivitäten, die für Netzwerkangriffe typisch sind, im Komponentenprotokoll.

5. Mit dem Kontrollkästchen **Port-Scanning und Netzwerk-Flooding als Angriffe betrachten** können Sie die Erkennung der entsprechenden Angriffe aktivieren oder deaktivieren.

6. Aktivieren Sie bei Bedarf das Kontrollkästchen **Angreifende Geräte sperren für n Min**.

7. Aktivieren oder deaktivieren Sie im Block **MAC spoofing protection** das Kontrollkästchen **Schutz vor MAC-Spoofing-Angriffen aktivieren**.

8. Bei Bedarf können Sie Ausnahmen hinzufügen, für die keine Sperrung erfolgen soll.

9. Speichern Sie die vorgenommenen Änderungen.

Eine Ausnahme von der Sperrung erstellen

Kaspersky Embedded Systems 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.

Kaspersky Embedded Systems Security 4.0 bietet die Möglichkeit, Protokolle und Ports für Ausnahmen auszuwählen. Stellen Sie sicher, dass die App und das Verwaltungs-Plug-in auf Version 4.0 oder höher aktualisiert sind. Wenn Sie eine ältere Version der App oder des Verwaltungs-Plug-ins verwenden, kann Kaspersky Embedded Systems Security Netzwerkaktivitäten nur nach IP-Adresse zulassen.

So erstellen Sie eine Ausnahme von der Sperrung (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der Netzwerkaktivität**.
4. Klicken Sie im Block **Schutz vor Netzwerkbedrohungen** auf **Einstellungen**.

   Das Fenster **Schutz vor Netzwerkbedrohungen** wird geöffnet.
5. Gehen Sie auf die Registerkarte **Ausnahmen**.
6. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene Adressen nicht kontrollieren**, um zu verhindern, dass Kaspersky Embedded Systems Security den eingehenden Datenverkehr auf ausgeschlossene IP-Adressen untersucht.
7. Klicken Sie auf **Hinzufügen**.
8. Geben Sie im Fenster **Ausnahme** die IP-Adresse des Geräts ein, dessen Netzwerkangriffe nicht blockiert werden sollen.
9. Wählen Sie bei Bedarf das Protokoll und die Ports aus, über die die Daten übertragen werden.
10. Klicken Sie auf **OK**.
11. Führen Sie die Schritte c bis f für jede hinzugefügte Ausnahme aus.
12. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Ausnahme von der Sperrung (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie **Kontrolle der Netzwerkaktivität → Schutz vor Netzwerkbedrohungen** aus und klicken Sie auf die Schaltfläche **Anpassen**.

5. Gehen Sie auf die Registerkarte **Ausnahmen**.

6. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene IP-Adressen nicht kontrollieren**, um zu verhindern, dass Kaspersky Embedded Systems Security den eingehenden Datenverkehr auf ausgeschlossene IP-Adressen untersucht.

7. Klicken Sie auf **Hinzufügen**.

8. Geben Sie im Fenster **Ausnahme hinzufügen** die IP-Adresse des Geräts ein, dessen Netzwerkangriffe nicht blockiert werden sollen.

9. Wählen Sie bei Bedarf das Protokoll und die Ports aus, über die die Daten übertragen werden.

10. Klicken Sie auf **OK**.

11. Führen Sie die Schritte c bis f für jede hinzugefügte Ausnahme aus.

12. Speichern Sie die vorgenommenen Änderungen.

So erstellen Sie eine Ausnahme von der Sperrung (in der Programmkonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Echtzeit-Computerschutz → Schutz vor Netzwerkbedrohungen**.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Eigenschaften: Schutz vor Netzwerkbedrohungen** wird geöffnet.

3. Gehen Sie auf die Registerkarte **Ausnahmen**.

4. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene Adressen nicht kontrollieren**, um zu verhindern, dass Kaspersky Embedded Systems Security den eingehenden Datenverkehr auf ausgeschlossene IP-Adressen untersucht.

5. Klicken Sie auf **Hinzufügen**.

6. Geben Sie im Fenster **Ausnahme** die IP-Adresse des Geräts ein, dessen Netzwerkangriffe nicht blockiert werden sollen.

7. Wählen Sie bei Bedarf das Protokoll und die Ports aus, über die die Daten übertragen werden.

8. Klicken Sie auf **OK**.

9. Führen Sie die Schritte c bis f für jede hinzugefügte Ausnahme aus.

10. 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 Ausnahmen anzulegen oder die Listen auf einen anderen Server zu migrieren.

So exportieren und importieren Sie eine Liste der Ausnahmen (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der Netzwerkaktivität**.
4. Klicken Sie im Block **Schutz vor Netzwerkbedrohungen** auf **Einstellungen**.

   Das Fenster **Schutz vor Netzwerkbedrohungen** wird geöffnet.
5. Gehen Sie auf die Registerkarte **Ausnahmen**.
6. Um die Regelliste zu exportieren, führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie die Kontrollkästchen der zu exportierenden Ausnahmen. Klicken Sie auf den Pfeil und wählen Sie in der Dropdown-Liste den Punkt **Ausgewählte exportieren** aus.
   - Um die gesamte Ausnahmeliste zu exportieren, klicken Sie auf den Pfeil und wählen Sie in der Dropdown-Liste den Punkt **Exportieren** aus.

     Kaspersky Embedded Systems Security speichert die Datei „networkExclusions.xml“ im standardmäßigen Download-Ordner.
7. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf den Pfeil und wählen Sie **Importieren** aus.

   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 Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XML-Datei ergänzt werden soll.
8. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste der Ausnahmen (in der Web Console)

1. Wählen Sie im „Web Console“-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz → Schutz vor Netzwerkbedrohungen** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Wählen Sie im folgenden Fenster die Registerkarte **Ausnahmen** aus.
6. So exportieren Sie die Liste der vertrauenswürdigen Geräte:

   a. Wählen Sie bei Bedarf die Ausnahmen aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche **Export** und wählen Sie den Exportmodus aus: die gesamte Ausnahmeliste oder nur ausgewählte Ausnahmen exportieren.

   c. Klicken Sie auf **Export**.

   Kaspersky Embedded Systems Security speichert die Datei „networkExclusions.xml“ im standardmäßigen Download-Ordner.
7. So importieren Sie die Ausnahmeliste:

   a. Klicken Sie auf die Schaltfläche **Import** und wählen Sie einen Importmodus aus: **Zu vorhandenen Einträgen hinzufügen** oder **Vorhandene Einträge überschreiben**.

   b. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Ausnahmen importieren möchten.

   c. Öffnen Sie die Datei.

   Kaspersky Embedded Systems Security importiert die Ausnahmen im ausgewählten Modus.
8. Speichern Sie die vorgenommenen Änderungen.

AMSI-Untersuchung

Wenn die Aufgabe AMSI-Scanner ausgeführt wird, kontrolliert Kaspersky Embedded Systems Security die Ausführung von Skripten, die mit den Skript-Technologien von Microsoft Windows (Active Scripting) wie VBScript oder JScript erstellt wurden. Das Programm verarbeitet außerdem PowerShell-Skripte und Skripte, die in Microsoft Office-Programmen unter Betriebssystemen mit installiertem Antimalware Scan Interface (AMSI) ausgeführt werden.

AMSI erlaubt Programmen und Diensten eine Integration mit jeder beliebigen auf einem Gerät installierten Antimalware-Software, damit alle ausgeführten Skripte von der Antimalware abgefangen und untersucht werden. Weitere Informationen über die AMSI-Funktionalität finden Sie auf der Website von Microsoft.

In den Einstellungen der Komponenten können Sie die Ausführung gefährlicher Skripte erlauben oder verbieten. Wenn Kaspersky Embedded Systems Security ein Skript als gefährlich eingestuft hat, wird die Ausführung des Skripts entsprechend der ausgewählten Aktion verboten oder erlaubt. Wenn Sie die Aktion **Blockieren** auswählen, blockiert das Programm gefährliche Skripte und erlaubt andere Skripte.

Kaspersky Embedded Systems Security unterstützt die AMSI-Technologie in Microsoft Windows 10 und Microsoft Windows Server 2016 und höher.

AMSI-Scanner aktivieren und deaktivieren

So aktivieren oder deaktivieren Sie den AMSI-Scanner (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Echtzeit-Computerschutz**.
4. Klicken Sie im Block **AMSI-Scanner** auf **Einstellungen**.

   Das Fenster **AMSI-Scanner** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen **AMSI-Scanner**, wenn Sie den AMSI-Scanner aktivieren möchten.
   - Deaktivieren Sie das Kontrollkästchen **AMSI-Scanner**, wenn Sie den AMSI-Scanner deaktivieren möchten.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie den AMSI-Scanner (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Echtzeit-Computerschutz → AMSI-Scanner** aus.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **AMSI-Scanner** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

3. Führen Sie einen der folgenden Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **AMSI-Scanner**, wenn Sie den AMSI-Scanner aktivieren möchten.
   - Deaktivieren Sie das Kontrollkästchen **AMSI-Scanner**, wenn Sie den AMSI-Scanner deaktivieren möchten.

4. Klicken Sie im Fenster **AMSI-Scanner** auf die Schaltfläche **OK**.

So aktivieren Sie den AMSI-Scanner (in der Konsole für 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 Embedded Systems Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeit-Computerschutz** aus.
5. Klicken Sie im Block **AMSI-Scanner** auf **Anpassen**.
   Das Fenster **AMSI-Scanner** wird geöffnet.
6. Führen Sie einen der folgenden Schritte aus:

   - Aktivieren Sie das Kontrollkästchen **AMSI-Scanner**, wenn Sie den AMSI-Scanner aktivieren möchten.
   - Deaktivieren Sie das Kontrollkästchen **AMSI-Scanner**, wenn Sie den AMSI-Scanner deaktivieren möchten.

7. Speichern Sie die vorgenommenen Änderungen.

Einstellungen für den AMSI-Scanner

So konfigurieren Sie die Einstellungen des AMSI-Scanners (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Echtzeit-Computerschutz**.
4. Klicken Sie im Block **AMSI-Scanner** auf **Einstellungen**.
   Das Fenster **AMSI-Scanner** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Wählen Sie die Aktion aus, die Kaspersky Embedded Systems Security ausführen soll, wenn ein gefährliches Skript ausgeführt wird:

   - **Informieren**. Das Programm erlaubt die Ausführung von möglicherweise gefährlichen Skripten. Im Aufgabenprotokoll wird ein entsprechendes Ereignis protokolliert.
   - **Blockieren**. Das Programm blockiert möglicherweise gefährliche Skripte.

6. Geben Sie im Block **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Office-Format-Dateien.

7. Führen Sie im Block **Größenbeschränkung** eine der folgenden Aktionen aus:

   - Wenn die Komponente „AMSI-Scanner“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße (MB)** einen entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Scanner“ nicht entpackt.

   - Wenn die Komponente „AMSI-Scanner“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

   Die Komponente „AMSI-Scanner“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

8. Klicken Sie im Fenster **AMSI-Scanner** auf die Schaltfläche **OK**.

9. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

So konfigurieren Sie die Einstellungen des AMSI-Scanners (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Echtzeit-Computerschutz → AMSI-Scanner** aus.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **AMSI-Scanner** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

3. Wählen Sie die Aktion aus, die Kaspersky Embedded Systems Security ausführen soll, wenn ein gefährliches Skript ausgeführt wird:

   - **Informieren**. Das Programm erlaubt die Ausführung von möglicherweise gefährlichen Skripten. Im Aufgabenprotokoll wird ein entsprechendes Ereignis protokolliert.

   - **Blockieren**. Das Programm blockiert möglicherweise gefährliche Skripte.

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-Scanner“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße (MB)** einen entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Scanner“ nicht entpackt.

   - Wenn die Komponente „AMSI-Scanner“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

Die Komponente „AMSI-Scanner“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

6. Klicken Sie im Fenster **AMSI-Scanner** auf die Schaltfläche **OK**.

So konfigurieren Sie die Einstellungen des AMSI-Scanners (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeit-Computerschutz** aus.
5. Klicken Sie im Block **AMSI-Scanner** auf **Anpassen**.

   Das Fenster **AMSI-Scanner** wird geöffnet.
6. Wählen Sie die Aktion aus, die Kaspersky Embedded Systems Security ausführen soll, wenn ein gefährliches Skript ausgeführt wird:

   - **Informieren**. Das Programm erlaubt die Ausführung von möglicherweise gefährlichen Skripten. Im Aufgabenprotokoll wird ein entsprechendes Ereignis protokolliert.
   - **Blockieren**. Das Programm blockiert möglicherweise gefährliche Skripte.
7. Geben Sie im Block **Untersuchung von zusammengesetzten Dateien** an, welche zusammengesetzten Dateien untersucht werden sollen: Archive, Programmpakete oder Office-Format-Dateien.
8. Führen Sie im Block **Größenbeschränkung** eine der folgenden Aktionen aus:

   - Wenn die Komponente „AMSI-Scanner“ große zusammengesetzte Dateien nicht entpacken soll, aktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und geben Sie im Feld **Maximale Dateigröße (MB)** einen entsprechenden Wert an. Zusammengesetzte Dateien, welche die angegebene Größe überschreiten, werden von der Komponente „AMSI-Scanner“ nicht entpackt.
   - Wenn die Komponente „AMSI-Scanner“ große zusammengesetzte Dateien entpacken soll, deaktivieren Sie das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken**.

   Die Komponente „AMSI-Scanner“ untersucht große Dateien, die aus Archiven extrahiert werden, unabhängig davon, ob das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.
9. Klicken Sie im Fenster **AMSI-Scanner** auf **OK**.
10. Klicken Sie im Fenster **<Name der Richtlinie>** auf **Speichern**.

Kontrolle des Programmstarts

Die Komponente Kontrolle des Programmstarts von Kaspersky Embedded Systems Security schützt Geräte vor dem unbefugten Start von Programmen. Die Kontrolle des Programmstarts basiert auf dem Prinzip „Alles standardmäßig verbieten“. Dies bedeutet: Alle Programme, die in den Komponenteneinstellungen nicht erlaubt sind, werden automatisch blockiert. Sie können den Start von Programmen zulassen, indem Sie Erlaubnisregeln der Komponente für diese Programme erstellen.

Wenn die Regeln für die Kontrolle des Programmstarts so vollständig wie möglich erstellt wurden, blockiert Kaspersky Embedded Systems Security den Start aller neuen Programme, die nicht vom Administrator des lokalen Unternehmensnetzwerks überprüft wurden, gewährleistet jedoch die Funktionsfähigkeit des Betriebssystems und der überprüften Programme, die Benutzer zur Erfüllung ihrer Aufgaben benötigen. Sie können mithilfe der Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* Informationen zu den auf geschützten Geräten installierten Programmen abrufen.

Wenn die Komponente Kontrolle des Programmstarts aktiviert ist, fängt Kaspersky Embedded Systems Security jedes Betriebssystemereignis ab, das mit einer Anforderung zum Erstellen eines Prozesses zusammenhängt und beim Start einer ausführbaren Datei auf einem geschützten Gerät auftritt. Anschließend erfasst das Programm Informationen über die ausführbare Datei, das Skript oder das MSI-Paket, die bzw. das gestartet wird, und vergleicht sie mit den Bedingungen für das Auslösen der Regeln für die Kontrolle des Programmstarts. Wenn alle Bedingungen mindestens einer Erlaubnisregel erfüllt sind, lässt Kaspersky Embedded Systems Security den Start des Programms zu. Wenn das zu startende Programm die Bedingungen keiner Erlaubnisregel erfüllt oder eine Blockierungsregel ausgelöst wird, blockiert Kaspersky Embedded Systems Security den Versuch, das Programm zu starten, indem die Erstellung des Prozesses abgebrochen wird.

Alle Versuche zum Starten von Programmen werden im Komponentenprotokoll aufgezeichnet.

Die Komponente Kontrolle des Programmstarts bietet zwei Modi zur Auswahl:

- **Verbieten**. Kaspersky Embedded Systems Security kontrolliert den Start von Programmen anhand der Regeln zur Kontrolle des Programmstarts. Der Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts wird in den allgemeinen Einstellungen der Komponente Kontrolle des Programmstarts angegeben. Wenn ein Programm die Regeln für die Kontrolle des Programmstarts erfüllt, aber keine der Regeln dem Gültigkeitsbereich der Regeln für die Kontrolle des Programmstarts entspricht, wird die Ausführung des Programms verhindert.

  Die Ausführung von Programmen, die nicht unter die Regeln für die Kontrolle des Programmstarts fallen, wird verboten.

  > Die Komponente Kontrolle des Programmstarts kann nicht im aktiven Modus gestartet werden, wenn keine Regeln für die Kontrolle des Programmstarts erstellt wurden oder wenn es mehr als 65.535 Regeln zur Kontrolle des Programmstarts für ein geschütztes Gerät gibt.

- **Informieren**. Kaspersky Embedded Systems Security erlaubt den Start aller Programme. Es werden nur Informationen aufgezeichnet. Dazu gehören Informationen über alle Programmstarts, über Regeln für die gestarteten Programme und über Aktionen, die im Modus **Verbieten** von der Aufgabe ausgeführt würden. Dieser Modus ist standardmäßig eingestellt.

Wenn Sie Regeln zur Kontrolle des Programmstarts erstellen, müssen Sie sicherstellen, dass diese die Ausführung von Programmen des Betriebssystems nicht blockieren.

Kaspersky Embedded Systems Security fängt außerdem Prozesse ab, die unter dem Windows Subsystem for Linux gestartet werden (außer Skripten, die von der UNIX™-Shell oder aus dem Kommandozeileninterpreter gestartet werden). Für solche Prozesse wendet die Komponente Kontrolle des Programmstarts die durch die aktuelle Konfiguration festgelegten Aktionen an. Die Aufgabe zum *Erstellen von Regeln für die Kontrolle des Programmstarts* erkennt den Start von Programmen und erstellt entsprechende Regeln für Programme, die unter Windows Subsystem for Linux laufen.

Über die Regeln für die Kontrolle des Programmstarts

So funktionieren Regeln für die Kontrolle des Programmstarts

Die Funktion der Regeln für die Kontrolle des Programmstarts basiert auf folgenden Elementen:

- Regeltyp.

  Regeln der Kontrolle des Programmstarts können den Start von Programmen erlauben oder verbieten. Demgemäß werden sie als *Erlaubnisregeln* oder *Verbotsregeln* bezeichnet.

- Gültigkeitsbereich der Regel.

  Regeln für die Kontrolle des Programmstarts können auf *ausführbare Dateien*, *Skripts* und *MSI-Pakete* angewendet werden.

- Auslösebedingungen für eine Regel.

  Regeln zur Kontrolle des Programmstarts regeln den Start von Dateien, die mindestens eine in den Regeleinstellungen angegebene Auslösebedingung erfüllen. Beispiele: Ausführbare Dateien sind mit dem angegebenen *digitalen Zertifikat* signiert, haben den angegebenen *SHA256-Hash*, befinden sich am angegebenen *Pfad* oder entsprechen den angegebenen Argumenten für die *Befehlszeile*. Sie müssen mindestens eine Auslösebedingung für die Regel hinzufügen. Andernfalls wird die Regel für die "Kontrolle des Programmstarts" nicht hinzugefügt.

- Ausnahmen für die Regel.

  Sie können Ausnahmen für die Regel zur Kontrolle des Programmstarts konfigurieren, die auf den gleichen Kriterien basieren können wie die Auslösebedingungen der Regel. Ausnahmen von den Regeln für die Kontrolle des Programmstarts können für bestimmten Erlaubnisregeln erforderlich werden: z. B., wenn Sie Benutzern den Start von Programmen aus dem Pfad C:\Windows erlauben möchten, den Start der Datei Regedit.exe jedoch verbieten wollen.

- Benutzer oder Benutzergruppe

  Mit Regeln zur Kontrolle des Programmstarts können Sie den Start von bestimmten Programmen durch einen Benutzer und/oder eine Benutzergruppe kontrollieren.

Wenn Sie Regeln zur Kontrolle des Programmstarts erstellen, müssen Sie sicherstellen, dass die neuen Regeln die Ausführung von Programmen des Betriebssystems nicht blockieren.

Verwaltung der Regeln für die Kontrolle des Programmstarts

Für die Regel für die Kontrolle des Programmstarts stehen Ihnen die folgenden Aktionen zur Verfügung:

- Manuell hinzufügen.
- Regeln automatisch erstellen und hinzufügen
- Löschen.
- Importieren und exportieren.
- Liste der Regeln filtern.

Über die Kontrolle der Software-Verteilung

Die Generierung der Kontrolle des Programmstarts kann komplizierter werden, wenn Sie die Verteilung von Programmen kontrollieren möchten. Dies ist beispielsweise auf geschützten Geräten möglich, auf denen die installierte Software regelmäßig automatisch aktualisiert wird. In diesem Fall muss die Liste der Erlaubnisregeln nach jedem Software-Update aktualisiert werden, damit neu erstellte Dateien in den Einstellungen der Komponente Kontrolle des Programmstarts berücksichtigt werden. Um die Startkontrolle bei Software-Verteilungsszenarien zu vereinfachen, können Sie die Kontrolle der Software-Verteilung verwenden.

Ein *Installationspaket* (im Folgenden „Paket“ genannt) enthält ein oder mehrere Programme, die auf einem geschützten Gerät installiert werden sollen. Ein Installationspaket kann auch Updates und einzelne Befehle enthalten.

Das Subsystem „Kontrolle der Software-Verteilung“ wird als zusätzliche Liste von Ausnahmen implementiert. Wenn ein Installationspaket zur Liste hinzugefügt wird, wird es vertrauenswürdig. Das Entpacken ist für vertrauenswürdige Pakete erlaubt, und der automatische Start ist für Programme erlaubt, die aus vertrauenswürdigen Paketen installiert oder aktualisiert wurden. Die extrahierten Dateien können das Merkmal für die Vertrauenswürdigkeit von einem Hauptprogrammpaket erben. Ein *Hauptprogrammpaket* ist ein Paket, das vom Benutzer zur Liste der Ausnahmen von der Kontrolle der Software-Verteilung hinzugefügt wurde und nun als vertrauenswürdiges Paket gilt.

Kaspersky Embedded Systems Security kontrolliert nur den vollständigen Zyklus einer Software-Verteilung und kann den Start von Dateien, die von einem vertrauenswürdigen Paket modifiziert wurden, nicht korrekt verarbeiten, falls beim ersten Start des Pakets die Kontrolle der Software-Verteilung deaktiviert war oder die Komponente Kontrolle des Programmstarts nicht installiert war.

Um die Kontrolle der Installationspakete zu verwenden, müssen Sie die Funktionalität **Regeln auf ausführbare Dateien anwenden** in den allgemeinen Einstellungen der Komponente Kontrolle des Programmstarts aktivieren.

Software-Verteilungscache

Kaspersky Embedded Systems Security verwendet einen dynamisch erzeugten Software-Verteilungscache (im Folgenden „Verteilungscache“ genannt), um die Beziehung zwischen vertrauenswürdigen Paketen und Dateien herzustellen, die während der Softwareverteilung erstellt wurden. Wenn ein Paket erstmals gestartet wird, erkennt Kaspersky Embedded Systems Security alle Dateien, die von dem Paket während des Softwareverteilungsprozesses erstellt werden, und speichert die Prüfsummen und Pfade der Dateien im Verteilungscache. Anschließend können standardmäßig alle Dateien gestartet werden, über die Informationen im Verteilungscache gespeichert sind.

Sie können den Verteilungscache nicht über die Benutzeroberfläche überprüfen, löschen oder manuell ändern. Der Cache wird von Kaspersky Embedded Systems Security mit Daten gefüllt und kontrolliert.

Sie können den Verteilungscache in eine Konfigurationsdatei (XML-Format) exportieren oder den Verteilungscache über die Befehlszeile löschen.

Kaspersky Embedded Systems Security aktualisiert den Verteilungscache alle 24 Stunden. Wenn die Prüfsumme einer zuvor erlaubten Datei geändert wird, löscht das Programm den Datensatz für diese Datei aus dem Verteilungscache. Wenn die Komponente Kontrolle des Programmstarts im Aktiv-Modus ausgeführt wird, werden weitere Startversuche für diese Datei blockiert. Wenn der vollständige Pfad einer zuvor erlaubten Datei geändert wird, werden weitere Ausführungsversuche dieser Datei unterbunden, da die Prüfsumme im Verteilungscache gespeichert ist.

Verarbeiten der extrahierten Dateien

Extrahierte Dateien und Pakete, die von einem primären vertrauenswürdigen Verteilungspaket (auf der ersten Verschachtelungsebene) erstellt wurden, erben das Attribut „vertrauenswürdig“, falls ihre Prüfsummen dem Verteilungscache hinzugefügt werden, wenn das Software-Verteilungspaket in der Ausnahmeliste zum ersten Mal geöffnet wird. Als Folge gelten sowohl das Installationspaket selbst als auch alle extrahierten Dateien des Pakets als vertrauenswürdig.

Wenn beispielsweise test.msi (ein Paket, das mehrere Pakete und Programme enthält) zur Ausnahmeliste hinzugefügt wird und die Funktionalität **Start für alle untergeordneten Dateien als vertrauenswürdige Verteilungspakete erlauben** aktiviert ist, können alle im Paket test.msi enthaltenen Pakete und Programme entpackt und gestartet werden, auch wenn sie andere verschachtelte Dateien enthalten. Dieses Szenario gilt für extrahierte Dateien auf allen Verschachtelungsebenen.

Wenn das Paket test.msi zur Ausnahmeliste hinzugefügt wird und die Funktionalität **Start für alle untergeordneten Dateien als vertrauenswürdige Verteilungspakete erlauben** aktiviert ist, weist das Programm das Attribut „vertrauenswürdig“ nur jenen Paketen und ausführbaren Dateien zu, die direkt aus dem vertrauenswürdigen Paket extrahiert wurden (auf der ersten Verschachtelungsebene). Die Prüfsummen dieser Dateien werden im Verteilungscache gespeichert. Alle Dateien, die sich auf der zweiten Verschachtelungsebene und tiefer befinden, werden nach dem Prinzip des standardmäßigen Verbots (Default Deny) blockiert.

Extrahierte Dateien behalten das Merkmal für die Vertrauenswürdigkeit nachdem das Betriebssystem neu gestartet wurde.

Um das Vererbungsattribut aus allen extrahierten Dateien zu entfernen, müssen Sie den Verteilungscache löschen und die Funktionalität **Start für alle untergeordneten Dateien als vertrauenswürdige Verteilungspakete erlauben** deaktivieren, bevor Sie das vertrauenswürdige Installationspaket erneut ausführen.

Arbeiten mit der Regelliste für die Kontrolle des Programmstarts

Die Liste für vertrauenswürdige Pakete der Kontrolle der Software-Verteilung ist eine Liste mit Ausnahmen. Diese Liste erweitert die allgemeine Liste der Regeln für die Kontrolle des Programmstarts, ersetzt sie jedoch nicht.

Verbotsregeln der Kontrolle des Programmstarts haben die höchste Priorität: Das Dekomprimieren vertrauenswürdiger Pakete und das Ausführen neuer oder modifizierter Dateien wird blockiert, wenn diese Pakete und Dateien von den Verbotsregeln zur Kontrolle des Programmstarts betroffen sind.

Ausnahmen für die Kontrolle der Software-Verteilung werden sowohl auf vertrauenswürdige Pakete als auch auf Dateien angewendet, die von diesen Paketen erstellt oder modifiziert wurden, wenn keine Verbotsregeln in der Liste der Kontrolle des Programmstarts auf diese Pakete und Dateien angewendet werden.

Über den Regelgenerator für die Anwendungsstartkontrolle

Sie können mithilfe der Aufgaben und Richtlinien von Kaspersky Security Center für alle Geräte und Gruppen von geschützten Geräten im Netzwerk des Unternehmens gleichzeitig Listen mit Regeln für die Kontrolle des Programmstarts erstellen. Die unten angeführten Szenarien werden empfohlen, wenn sich im Unternehmensnetzwerk keine Referenzcomputer befinden und Sie keine Möglichkeit haben, eine Liste von Erlaubnisregeln anhand der auf einem solchen Vorlagencomputer installierten Programme zu erstellen.

> Sie können die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* lokal über die Programmkonsole ausführen, um eine Liste von Regeln zu erstellen, die auf den Anwendungen basieren, die auf einem einzelnen geschützten Gerät ausgeführt werden.

Sie können Listen mit Regeln für die Kontrolle des Programmstarts in der Konsole von Kaspersky Security Center auf eine der folgenden Arten erstellen:

- Mithilfe der Gruppenaufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts*.

  Abhängig von den Einstellungen kann die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* Informationen über Programme erfassen, die auf geschützten Geräten ausgeführt werden, sowie über ausführbare Dateien und Skripte, die sich in den angegebenen Bereichen befinden. Auf Grundlage der erfassten Informationen erstellt die Aufgabe eine Liste mit Erlaubnisregeln für die Komponente Kontrolle des Programmstarts.

  Sie können den automatischen Import der erstellten Regeln in die Liste der Regeln für die Komponente Kontrolle des Programmstarts konfigurieren oder die erstellten Regeln manuell importieren.

  Es wird empfohlen, diese Option zu verwenden, wenn die rasche Erstellung von Listen mit Regeln für die Kontrolle des Programmstarts erforderlich ist. Wir empfehlen, den geplanten Start der Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* nur dann zu konfigurieren, wenn der zulässige Regelverwendungsbereich Ordner und Dateien umfasst, von denen Sie wissen, dass sie sicher sind.

- Auf Basis des Ereignisberichts, der in Kaspersky Security Center für die Komponente Kontrolle des Programmstarts, die im *Informieren*-Modus läuft, generiert wird.

In diesem Szenario verbietet Kaspersky Embedded Systems Security den Start von Programmen nicht. Wenn die Komponente Kontrolle des Programmstarts im *Informieren*-Modus ausgeführt wird, werden stattdessen alle erlaubten und verweigerten Programmstarts für alle geschützten Geräte im Netzwerk auf der Registerkarte **Ereignisse** im Arbeitsbereich des Knotens für den Kaspersky Security Center-Administrationsserver gemeldet. Kaspersky Security Center verwendet die Berichte, um eine einzelne Liste von Ereignissen zu erstellen, bei denen Programmstarts verboten wurden.

Während die Komponente ausgeführt wird, müssen alle möglichen Szenarien für geschützte Geräte und geschützte Gerätegruppen ausgeführt werden. Dazu zählt auch mindestens ein Neustart eines geschützten Geräts. Sie können Daten über Programmstarts aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (im txt-Format) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle des Programmstarts für solche Programme erstellen.

Dieses Szenario wird empfohlen, wenn das Netzwerk des Unternehmens eine große Anzahl an geschützten Geräten verschiedener Typen (mit unterschiedlicher Software) enthält.

- Auf Grundlage der Ereignisse über den verbotenen Start von Programmen, die über Kaspersky Security Center erhalten wurden, ohne Erstellen und Importieren der Konfigurationsdatei.

  Um die vorliegende Möglichkeit zu nutzen, muss sich die Komponente Kontrolle des Programmstarts auf dem geschützten Gerät unter der Verwaltung der aktiven Richtlinie für Kaspersky Security Center befinden. Alle Ereignisse auf dem geschützten Gerät werden dabei an den Administrationsserver übergeben.

Es wird empfohlen, die Regelliste bei Änderungen an der Zusammensetzung der auf den geschützten Geräten des Netzwerks installierten Programme zu aktualisieren (beispielsweise bei der Installation von Updates oder nach einer Neuinstallation des Betriebssystems). Es wird empfohlen, eine aktualisierte Liste mit Regeln zu erstellen. Führen Sie dazu auf den geschützten Geräten in der Test-Administrationsgruppe die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* oder die Komponente Kontrolle des Programmstarts im *Informieren*-Modus aus. Die Test-Administrationsgruppe beinhaltet die geschützten Geräte, die für den Test des Starts von neuen Programmen vor deren Installation auf den geschützten Geräten des Netzwerks erforderlich sind.

xml-Dateien, die Listen von Erlaubnisregeln enthalten, werden auf Grundlage einer Analyse der auf dem geschützten Gerät gestarteten Programme erstellt. Es ist wichtig, dass alle im Netzwerk verwendeten Programme berücksichtigt werden. Darum wird empfohlen, beim Erstellen von Regellisten die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* und die Komponente Kontrolle des Programmstarts im *Informieren*-Modus auf einem Referenzcomputer zu starten.

Überzeugen Sie sich vor dem Erstellen der Liste der Erlaubnisregeln nach Programmen, die auf dem Referenzcomputer des Unternehmens gestartet werden, dass der Vorlagencomputer sicher ist und es darauf keine Schadsoftware gibt.

Bevor Sie Erlaubnisregeln hinzufügen, wählen Sie einen der verfügbaren Modi zur Anwendung der Regeln aus. In der Regelliste der Richtlinie für Kaspersky Security Center werden nur Regeln angezeigt, die in dieser Richtlinie festgelegt sind, unabhängig vom Modus der Regelanwendung. Die Regelliste des lokalen Computers enthält alle angewendeten Regeln – sowohl lokale als auch durch eine Richtlinie hinzugefügte.

Kontrolle des Programmstarts aktivieren und konfigurieren

So aktivieren und konfigurieren Sie die allgemeinen Einstellungen für die Kontrolle des Programmstarts (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.
4. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Einstellungen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Aktivieren Sie das Kontrollkästchen **Kontrolle des Programmstarts**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Betriebsmodus der Komponente:

   - **Verbieten**. Kaspersky Embedded Systems Security verwendet alle erstellten Regeln zur Kontrolle des Programmstarts.
   - **Informieren**. Kaspersky Embedded Systems Security verwendet keine Regeln für die Kontrolle des Programmstarts. Es zeichnet nur Informationen über den Start von Programmen im Komponentenprotokoll auf. Allen Programmen wird der Start erlaubt. Sie können diesen Modus für die Erstellung einer Liste der Regeln für die Kontrolle des Programmstarts auf Grundlage der im Protokoll der Komponente enthaltenen Informationen über verbotene Programmstarts verwenden.
7. Konfigurieren Sie die Komponenteneinstellungen (s. folgende Tabelle).
8. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security wendet die neuen Komponenteneinstellungen sofort an. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

So aktivieren und konfigurieren Sie die allgemeinen Einstellungen für die Kontrolle des Programmstarts in der Konsole für Kaspersky Embedded Systems Security

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Kontrolle des Programmstarts** aus.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
3. Aktivieren Sie das Kontrollkästchen **Kontrolle des Programmstarts**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Betriebsmodus der Komponente:

   - **Verbieten**. Kaspersky Embedded Systems Security verwendet alle erstellten Regeln zur Kontrolle des Programmstarts.

   - **Informieren**. Kaspersky Embedded Systems Security verwendet keine Regeln für die Kontrolle des Programmstarts. Es zeichnet nur Informationen über den Start von Programmen im Komponentenprotokoll auf. Allen Programmen wird der Start erlaubt. Sie können diesen Modus für die Erstellung einer Liste der Regeln für die Kontrolle des Programmstarts auf Grundlage der im Protokoll der Komponente enthaltenen Informationen über verbotene Programmstarts verwenden.

5. Konfigurieren Sie die Komponenteneinstellungen (s. folgende Tabelle).

6. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security wendet die neuen Komponenteneinstellungen sofort an. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

So aktivieren und konfigurieren Sie die allgemeinen Einstellungen für die Kontrolle des Programmstarts (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.

5. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Anpassen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

6. Aktivieren Sie das Kontrollkästchen **Kontrolle des Programmstarts aktivieren**.

7. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Betriebsmodus der Komponente:

   - **Blockieren**. Kaspersky Embedded Systems Security verwendet alle erstellten Regeln zur Kontrolle des Programmstarts.

   - **Informieren**. Kaspersky Embedded Systems Security verwendet keine Regeln für die Kontrolle des Programmstarts. Es zeichnet nur Informationen über den Start von Programmen im Komponentenprotokoll auf. Allen Programmen wird der Start erlaubt. Sie können diesen Modus für die Erstellung einer Liste der Regeln für die Kontrolle des Programmstarts auf Grundlage der im Protokoll der Komponente enthaltenen Informationen über verbotene Programmstarts verwenden.

8. Konfigurieren Sie die Komponenteneinstellungen (s. folgende Tabelle).

9. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security wendet die neuen Komponenteneinstellungen sofort an. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Allgemeine Einstellungen für die Kontrolle des Programmstarts

Einstellung	Beschreibung
Aktion, die für den ersten Dateistart ausgeführt wurde, bei allen weiteren Starts dieser Datei wiederholen	Diese Option aktiviert oder deaktiviert die Kontrolle künftiger Programmstarts auf Basis von zwischengespeicherten Einträgen für Ereignisinformationen. Wenn die Option aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security künftige Starts eines Programms und berücksichtigt dabei, wie die Komponente beim ersten Programmstart eingestuft wurde. Wenn beispielsweise der erste Programmstart durch die Regeln für die Kontrolle des Programmstarts erlaubt wurde, so verbleibt der Eintrag über diese Entscheidung im Cache und der zweite und alle nachfolgenden Starts dieses Programms werden ohne erneute Überprüfung ebenfalls erlaubt. Wenn das Programm auf einem Computer mit Windows XP installiert ist und über den Explorer mit Dateien gearbeitet wird, werden die Analyseergebnisse des ersten Programmstarts möglicherweise überschrieben, wodurch die Funktion beeinträchtigt wird. Ist die Option deaktiviert, so analysiert Kaspersky Embedded Systems Security ein Programm bei jedem versuchten Programmstart von neuem.
Start des Befehlsinterpreters ohne ausführbaren Befehl verweigern	Wenn diese Funktion aktiviert ist, verweigert Kaspersky Embedded Systems Security den Start des Befehlszeileninterpreters, wenn eine der folgenden Bedingungen erfüllt ist: • Der Start eines Befehlszeileninterpreters wird durch Regeln für die Kontrolle des Programmstarts verweigert. • Der Befehlszeileninterpreter wird ohne Parameter gestartet. Ist die Option deaktiviert, so berücksichtigt Kaspersky Embedded Systems Security beim Start eines Kommandozeileninterpreters nur Erlaubnisregeln. Der Start wird blockiert, wenn keine der Erlaubnisregeln für die Kontrolle des Programmstarts zutrifft. Wenn die Erlaubnisregel der Kontrolle des Programmstarts zutrifft, kann ein Befehlszeileninterpreter mit oder ohne auszuführenden Befehl gestartet werden. Kaspersky Embedded Systems Security kontrolliert den Start der folgenden Befehlsinterpreter: • cmd.exe • powershell.exe • python.exe • perl.exe • wscript.exe Die Funktionalität ist standardmäßig deaktiviert.
Regeln auf ausführbare Dateien anwenden	Die Option aktiviert oder deaktiviert die Startkontrolle für ausführbare Dateien. Ist diese Funktionalität aktiviert, erlaubt oder verweigert Kaspersky Embedded Systems Security den Start ausführbarer Dateien anhand von Regeln zur Kontrolle des Programmstarts. Ist diese Funktionalität deaktiviert, kontrolliert Kaspersky Embedded Systems Security den Start ausführbarer Dateien nicht anhand von Regeln zur Kontrolle des Programmstarts. Der Start ausführbarer Dateien ist erlaubt. Diese Option ist standardmäßig aktiviert.
Laden von DLL-Modulen überwachen	Das Überwachen des Ladens von DLL-Modulen kann sich auf die Leistung des Betriebssystems auswirken. Diese Funktionalität ist verfügbar, wenn die Funktionalität **Regeln auf ausführbare Dateien anwenden** aktiviert ist. Diese Funktionalität aktiviert oder deaktiviert die Kontrolle für das Laden von DLL-Modulen. Ist diese Funktionalität aktiviert, erlaubt oder verweigert Kaspersky Embedded Systems Security das Laden von DLL-Modulen anhand von Regeln zur Kontrolle des Programmstarts. Ist diese Funktionalität deaktiviert, kontrolliert Kaspersky Embedded Systems Security das Laden von DLL-Modulen nicht anhand von Regeln zur Kontrolle des Programmstarts. Laden von DLL-Modulen ist erlaubt. Die Funktionalität ist standardmäßig deaktiviert.
Regeln auf Skripte und MSI-Pakete anwenden	Diese Option aktiviert oder deaktiviert die Kontrolle des Starts von Skripten und MSI-Paketen. Ist diese Funktionalität aktiviert, erlaubt oder verweigert Kaspersky Embedded Systems Security den Start von Skripten und MSI-Paketen anhand von Regeln zur Kontrolle des Programmstarts. Ist diese Funktionalität deaktiviert, erlaubt oder verweigert Kaspersky Embedded Systems Security den Start von Skripten und MSI-Paketen nicht anhand von Regeln zur Kontrolle des Programmstarts. Das Ausführen von Skripten und MSI-Paketen ist gestattet. Diese Option ist standardmäßig aktiviert.

Einstellung	Beschreibung
Beim Überprüfen von Zertifikaten fehlenden Signaturzeitstempel ignorieren	Ist diese Funktionalität aktiviert, erlaubt Kaspersky Embedded Systems Security den Start von Programmen, die mit Zertifikaten signiert sind, die abgelaufen sind oder ein unbestimmtes Ablaufdatum haben. Ist diese Funktionalität deaktiviert, verweigert Kaspersky Embedded Systems Security den Start von Programmen, die mit Zertifikaten signiert sind, die abgelaufen sind oder ein unbestimmtes Ablaufdatum haben. Die Funktionalität ist standardmäßig deaktiviert.

Konfiguration der Kontrolle für Installationspakete

So konfigurieren Sie die Kontrolle der Software-Verteilung (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.
4. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Einstellungen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Wählen Sie die Registerkarte **Kontrolle der Software-Verteilung** aus.
6. Aktivieren Sie die Funktion **Software-Verteilung über aufgelistete Programme und Pakete automatisch erlauben**. Diese Funktionalität erstellt automatisch Ausnahmen für alle Dateien, die mithilfe ausführbarer Dateien und mithilfe von Installationspaketen gestartet werden, die in der Liste angegeben sind.

   Sie können die Funktionalität **Software-Verteilung über aufgelistete Programme und Pakete automatisch erlauben** aktivieren, wenn auf der Registerkarte **Allgemein** die Funktionalität **Regeln auf ausführbare Dateien anwenden** aktiviert ist.
7. Deaktivieren Sie bei Bedarf die Funktionalität **Software-Verteilung über Windows-Installationsprogramm immer erlauben**. Diese Funktionalität erstellt automatisch Ausnahmen für alle Dateien, die mithilfe des Windows-Installationsprogramms gestartet werden.

   Abschalten dieser Funktion kann zu Problemen beim Update der Dateien des Betriebssystems führen und ferner den Start von Dateien verhindern, die aus einem Installationspaket extrahiert werden.
8. Aktivieren Sie bei Bedarf die Funktionalität **Software-Verteilung über SCCM unter Verwendung des intelligenten Hintergrundübertragungsdienstes immer erlauben**. Diese Funktion ermöglicht die Verteilung von Software mithilfe der Lösung System Center Configuration Manager.

   Wenn diese Funktion aktiviert ist, ermöglicht Kaspersky Embedded Systems Security die Bereitstellung von Microsoft Windows mithilfe von System Center Configuration Manager. Die Anwendung ermöglicht die Softwareverteilung nur über Background Intelligent Transfer Service. Das Programm kontrolliert den Start von ausführbaren Dateien mit den Erweiterungen .EXE und .MSI.

Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an das geschützte Gerät bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät ausgeführt wurde.

9. Fügen Sie ausführbare Dateien und Installationspakete hinzu, deren Start erlaubt werden soll:

- **Manuell hinzufügen**

  a. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Ein Programmpaket hinzufügen** aus.

  b. Klicken Sie im angezeigten Fenster auf **Durchsuchen**.

  c. Wählen Sie die ausführbare Datei oder das Installationspaket aus.

  Die Felder unter **Vertrauenskriterien** werden automatisch mit Informationen über die ausgewählte Datei ausgefüllt.

  d. Aktivieren Sie bei Bedarf die Funktionalität **Start für alle untergeordneten Dateien als vertrauenswürdige Verteilungspakete erlauben**.

  e. Wählen Sie das Kriterium für die Vertrauenswürdigkeit der ausführbaren Datei oder des Installationspakets aus: **Zertifikatdetails** oder **SHA256-Hash**.

  f. Klicken Sie auf **OK**.

  Die ausführbare Datei oder das Installationspaket wird der Liste hinzugefügt.

- **Mehrere mittels Hash hinzufügen**

  a. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Mehrere Pakte mittels Hash hinzufügen** aus.

  b. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster eine beliebige Anzahl von Dateien oder Installationspaketen aus.

  c. Klicken Sie auf **Öffnen**.

  Die ausführbaren Dateien oder die Installationspakete werden der Liste hinzugefügt. Der SHA256-Hash ist in den Eigenschaften angegeben.

- **Aus Datei importieren**

  a. Klicken Sie auf **Importieren**.

  b. Wählen Sie im angezeigten Fenster eine .txt-Datei mit Informationen über ausführbare Dateien und Installationspakete aus.

  c. Klicken Sie auf **Öffnen**.

  Die ausführbaren Dateien oder die Installationspakete werden der Liste hinzugefügt. Der SHA256-Hash ist in den Eigenschaften angegeben.

Wenn Sie ein vertrauenswürdiges Installationspaket auf Basis einer ausführbaren Datei erstellen und zuvor in den Einstellungen der vertrauenswürdigen Zone einen Prozess basierend auf dieser ausführbaren Datei hinzugefügt und ihn für die Komponente Kontrolle des Programmstarts als vertrauenswürdig eingestuft haben, besitzen die Einstellungen der vertrauenswürdigen Zone eine höhere Priorität. Kaspersky Embedded Systems Security blockiert den Start dieser ausführbaren Datei, betrachtet den Prozess der ausführbaren Datei jedoch als vertrauenswürdig.

10. Bearbeiten Sie bei Bedarf die Liste der hinzugefügten ausführbaren Dateien und Installationspakete, indem Sie auf die Schaltfläche **Ändern** klicken.

11. Entfernen Sie bei Bedarf die hinzugefügten ausführbaren Dateien und Installationspakete, indem Sie auf die Schaltfläche **Löschen** klicken. In diesem Fall wird die Ausführung von entpackten ausführbaren Dateien erlaubt.

    Um die Ausführung entpackter ausführbarer Dateien zu verhindern, müssen Sie Kaspersky Embedded Systems Security von dem geschützten Gerät entfernen oder für die entpackten Dateien Verbotsregeln der Kontrolle des Programmstarts erstellen.

12. Klicken Sie auf **OK**.

So konfigurieren Sie die Kontrolle der Software-Verteilung (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Kontrolle des Programmstarts** aus.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

3. Wählen Sie die Registerkarte **Kontrolle der Software-Verteilung** aus.

4. Aktivieren Sie die Funktion **Software-Verteilung über aufgelistete Programme und Pakete automatisch erlauben**. Diese Funktionalität erstellt automatisch Ausnahmen für alle Dateien, die mithilfe ausführbarer Dateien und mithilfe von Installationspaketen gestartet werden, die in der Liste angegeben sind.

   Sie können die Funktionalität **Software-Verteilung über aufgelistete Programme und Pakete automatisch erlauben** aktivieren, wenn auf der Registerkarte **Allgemein** die Funktionalität **Regeln auf ausführbare Dateien anwenden** aktiviert ist.

5. Deaktivieren Sie bei Bedarf die Funktionalität **Software-Verteilung über Windows-Installationsprogramm immer erlauben**. Diese Funktionalität erstellt automatisch Ausnahmen für alle Dateien, die mithilfe des Windows-Installationsprogramms gestartet werden.

   Abschalten dieser Funktion kann zu Problemen beim Update der Dateien des Betriebssystems führen und ferner den Start von Dateien verhindern, die aus einem Installationspaket extrahiert werden.

6. Aktivieren Sie bei Bedarf die Funktionalität **Software-Verteilung über SCCM unter Verwendung des intelligenten Hintergrundübertragungsdienstes immer erlauben**. Diese Funktion ermöglicht die Verteilung von Software mithilfe der Lösung System Center Configuration Manager.

Wenn diese Funktion aktiviert ist, ermöglicht Kaspersky Embedded Systems Security die Bereitstellung von Microsoft Windows mithilfe von System Center Configuration Manager. Die Anwendung ermöglicht die Softwareverteilung nur über Background Intelligent Transfer Service. Das Programm kontrolliert den Start von ausführbaren Dateien mit den Erweiterungen .EXE und .MSI.

Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an das geschützte Gerät bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät ausgeführt wurde.

7. Fügen Sie ausführbare Dateien und Installationspakete hinzu, deren Start erlaubt werden soll:

- **Manuell hinzufügen**

  a. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Ein Programmpaket hinzufügen** aus.

  b. Klicken Sie im angezeigten Fenster auf **Durchsuchen**.

  c. Wählen Sie die ausführbare Datei oder das Installationspaket aus.

  Die Felder unter **Vertrauenskriterien** werden automatisch mit Informationen über die ausgewählte Datei ausgefüllt.

  d. Aktivieren Sie bei Bedarf die Funktionalität **Start für alle untergeordneten Dateien als vertrauenswürdige Verteilungspakete erlauben**.

  e. Wählen Sie das Kriterium für die Vertrauenswürdigkeit der ausführbaren Datei oder des Installationspakets aus: **Zertifikatdetails** oder **SHA256-Hash**.

  f. Klicken Sie auf **OK**.

  Die ausführbare Datei oder das Installationspaket wird der Liste hinzugefügt.

- **Mehrere mittels Hash hinzufügen**

  a. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** den Punkt **Mehrere Pakte mittels Hash hinzufügen** aus.

  b. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster eine beliebige Anzahl von Dateien oder Installationspaketen aus.

  c. Klicken Sie auf **Öffnen**.

  Die ausführbaren Dateien oder die Installationspakete werden der Liste hinzugefügt. Der SHA256-Hash ist in den Eigenschaften angegeben.

- **Aus Datei importieren**

  a. Klicken Sie auf **Importieren**.

  b. Wählen Sie im angezeigten Fenster eine .txt-Datei mit Informationen über ausführbare Dateien und Installationspakete aus.

  c. Klicken Sie auf **Öffnen**.

Die ausführbaren Dateien oder die Installationspakete werden der Liste hinzugefügt. Der SHA256-Hash ist in den Eigenschaften angegeben.

Wenn Sie ein vertrauenswürdiges Installationspaket auf Basis einer ausführbaren Datei erstellen und zuvor in den Einstellungen der vertrauenswürdigen Zone einen Prozess basierend auf dieser ausführbaren Datei hinzugefügt und ihn für die Komponente Kontrolle des Programmstarts als vertrauenswürdig eingestuft haben, besitzen die Einstellungen der vertrauenswürdigen Zone eine höhere Priorität. Kaspersky Embedded Systems Security blockiert den Start dieser ausführbaren Datei, betrachtet den Prozess der ausführbaren Datei jedoch als vertrauenswürdig.

8. Bearbeiten Sie bei Bedarf die Liste der hinzugefügten ausführbaren Dateien und Installationspakete, indem Sie auf die Schaltfläche **Ändern** klicken.

9. Entfernen Sie bei Bedarf die hinzugefügten ausführbaren Dateien und Installationspakete, indem Sie auf die Schaltfläche **Löschen** klicken. In diesem Fall wird die Ausführung von entpackten ausführbaren Dateien erlaubt.

Um die Ausführung entpackter ausführbarer Dateien zu verhindern, müssen Sie Kaspersky Embedded Systems Security von dem geschützten Gerät entfernen oder für die entpackten Dateien Verbotsregeln der Kontrolle des Programmstarts erstellen.

10. Klicken Sie auf **OK**.

So konfigurieren Sie die Kontrolle der Software-Verteilung (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.

5. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Anpassen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

6. Wählen Sie die Registerkarte **Kontrolle der Software-Verteilung** aus.

7. Aktivieren Sie die Funktion **Verteilung von Programmen mittels aufgelisteter Programme und Installationspakete automatisch erlauben**. Diese Funktionalität erstellt automatisch Ausnahmen für alle Dateien, die mithilfe ausführbarer Dateien und mithilfe von Installationspaketen gestartet werden, die in der Liste angegeben sind.

Sie können die Funktionalität **Verteilung von Programmen mittels aufgelisteter Programme und Installationspakete automatisch erlauben** aktivieren, wenn auf der Registerkarte **Allgemein** die Funktionalität **Regeln auf ausführbare Dateien anwenden** aktiviert ist.

8. Deaktivieren Sie bei Bedarf die Funktionalität **Verteilung von Programmen mittels Windows Installer immer erlauben**. Diese Funktionalität erstellt automatisch Ausnahmen für alle Dateien, die mithilfe des Windows-Installationsprogramms gestartet werden.

   Abschalten dieser Funktion kann zu Problemen beim Update der Dateien des Betriebssystems führen und ferner den Start von Dateien verhindern, die aus einem Installationspaket extrahiert werden.

9. Aktivieren Sie bei Bedarf die Funktionalität **Verteilung von Programmen mittels SCCM und unter Verwendung des intelligenten Hintergrundübertragungsdienstes immer erlauben**. Diese Funktion ermöglicht die Verteilung von Software mithilfe der Lösung System Center Configuration Manager.

   Wenn diese Funktion aktiviert ist, ermöglicht Kaspersky Embedded Systems Security die Bereitstellung von Microsoft Windows mithilfe von System Center Configuration Manager. Die Anwendung ermöglicht die Softwareverteilung nur über Background Intelligent Transfer Service. Das Programm kontrolliert den Start von ausführbaren Dateien mit den Erweiterungen .EXE und .MSI.

   Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an das geschützte Gerät bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät ausgeführt wurde.

10. Fügen Sie ausführbare Dateien und Installationspakete hinzu, deren Start erlaubt werden soll:

    - **Manuell**

      a. Klicken Sie auf **Hinzufügen**.

      b. Wählen Sie unter **Vertrauenskriterien** das Kriterium für die Vertrauenswürdigkeit der ausführbaren Datei oder des Installationspakets aus: **Digitales Zertifikat verwenden** oder **SHA256-Hash verwenden**.

      c. Wenn Sie **Digitales Zertifikat verwenden** ausgewählt haben, geben Sie die Kopfzeile und den Fingerabdruck des Zertifikats ein, mit der bzw. dem die ausführbare Datei oder das Installationspaket signiert ist, sowie den Namen der ausführbaren Datei oder des Installationspakets.

      d. Wenn Sie **SHA256-Hash verwenden** ausgewählt haben, klicken Sie auf **Durchsuchen**, um die ausführbare Datei oder das Installationspaket auszuwählen.

      e. Aktivieren Sie bei Bedarf die Funktionalität **Start aller untergeordneten Dateien als vertrauenswürdige Installationspakete erlauben**.

      f. Klicken Sie auf **OK**.

      Die ausführbare Datei oder das Installationspaket wird der Liste hinzugefügt.

    - **Aus Datei importieren**

      a. Klicken Sie auf **Importieren**.

      b. Wählen Sie im angezeigten Fenster eine .txt-Datei mit Informationen über ausführbare Dateien und Installationspakete aus.

      c. Klicken Sie auf die Schaltfläche **Öffnen**.

Die ausführbaren Dateien oder die Installationspakete werden der Liste hinzugefügt. Der SHA256-Hash ist in den Eigenschaften angegeben.

Wenn Sie ein vertrauenswürdiges Installationspaket auf Basis einer ausführbaren Datei erstellen und zuvor in den Einstellungen der vertrauenswürdigen Zone einen Prozess basierend auf dieser ausführbaren Datei hinzugefügt und ihn für die Komponente Kontrolle des Programmstarts als vertrauenswürdig eingestuft haben, besitzen die Einstellungen der vertrauenswürdigen Zone eine höhere Priorität. Kaspersky Embedded Systems Security blockiert den Start dieser ausführbaren Datei, betrachtet den Prozess der ausführbaren Datei jedoch als vertrauenswürdig.

11. Bearbeiten Sie bei Bedarf die Liste der hinzugefügten ausführbaren Dateien und Installationspakete, indem Sie auf die Schaltfläche **Ändern** klicken.
12. Entfernen Sie bei Bedarf die hinzugefügten ausführbaren Dateien und Installationspakete, indem Sie auf die Schaltfläche **Löschen** klicken. In diesem Fall wird die Ausführung von entpackten ausführbaren Dateien erlaubt.

    Um die Ausführung entpackter ausführbarer Dateien zu verhindern, müssen Sie Kaspersky Embedded Systems Security von dem geschützten Gerät entfernen oder für die entpackten Dateien Verbotsregeln der Kontrolle des Programmstarts erstellen.

13. Klicken Sie auf **OK**.
14. Klicken Sie im Fenster **Kontrolle des Programmstarts** auf **OK**.

Regeln der Kontrolle des Programmstarts verwenden

Dieser Abschnitt enthält Anweisungen zum Erstellen einer Liste mit Regeln für die Kontrolle des Programmstarts.

Regeln zur Kontrolle des Programmstarts hinzufügen

So fügen Sie Regeln für die Kontrolle des Programmstarts hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.
4. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Einstellungen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

5. Wählen Sie die Registerkarte **Regeln** aus.

6. Wählen Sie in der Dropdown-Liste **Verwendung der Regeln** den Modus der Regelanwendung aus:

   - **Richtlinienregeln zu lokalen Regeln hinzufügen**. Das Programm wendet die in der Richtlinie festgelegte Regelliste zusammen mit den lokalen Regellisten an.

   - **Lokale Regeln durch Richtlinienregeln ersetzen**. Das Programm wendet die in der Richtlinie festgelegte Regelliste für die Kontrolle des Programmstarts auf der Gruppe von geschützten Geräten an. Das Erstellen, Bearbeiten und Anwenden der lokalen Regellisten ist nicht verfügbar.

7. Aktivieren Sie bei Bedarf die Funktionalität **Änderung lokaler Regeln durch Benutzer verweigern**.

   Ist diese Funktionalität aktiviert, so verweigert das Programm die lokale Bearbeitung von Regeln zur Kontrolle des Programmstarts in der Anwendungskonsole. Die Funktionalität ist standardmäßig deaktiviert.

8. Fügen Sie Regeln zur Kontrolle des Programmstarts auf eine der folgenden Arten hinzu:

   - **Manuell**

     a. Klicken Sie auf **Hinzufügen**.

        Das Fenster **Kontrolle des Programmstarts** wird geöffnet.

     b. Tragen Sie im Feld **Name** einen Namen für die Regel ein.

     c. Geben Sie bei Bedarf im Feld **Beschreibung** eine Beschreibung für die Regel ein.

     d. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Regel:

        - **Erlauben**, damit die Regel das Ausführen von in der Regel beschriebenen Programmen erlaubt.

        - **Ablehnen**, damit die Regel den Start von in der Regel beschriebenen Programmen blockiert.

     e. Wählen Sie in der Dropdown-Liste **Bereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

        - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Dateien kontrolliert.

        - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert. Dateien mit den folgenden Erweiterungen werden unterstützt: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

     f. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Kaspersky Embedded Systems 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 Embedded Systems 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.

     g. Fügen Sie Auslösebedingungen für die Regel der Kontrolle des Programmstarts hinzu.

     h. Fügen Sie Ausnahmen für die Auslösebedingungen der Regel der Kontrolle des Programmstarts hinzu.

i. Fügen Sie Benutzer und/oder Benutzergruppen hinzu, denen es erlaubt oder verboten ist, regelkonforme Programme zu starten.

j. Klicken Sie auf **OK**.

- **Durch das Importieren einer xml-Datei, die Regeln zur Kontrolle des Programmstarts enthält**

  a. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Importieren → Aus XML-Datei** aus.

  b. Wählen Sie aus, wie Sie Regeln zur Gerätekontrolle aus einer XML-Datei zu den in der Richtlinie verfügbaren Regeln hinzufügen möchten:

  - **Vorhandene Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
  - **Zu vorhandenen Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
  - **Mit vorhandenen Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht dupliziert. Wenn mindestens eine Regeleinstellung eindeutig ist, wird die Regel hinzugefügt.

  c. Geben Sie im folgenden Fenster den Pfad der xml-Datei an, die nach Abschluss der lokalen Aufgabe oder Gruppenaufgabe für *Erstellen von Regeln für die Kontrolle des Programmstarts* erstellt wurde.

  d. Klicken Sie auf **Öffnen**.

- **Basierend auf Kaspersky Security Center-Ereignissen mithilfe einer Anfrage**

  a. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Importieren → Erlaubnisregeln auf Basis von Kaspersky Security Center-Ereignissen (Anfrage) erstellen** aus.

  b. Wählen Sie das Prinzip aus, nach dem Regeln zur Liste der bereits festgelegten Regeln für die Kontrolle des Programmstarts hinzugefügt werden sollen:

  - **Zu vorhandenen Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
  - **Vorhandene Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
  - **Mit vorhandenen Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

  Das Fenster **Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.

  c. Wählen Sie die Ereignistypen aus, auf deren Grundlage das Programm Regeln für die Kontrolle des Programmstarts erstellen soll:

  - **Programmstart verweigert**.
  - **Modus „Nur Statistik“: App-Start verweigert**.

  d. Wählen Sie in der Dropdown-Liste **Anfrageereignisse, die in diesem Zeitraum generiert wurden** einen Zeitraum aus.

e. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Hash-Verwendung bevorzugen, wenn Regeln generiert werden**.

Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die Prüfsumme der Datei, um die Regel zu generieren, wenn sowohl die Prüfsumme als auch das Zertifikat der Datei verfügbar sind.

Wenn das Kontrollkästchen deaktiviert ist, verwendet Kaspersky Embedded Systems Security das digitale Zertifikat der Datei, um die Regel zu generieren, wenn sowohl die Prüfsumme als auch das Zertifikat der Datei verfügbar sind.

f. Klicken Sie auf **Regeln generieren**.

g. Klicken Sie auf **OK**.

- **Importieren einer txt-Datei mit einer Auswahl von Kaspersky Security Center-Ereignissen über blockierte 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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Protokolle und Meldungen**.
4. Klicken Sie im Block **Aufgabenprotokolle** auf **Einstellungen**.

   Das Fenster **Meldungen** wird geöffnet.
5. Erweitern Sie den Knoten **Kontrolle der lokalen Aktivität**.
6. Wählen Sie den Abschnitt **Kontrolle des Programmstarts** aus.
7. Aktivieren Sie in der Ereignisliste der Kontrolle des Programmstarts in der Spalte **Ereignisse an Kaspersky Security Center senden** die Kontrollkästchen für *Programmstart verboten* und *Programmstart im Testmodus verboten*.
8. Speichern Sie die vorgenommenen Änderungen.
9. Öffnen Sie die Registerkarte **Konfiguration von Ereignissen** der Richtlinie und vergewissern Sie sich, dass die Speicherdauer für Ereignisse, die im Feld **In der Administrationsserver-Datenbank speichern für (Tage)** angegeben ist, länger als der Zeitraum ist, für den Sie Informationen über verweigerte Programmstarts erfassen möchten (der Standardwert beträgt 30 Tage).

   Sobald die Speicherdauer für Protokolle der Komponente Kontrolle des Programmstarts abläuft, werden die protokollierten Ereignisse gelöscht und erscheinen nicht mehr im Bericht.
10. Aktivieren Sie die Richtlinie, die die Erfassung von Daten über verweigerte Programmstarts festlegt.
11. Ändern Sie bei Bedarf den Betriebsmodus der Komponente Kontrolle des Programmstarts.
12. Nach dem Ende des Zeitraums für das Sammeln von Informationen über verhinderte Programmstarts können Sie Ereignisse aus *Programmstart verboten* und *Programmstart im Testmodus verboten* auswählen und in eine txt-Datei exportieren. Einzelheiten finden Sie im Abschnitt „Ereignisauswahlen“ in der Hilfe zu Kaspersky Security Center.

13. Öffnen Sie die exportierte txt-Datei.

14. Bearbeiten Sie bei Bedarf die Liste der Ereignisse.

Die hinzugefügten Regeln für die Kontrolle des Programmstarts werden in der Liste angezeigt.

9. Führen Sie bei Bedarf Schritt 5 aus, um weitere Regeln für die Kontrolle des Programmstarts hinzuzufügen.

10. Bearbeiten Sie bei Bedarf die hinzugefügten Regeln der Kontrolle des Programmstarts, indem Sie auf die Schaltfläche **Ändern** klicken.

11. Löschen Sie bei Bedarf die hinzugefügten Regeln zur Kontrolle des Programmstarts, indem Sie auf die Schaltfläche **Löschen** klicken.

12. Klicken Sie auf **OK**.

So fügen Sie Regeln zur Kontrolle des Programmstarts hinzu (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Kontrolle des Programmstarts** aus.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

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

4. Fügen Sie Regeln zur Kontrolle des Programmstarts auf eine der folgenden Arten hinzu:

   - **Manuell**

     a. Klicken Sie auf **Hinzufügen**.

     Das Fenster **Kontrolle des Programmstarts** wird geöffnet.

     b. Tragen Sie im Feld **Name** einen Namen für die Regel ein.

     c. Geben Sie bei Bedarf im Feld **Beschreibung** eine Beschreibung für die Regel ein.

     d. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Regel:

     - **Erlauben**, damit die Regel das Ausführen von in der Regel beschriebenen Programmen erlaubt.
     - **Ablehnen**, damit die Regel den Start von in der Regel beschriebenen Programmen blockiert.

     e. Wählen Sie in der Dropdown-Liste **Bereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

     - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Dateien kontrolliert.
     - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert. Dateien mit den folgenden Erweiterungen werden unterstützt: .js, .vbs, .cmd, .bat, .py, .ps1, .pl, .msi, .msp, .mst, .com, .vbe, .jse, .psd1, .psm1, .pyd, .pyc, .pm, .hta, .chm, .wsf, .wsc, .wsh, .sct.

f. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Kaspersky Embedded Systems 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 Embedded Systems 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.

g. Fügen Sie Auslösebedingungen für die Regel der Kontrolle des Programmstarts hinzu.

h. Fügen Sie Ausnahmen für die Auslösebedingungen der Regel der Kontrolle des Programmstarts hinzu.

i. Fügen Sie Benutzer und/oder Benutzergruppen hinzu, denen es erlaubt oder verboten ist, regelkonforme Programme zu starten.

j. Klicken Sie auf **OK**.

- **Durch das Importieren einer xml-Datei, die Regeln zur Kontrolle des Programmstarts enthält**

a. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Importieren → Aus XML-Datei** aus.

b. Wählen Sie aus, wie Sie Regeln zur Gerätekontrolle aus einer XML-Datei zu den in der Richtlinie verfügbaren Regeln hinzufügen möchten:

- **Vorhandene Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
- **Zu vorhandenen Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
- **Mit vorhandenen Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht dupliziert. Wenn mindestens eine Regeleinstellung eindeutig ist, wird die Regel hinzugefügt.

c. Geben Sie im folgenden Fenster den Pfad der xml-Datei an, die nach Abschluss der lokalen Aufgabe oder Gruppenaufgabe für *Erstellen von Regeln für die Kontrolle des Programmstarts* erstellt wurde.

d. Klicken Sie auf **Öffnen**.

Die hinzugefügten Regeln für die Kontrolle des Programmstarts werden in der Liste angezeigt.

5. Führen Sie bei Bedarf Schritt 5 aus, um weitere Regeln für die Kontrolle des Programmstarts hinzuzufügen.
6. Bearbeiten Sie bei Bedarf die hinzugefügten Regeln der Kontrolle des Programmstarts, indem Sie auf die Schaltfläche **Ändern** klicken.
7. Löschen Sie bei Bedarf die hinzugefügten Regeln zur Kontrolle des Programmstarts, indem Sie auf die Schaltfläche **Löschen** klicken.
8. Klicken Sie auf **OK**.

So fügen Sie Regeln zur Kontrolle des Programmstarts hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.
5. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Anpassen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
6. Wählen Sie die Registerkarte **Regeln** aus.
7. Wählen Sie in der Dropdown-Liste **Anwendung von Regeln** den Modus der Regelanwendung aus:

   - **Richtlinienregeln zu lokalen Regeln hinzufügen**. Das Programm wendet die in der Richtlinie festgelegte Regelliste zusammen mit den lokalen Regellisten an.
   - **Lokale Regeln durch Richtlinienregeln ersetzen**. Das Programm wendet die in der Richtlinie festgelegte Regelliste für die Kontrolle des Programmstarts auf der Gruppe von geschützten Geräten an. Das Erstellen, Bearbeiten und Anwenden der lokalen Regellisten ist nicht verfügbar.
8. Aktivieren Sie bei Bedarf die Funktionalität **Änderung lokaler Regeln durch Benutzer verweigern**.

   Ist diese Funktionalität aktiviert, so verweigert das Programm die lokale Bearbeitung von Regeln zur Kontrolle des Programmstarts in der Anwendungskonsole. Die Funktionalität ist standardmäßig deaktiviert.
9. Fügen Sie Regeln zur Kontrolle des Programmstarts auf eine der folgenden Arten hinzu:

   - **Manuell**

     a. Klicken Sie auf **Hinzufügen**.

     Das Fenster **Einstellungen der Regel** wird geöffnet.

     b. Tragen Sie im Feld **Name** einen Namen für die Regel ein.

     c. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Regel:

     - **Erlauben**, damit die Regel das Ausführen von in der Regel beschriebenen Programmen erlaubt.
     - **Ablehnen**, damit die Regel den Start von in der Regel beschriebenen Programmen blockiert.

     d. Wählen Sie in der Dropdown-Liste **Bereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

     - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Dateien kontrolliert.
     - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.

e. Aktivieren Sie das Kontrollkästchen **Für andere Benutzer verbieten**, damit das Programm den Start von in der Regel beschriebenen Programmen für alle Benutzer blockiert, die nicht auf der Registerkarte **Benutzer oder Gruppe** genannt sind.

f. Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Programme mit Update-Funktionen**, damit Kaspersky Embedded Systems 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 Embedded Systems 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.

g. Fügen Sie Auslösebedingungen für die Regel der Kontrolle des Programmstarts hinzu.

h. Fügen Sie Ausnahmen für die Auslösebedingungen der Regel der Kontrolle des Programmstarts hinzu.

i. **Fügen Sie Benutzer und/oder Benutzergruppen hinzu, denen es erlaubt oder verboten ist, regelkonforme Programme zu starten**.

a. Wählen Sie die Registerkarte **Benutzer oder Gruppe** aus.

b. Klicken Sie auf **Hinzufügen**.

c. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Namen eines Benutzers bzw. einer Benutzergruppe ein oder wählen Sie einen Benutzer bzw. eine Gruppe aus.

d. Klicken Sie auf **Auswählen**.

e. Führen Sie die Schritte b bis d für jeden Benutzer oder jede Benutzergruppe aus.

j. Klicken Sie auf **OK**.

Die hinzugefügten Regeln für die Kontrolle des Programmstarts werden in der Liste angezeigt.

- **Durch das Importieren einer xml-Datei, die Regeln zur Kontrolle des Programmstarts enthält**

a. Klicken Sie auf **Import**.

b. Klicken Sie im folgenden Fenster **Aus Datei importieren** auf die Schaltfläche **Auswählen**.

c. Geben Sie den Pfad der xml-Datei an, die nach Abschluss der lokalen Aufgabe oder Gruppenaufgabe für *Erstellen von Regeln für die Kontrolle des Programmstarts*.

d. Klicken Sie auf **Öffnen**.

e. Klicken Sie auf **Import**.

Die importierten Regeln zur Kontrolle des Programmstarts werden der Liste der vorhandenen Regeln hinzugefügt. Regeln mit identischen Einstellungen werden nicht dupliziert. Wenn mindestens eine Regeleinstellung eindeutig ist, wird die Regel hinzugefügt.

- **Durch das Importieren einer xml-Datei, die Regeln zur Kontrolle des Programmstarts aus Kaspersky Embedded Systems Security 3.4 enthält**

  a. Klicken Sie auf **Aus vorheriger Version importieren**.

  b. Klicken Sie im folgenden Fenster **Aus Datei importieren** auf die Schaltfläche **Auswählen**.

  c. Geben Sie den Pfad der xml-Datei mit Regeln für die Kontrolle des Programmstarts an, die aus Kaspersky Embedded Systems Security 3.4 exportiert wurde.

  d. Klicken Sie auf **Öffnen**.

  e. Klicken Sie auf **Import**.

  Die importierten Regeln zur Kontrolle des Programmstarts werden der Liste der vorhandenen Regeln hinzugefügt. Regeln mit identischen Einstellungen werden nicht dupliziert. Wenn mindestens eine Regeleinstellung eindeutig ist, wird die Regel hinzugefügt.

- **Durch den Import von Regeln aus einer Berichtsdatei von Kaspersky Security Center**

  a. Klicken Sie auf **Aus KSC-Bericht importieren**.

  b. Wählen Sie im folgenden Fenster die txt-Datei aus, in die die Ereignisse aus dem Bericht exportiert wurden.

  c. Klicken Sie auf **Öffnen**.

  Regeln, die auf dem Bericht von Kaspersky Security Center basieren, werden zur Regelliste in der Richtlinie hinzugefügt.

- **Basierend auf Kaspersky Security Center-Ereignissen mithilfe einer Anfrage**

  a. Klicken Sie auf **Regeln aus KSC-Ereignissen erlauben**.

  Das Fenster **Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.

  b. Wählen Sie die Typen der Ereignisse aus, auf deren Grundlage das Programm Regeln für die Kontrolle des Programmstarts erstellen soll:

  - **Alle Ereignisse**.
  - **Programmstart verboten**.
  - **Modus "Nur Statistik": Programmstart verboten**.

  c. Wählen Sie in der Dropdown-Liste **Ereignisse verwenden, die in diesem Zeitraum erstellt wurden** einen Zeitraum aus.

  d. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Nutzung des Hashs beim Generieren von Regeln priorisieren**.

  Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die Prüfsumme der Datei, um die Regel zu generieren, wenn sowohl die Prüfsumme als auch das Zertifikat der Datei verfügbar sind.

Wenn das Kontrollkästchen deaktiviert ist, verwendet Kaspersky Embedded Systems Security das digitale Zertifikat der Datei, um die Regel zu generieren, wenn sowohl die Prüfsumme als auch das Zertifikat der Datei verfügbar sind.

e. Geben Sie bei Bedarf im Feld **Ereignisse verwenden, die für eine Gruppe von verwalteten Geräten erstellt wurden** den Namen der Gruppe für verwaltete Geräte an.

f. Klicken Sie auf **Regeln erstellen**.

g. Wählen Sie in der Dropdown-Liste **Regel zum Hinzufügen zur Hauptliste** das Prinzip aus, nach dem die Regeln zur Liste der bereits erstellten Regeln für die Kontrolle des Programmstarts hinzugefügt werden sollen:

- **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
- **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.

h. Wählen Sie die Regeln aus, die in die Regeln für die Kontrolle des Programmstarts innerhalb der Richtlinie exportiert werden sollen, und klicken Sie auf die Schaltfläche **Export**.

i. Speichern Sie die vorgenommenen Änderungen.

10. Führen Sie bei Bedarf Schritt 5 aus, um weitere Regeln für die Kontrolle des Programmstarts hinzuzufügen.
11. Bearbeiten Sie bei Bedarf die hinzugefügten Regeln der Kontrolle des Programmstarts, indem Sie auf die Schaltfläche **Ändern** klicken.
12. Löschen Sie bei Bedarf die hinzugefügten Regeln zur Kontrolle des Programmstarts, indem Sie auf die Schaltfläche **Löschen** klicken.
13. Klicken Sie auf **OK**.

Auslösebedingungen für die Regel der Kontrolle des Programmstarts hinzufügen

So fügen Sie Auslösebedingungen für eine Regel der Kontrolle des Programmstarts hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.
4. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Einstellungen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Wählen Sie die Registerkarte **Regeln** aus.

6. Führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**, wenn Sie eine neue Regel für die Kontrolle des Programmstarts hinzufügen.

   b. Wählen Sie in der Liste der Regeln für die Kontrolle des Programmstarts die Regel aus, für die Sie Auslösebedingungen hinzufügen möchten, und klicken Sie auf die Schaltfläche **Ändern**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.

7. Wählen Sie auf der Registerkarte **Bedingungen** im Kontextmenü der Schaltfläche **Hinzufügen** eine Auslösebedingung für die Regel der Kontrolle des Programmstarts aus:

   - **Informationen aus Datei**. **Informationen aus der ausgewählten Datei** werden als Auslösebedingung der Regel verwendet.

     a. Klicken Sie im Fenster **Informationen aus Datei** auf **Durchsuchen**.

     Das Microsoft Windows-Standardfenster **Datei öffnen** wird geöffnet.

     b. Wählen Sie die Datei aus.

     c. Klicken Sie auf **Öffnen**.

     Informationen über die ausgewählte Datei werden im Fenster **Informationen aus Datei** angezeigt.

     d. Wählen Sie mindestens eine Option aus:

     - **Zertifikatdetails**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die mit einem digitalen Zertifikat mit den angegebenen Daten signiert sind, nicht von der Regel kontrolliert.
     - **Metadaten**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die die angegebenen Metadaten haben, nicht von der Regel kontrolliert.
     - **Datei-Hash**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die den angegebenen SHA256-Hash haben, nicht von der Regel kontrolliert.
     - **Dateipfad**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen unter dem angegebenen Pfad, nicht von der Regel kontrolliert.

     e. Geben Sie bei Bedarf im Feld **Befehlszeile** den Befehl ein, mit dem das Programm über die Befehlszeile gestartet werden soll. Der Start dieses Programms wird von der Regel kontrolliert. Um eine Maske festzulegen, können Sie die Zeichen „?“ und „*“ verwenden.

     > Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie in Pfaden den umgekehrten Schrägstrich („\“).

     f. Klicken Sie auf **OK**.

   - **Laufwerkstyp**. Der Start von Programmen von allen Wechseldatenträgern, die mit dem geschützten Computer verbunden sind, wird von der Regel kontrolliert.
   - **KL-Kategorie**. Der Start von Programmen, die zu den ausgewählten KL-Kategorien gehören, wird von der Regel kontrolliert.

- **Laut KSN vertrauenswürdig**. Der Start von Programmen, die laut KSN vertrauenswürdig sind, wird von der Regel kontrolliert.
- **Laut KSN nicht vertrauenswürdig**. Der Start von Programmen, die laut KSN nicht vertrauenswürdig sind, wird von der Regel kontrolliert.
- **Laut Betriebssystem vertrauenswürdig**. Der Start von Programmen, die im Betriebssystem als vertrauenswürdig gelten, wird von der Regel kontrolliert.

Die hinzugefügte Bedingung wird in der Liste angezeigt.

8. Führen Sie bei Bedarf den vorherigen Schritt der Anleitung für jede weitere Auslösebedingung der Regel aus.
9. Bearbeiten Sie bei Bedarf die Auslösebedingungen der Regel, indem Sie auf die Schaltfläche **Ändern** klicken.
10. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Auslösebedingungen für eine Regel zur Kontrolle des Programmstarts hinzu (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Kontrolle des Programmstarts** aus.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
3. Wählen Sie die Registerkarte **Regeln** aus.
4. Führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**, wenn Sie eine neue Regel für die Kontrolle des Programmstarts hinzufügen.

   b. Wählen Sie in der Liste der Regeln für die Kontrolle des Programmstarts die Regel aus, für die Sie Auslösebedingungen hinzufügen möchten, und klicken Sie auf die Schaltfläche **Ändern**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.
5. Wählen Sie auf der Registerkarte **Bedingungen** im Kontextmenü der Schaltfläche **Hinzufügen** eine Auslösebedingung für die Regel der Kontrolle des Programmstarts aus:

   - **Informationen aus Datei**. **Informationen aus der ausgewählten Datei** werden als Auslösebedingung der Regel verwendet.

     a. Klicken Sie im Fenster **Informationen aus Datei** auf **Durchsuchen**.

     Das Microsoft Windows-Standardfenster **Datei öffnen** wird geöffnet.

     b. Wählen Sie die Datei aus.

     c. Klicken Sie auf **Öffnen**.

     Informationen über die ausgewählte Datei werden im Fenster **Informationen aus Datei** angezeigt.

d. Wählen Sie mindestens eine Option aus:

- **Zertifikatdetails**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die mit einem digitalen Zertifikat mit den angegebenen Daten signiert sind, nicht von der Regel kontrolliert.
- **Metadaten**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die die angegebenen Metadaten haben, nicht von der Regel kontrolliert.
- **Datei-Hash**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die den angegebenen SHA256-Hash haben, nicht von der Regel kontrolliert.
- **Dateipfad**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen unter dem angegebenen Pfad, nicht von der Regel kontrolliert.

e. Geben Sie bei Bedarf im Feld **Befehlszeile** den Befehl ein, mit dem das Programm über die Befehlszeile gestartet werden soll. Der Start dieses Programms wird von der Regel kontrolliert. Um eine Maske festzulegen, können Sie die Zeichen „?“ und „*“ verwenden.

> Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie in Pfaden den umgekehrten Schrägstrich („\“).

f. Klicken Sie auf **OK**.

- **Laufwerkstyp**. Der Start von Programmen von allen Wechseldatenträgern, die mit dem geschützten Computer verbunden sind, wird von der Regel kontrolliert.
- **KL-Kategorie**. Der Start von Programmen, die zu den ausgewählten KL-Kategorien gehören, wird von der Regel kontrolliert.
- **Laut KSN vertrauenswürdig**. Der Start von Programmen, die laut KSN vertrauenswürdig sind, wird von der Regel kontrolliert.
- **Laut KSN nicht vertrauenswürdig**. Der Start von Programmen, die laut KSN nicht vertrauenswürdig sind, wird von der Regel kontrolliert.
- **Laut Betriebssystem vertrauenswürdig**. Der Start von Programmen, die im Betriebssystem als vertrauenswürdig gelten, wird von der Regel kontrolliert.

Die hinzugefügte Bedingung wird in der Liste angezeigt.

6. Führen Sie bei Bedarf den vorherigen Schritt der Anleitung für jede weitere Auslösebedingung der Regel aus.
7. Bearbeiten Sie bei Bedarf die Auslösebedingungen der Regel, indem Sie auf die Schaltfläche **Ändern** klicken.
8. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Auslösebedingungen für eine Regel zur Kontrolle des Programmstarts hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.

5. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Anpassen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

6. Wählen Sie die Registerkarte **Regeln** aus.

7. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Einstellungen der Regel** wird geöffnet.

8. Klicken Sie auf der Registerkarte **Bedingungen** auf **Hinzufügen**.

   Das Fenster **Einstellungen der Regel** wird geöffnet.

9. Wählen Sie eine Auslösebedingungen für die Regel der Kontrolle des Programmstarts aus:

   - **Informationen aus Datei**. **Informationen aus der Datei** werden als Auslösebedingung der Regel verwendet.

     a. Geben Sie unter **Auslösekriterien für die Regel** einen Wert für mindestens ein Kriterium an:

     - **Digitales Zertifikat**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die mit einem digitalen Zertifikat mit den angegebenen Daten signiert sind, nicht von der Regel kontrolliert.
     - **Metadaten**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die die angegebenen Metadaten haben, nicht von der Regel kontrolliert.
     - **SHA256-Hash**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die den angegebenen SHA256-Hash haben, nicht von der Regel kontrolliert.
     - **Dateipfad**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen unter dem angegebenen Pfad, nicht von der Regel kontrolliert.

     b. Klicken Sie auf **OK**.

   - **Aus KL-Kategorie**. Der Start von Programmen, die zu den ausgewählten KL-Kategorien gehören, wird von der Regel kontrolliert.
   - **Wechseldatenträger**. Der Start von Programmen von allen Wechseldatenträgern, die mit dem geschützten Computer verbunden sind, wird von der Regel kontrolliert.
   - **Laut Betriebssystem vertrauenswürdig**. Der Start von Programmen, die im Betriebssystem als vertrauenswürdig gelten, wird von der Regel kontrolliert.

   Die hinzugefügte Bedingung wird in der Liste angezeigt.

10. Führen Sie bei Bedarf die Schritte 4 bis 5 der Anweisungen für jede weitere Auslösebedingung der Regel aus.

11. Bearbeiten Sie bei Bedarf die Auslösebedingungen der Regel, indem Sie auf die Schaltfläche **Ändern** klicken.

12. Speichern Sie die vorgenommenen Änderungen.

Ausnahmen für den Gültigkeitsbereich einer Regel für die Kontrolle des Programmstarts hinzufügen

So fügen Sie Ausnahmen für den Gültigkeitsbereich einer Regel der Kontrolle des Programmstarts hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.
4. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Einstellungen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Wählen Sie die Registerkarte **Regeln** aus.
6. Führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**, wenn Sie eine neue Regel für die Kontrolle des Programmstarts hinzufügen.

   b. Wählen Sie in der Liste der Regeln für die Kontrolle des Programmstarts die Regel aus, für die Sie Ausnahmen hinzufügen möchten, und klicken Sie auf die Schaltfläche **Ändern**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.
7. Wählen Sie auf der Registerkarte **Ausnahmen** im Kontextmenü der Schaltfläche **Hinzufügen** ein Kriterium für das Erstellen einer Ausnahme für den Gültigkeitsbereich der Regel für die Kontrolle des Programmstarts aus:

   - **Informationen aus Datei**. **Informationen aus der ausgewählten Datei** werden als Kriterium verwendet.

     a. Klicken Sie im Fenster **Informationen aus Datei** auf **Durchsuchen**.

     Das Microsoft Windows-Standardfenster **Datei öffnen** wird geöffnet.

     b. Wählen Sie die Datei aus.

     c. Klicken Sie auf **Öffnen**.

     Informationen über die ausgewählte Datei werden im Fenster **Informationen aus Datei** angezeigt.

     d. Wählen Sie mindestens eine Option aus:

     - **Zertifikatdetails**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die mit einem digitalen Zertifikat mit den angegebenen Daten signiert sind, nicht von der Regel kontrolliert.
     - **Metadaten**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die die angegebenen Metadaten haben, nicht von der Regel kontrolliert.

- **Datei-Hash**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die den angegebenen SHA256-Hash haben, nicht von der Regel kontrolliert.

- **Dateipfad**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen unter dem angegebenen Pfad, nicht von der Regel kontrolliert.

e. Geben Sie bei Bedarf im Feld **Befehlszeile** den Befehl ein, mit dem das Programm über die Befehlszeile gestartet werden soll. Der Start dieses Programms wird nicht von der Regel kontrolliert. Um eine Maske festzulegen, können Sie die Zeichen „?“ und „*“ verwenden.

> Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie in Pfaden den umgekehrten Schrägstrich („\“).

f. Klicken Sie auf **OK**.

- **Laufwerkstyp**. Der Start von Programmen von allen Wechseldatenträgern, die mit dem geschützten Computer verbunden sind, wird nicht von der Regel kontrolliert.

- **KL-Kategorie**. Der Start von Programmen, die zu den ausgewählten KL-Kategorien gehören, wird nicht von der Regel kontrolliert.

- **Laut KSN vertrauenswürdig**. Der Start von Programmen, die laut KSN vertrauenswürdig sind, wird nicht von der Regel kontrolliert.

- **Laut KSN nicht vertrauenswürdig**. Der Start von Programmen, die laut KSN nicht vertrauenswürdig sind, wird nicht von der Regel kontrolliert.

- **Laut Betriebssystem vertrauenswürdig**. Der Start von Programmen, die im Betriebssystem als vertrauenswürdig gelten, wird nicht von der Regel kontrolliert.

Die hinzugefügte Ausnahme wird in der Liste angezeigt.

8. Führen Sie bei Bedarf den vorherigen Schritt der Anleitung aus, um die jeweils nächste Ausnahme für den Gültigkeitsbereich der Regel für die Kontrolle des Programmstarts hinzuzufügen.

9. Bearbeiten Sie bei Bedarf die Ausnahmen, indem Sie auf die Schaltfläche **Ändern** klicken.

10. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Ausnahmen für den Gültigkeitsbereich einer Regel der Kontrolle des Programmstarts hinzu (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Kontrolle des Programmstarts** aus.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

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

4. Führen Sie einen der folgenden Schritte aus:

   a. Klicken Sie auf die Schaltfläche **Hinzufügen**, wenn Sie eine neue Regel für die Kontrolle des Programmstarts hinzufügen.

   b. Wählen Sie in der Liste der Regeln für die Kontrolle des Programmstarts die Regel aus, für die Sie Ausnahmen hinzufügen möchten, und klicken Sie auf die Schaltfläche **Ändern**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.

5. Wählen Sie auf der Registerkarte **Ausnahmen** im Kontextmenü der Schaltfläche **Hinzufügen** ein Kriterium für das Erstellen einer Ausnahme für den Gültigkeitsbereich der Regel für die Kontrolle des Programmstarts aus:

   - **Informationen aus Datei**. **Informationen aus der ausgewählten Datei** werden als Kriterium verwendet.

     a. Klicken Sie im Fenster **Informationen aus Datei** auf **Durchsuchen**.

     Das Microsoft Windows-Standardfenster **Datei öffnen** wird geöffnet.

     b. Wählen Sie die Datei aus.

     c. Klicken Sie auf **Öffnen**.

     Informationen über die ausgewählte Datei werden im Fenster **Informationen aus Datei** angezeigt.

     d. Wählen Sie mindestens eine Option aus:

     - **Zertifikatdetails**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die mit einem digitalen Zertifikat mit den angegebenen Daten signiert sind, nicht von der Regel kontrolliert.
     - **Metadaten**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die die angegebenen Metadaten haben, nicht von der Regel kontrolliert.
     - **Datei-Hash**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die den angegebenen SHA256-Hash haben, nicht von der Regel kontrolliert.
     - **Dateipfad**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen unter dem angegebenen Pfad, nicht von der Regel kontrolliert.

     e. Geben Sie bei Bedarf im Feld **Befehlszeile** den Befehl ein, mit dem das Programm über die Befehlszeile gestartet werden soll. Der Start dieses Programms wird nicht von der Regel kontrolliert. Um eine Maske festzulegen, können Sie die Zeichen „?“ und „*“ verwenden.

     > Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie in Pfaden den umgekehrten Schrägstrich („\“).

     f. Klicken Sie auf **OK**.

   - **Laufwerkstyp**. Der Start von Programmen von allen Wechseldatenträgern, die mit dem geschützten Computer verbunden sind, wird nicht von der Regel kontrolliert.
   - **KL-Kategorie**. Der Start von Programmen, die zu den ausgewählten KL-Kategorien gehören, wird nicht von der Regel kontrolliert.
   - **Laut KSN vertrauenswürdig**. Der Start von Programmen, die laut KSN vertrauenswürdig sind, wird nicht von der Regel kontrolliert.

- **Laut KSN nicht vertrauenswürdig**. Der Start von Programmen, die laut KSN nicht vertrauenswürdig sind, wird nicht von der Regel kontrolliert.

- **Laut Betriebssystem vertrauenswürdig**. Der Start von Programmen, die im Betriebssystem als vertrauenswürdig gelten, wird nicht von der Regel kontrolliert.

Die hinzugefügte Ausnahme wird in der Liste angezeigt.

6. Führen Sie bei Bedarf den vorherigen Schritt der Anleitung aus, um die jeweils nächste Ausnahme für den Gültigkeitsbereich der Regel für die Kontrolle des Programmstarts hinzuzufügen.

7. Bearbeiten Sie bei Bedarf die Ausnahmen, indem Sie auf die Schaltfläche **Ändern** klicken.

8. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie Ausnahmen für den Gültigkeitsbereich einer Regel der Kontrolle des Programmstarts hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.

5. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Anpassen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

6. Wählen Sie die Registerkarte **Regeln** aus.

7. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Einstellungen der Regel** wird geöffnet.

8. Klicken Sie auf der Registerkarte **Ausnahmen** auf **Hinzufügen**.

   Das Fenster **Einstellungen der Regel** wird geöffnet.

9. Wählen Sie ein Kriterium aus, das eine Ausnahme für den Gültigkeitsbereich der Regel für die Kontrolle des Programmstarts festlegt:

   - **Informationen aus Datei**. Der Start von Programmen, deren Daten mit den **Daten in der Datei** übereinstimmen, wird nicht von der Regel kontrolliert.

     a. Geben Sie unter **Auslösekriterien für die Regel** einen Wert für mindestens ein Kriterium an:

     - **Digitales Zertifikat**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die mit einem digitalen Zertifikat mit den angegebenen Daten signiert sind, nicht von der Regel kontrolliert.

     - **Metadaten**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die die angegebenen Metadaten haben, nicht von der Regel kontrolliert.

- **SHA256-Hash**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen, die den angegebenen SHA256-Hash haben, nicht von der Regel kontrolliert.

- **Dateipfad**. Ist dieses Kontrollkästchen aktiviert, wird der Start von Programmen unter dem angegebenen Pfad, nicht von der Regel kontrolliert.

b. Klicken Sie auf **OK**.

- **KL-Kategorie**. Der Start von Programmen, die zu den ausgewählten KL-Kategorien gehören, wird nicht von der Regel kontrolliert.

- **Laufwerkstyp**. Der Start von Programmen von allen Wechseldatenträgern, die mit dem geschützten Computer verbunden sind, wird nicht von der Regel kontrolliert.

- **Laut Betriebssystem vertrauenswürdig**. Der Start von Programmen, die im Betriebssystem als vertrauenswürdig gelten, wird nicht von der Regel kontrolliert.

Die hinzugefügte Bedingung wird in der Liste angezeigt.

10. Führen Sie bei Bedarf die Schritte 4 und 5 der Anleitung aus, um die jeweils nächste Ausnahme für den Gültigkeitsbereich der Regel für die Kontrolle des Programmstarts hinzuzufügen.

11. Bearbeiten Sie bei Bedarf die Ausnahmen, indem Sie auf die Schaltfläche **Ändern** klicken.

12. Speichern Sie die vorgenommenen Änderungen.

Ausführung aller Programme erlauben

Sie können den Start aller Programme mithilfe von speziell konfigurierten Erlaubnisregeln für die Kontrolle des Programmstarts zulassen.

So erlauben Sie den Start aller Programme:

1. Fügen Sie manuell zwei Erlaubnisregeln für die Kontrolle des Programmstarts mit den folgenden Parametern hinzu:

   - Regeltyp: *Erlauben*, Geltungsbereich: *Ausführbare Dateien*, Dateipfad: `?:\`.

   - Regeltyp: *Erlauben*, Geltungsbereich: *Skripte und MSI-Pakete*, Dateipfad: `?:\`.

2. Falls Verbotsregeln für die Kontrolle des Programmstarts hinzugefügt wurden, löschen Sie diese Verbotsregeln.

3. Löschen Sie die Ausnahmen für alle zuvor erstellten Erlaubnisregeln der Kontrolle des Programmstarts.

4. Speichern Sie die vorgenommenen Änderungen.

Regeln für die Kontrolle des Programmstarts exportieren

Sie können die Liste der Regeln für die Kontrolle des Programmstarts und die Liste der vertrauenswürdigen Installationspakete für die Kontrolle der Installationspakete in eine XML-Datei exportieren. Mit der Exportfunktion können Sie ein Backup für die Liste der Regeln für die Kontrolle des Programmstarts anlegen oder die Liste auf einen anderen Server migrieren.

Exportieren von Regeln für die Kontrolle des Programmstarts in der Kaspersky Security Center Verwaltungskonsole

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.
4. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Einstellungen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
5. Wechseln Sie zur Registerkarte **Regeln**, um Regeln für die Kontrolle des Programmstarts zu exportieren, oder zur Registerkarte **Kontrolle der Software-Verteilung**, um Regeln für die Kontrolle der Installationspakete zu exportieren.
6. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.
7. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

   a. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

   b. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.
8. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

Kaspersky Embedded Systems Security exportiert die Liste der Regeln in die XLM-Datei.

Exportieren von Regeln für die Kontrolle des Programmstarts in der Konsole für Kaspersky Embedded Systems Security

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Kontrolle des Programmstarts** aus.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
3. Wechseln Sie zur Registerkarte **Regeln**, um Regeln für die Kontrolle des Programmstarts zu exportieren, oder zur Registerkarte **Kontrolle der Software-Verteilung**, um Regeln für die Kontrolle der Installationspakete zu exportieren.

4. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

5. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

   a. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

   b. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

6. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

Kaspersky Embedded Systems Security exportiert die Liste der Regeln in die XLM-Datei.

Exportieren von Regeln für die Kontrolle des Programmstarts 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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.

5. Klicken Sie im Block **Kontrolle des Programmstarts** auf **Anpassen**.

   Das Fenster **Kontrolle des Programmstarts** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.

6. Wechseln Sie zur Registerkarte **Regeln**, um Regeln für die Kontrolle des Programmstarts zu exportieren, oder zur Registerkarte **Kontrolle der Software-Verteilung**, um Regeln für die Kontrolle der Installationspakete zu exportieren.

7. Aktivieren Sie die Kontrollkästchen der zu exportierenden Regeln.

8. Klicken Sie auf die Schaltfläche **Export**. Dadurch wir ein Fenster geöffnet. Geben Sie in diesem Fenster an, ob Sie nur die ausgewählten Regeln oder alle Regeln exportieren möchten, und klicken Sie dann auf **Export**.

   Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Embedded Systems Security alle Regeln.

Kaspersky Embedded Systems Security exportiert die Liste der Regeln in die XLM-Datei.

Generieren einer txt-Datei mit einer Auswahl von Kaspersky Security Center-Ereignissen über blockierte Programme

Sie können eine Auswahl von Kaspersky Security Center-Ereignissen über blockierte Programme in eine txt-Datei exportieren, diese Daten anschließend importieren und in einer zu konfigurierenden Richtlinie eine Erlaubnisregel-Liste für die Kontrolle des Programmstarts erstellen.

So erstellen Sie eine txt-Datei mit einer Auswahl von Kaspersky Security Center-Ereignissen über blockierte Programme (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Protokolle und Meldungen**.
4. Klicken Sie im Block **Aufgabenprotokolle** auf **Einstellungen**.

   Das Fenster **Meldungen** wird geöffnet.
5. Erweitern Sie den Knoten **Kontrolle der lokalen Aktivität**.
6. Wählen Sie den Abschnitt **Kontrolle des Programmstarts** aus.
7. Aktivieren Sie in der Ereignisliste der Kontrolle des Programmstarts in der Spalte **Ereignisse an Kaspersky Security Center senden** die Kontrollkästchen für *Programmstart verboten* und *Programmstart im Testmodus verboten*.
8. Speichern Sie die vorgenommenen Änderungen.
9. Öffnen Sie die Registerkarte **Konfiguration von Ereignissen** der Richtlinie und vergewissern Sie sich, dass die Speicherdauer für Ereignisse, die im Feld **In der Administrationsserver-Datenbank speichern für (Tage)** angegeben ist, länger als der Zeitraum ist, für den Sie Informationen über verweigerte Programmstarts erfassen möchten (der Standardwert beträgt 30 Tage).

   Sobald die Speicherdauer für Protokolle der Komponente Kontrolle des Programmstarts abläuft, werden die protokollierten Ereignisse gelöscht und erscheinen nicht mehr im Bericht.
10. Aktivieren Sie die Richtlinie, die die Erfassung von Daten über verweigerte Programmstarts festlegt.
11. Ändern Sie bei Bedarf den Betriebsmodus der Komponente Kontrolle des Programmstarts.
12. Nach dem Ende des Zeitraums für das Sammeln von Informationen über verhinderte Programmstarts können Sie Ereignisse aus *Programmstart verboten* und *Programmstart im Testmodus verboten* auswählen und in eine txt-Datei exportieren. Einzelheiten finden Sie im Abschnitt „Ereignisauswahlen“ in der Hilfe zu Kaspersky Security Center.
13. Öffnen Sie die exportierte txt-Datei.
14. Bearbeiten Sie bei Bedarf die Liste der Ereignisse.

So erstellen Sie eine txt-Datei mit einer Auswahl von Kaspersky Security Center-Ereignissen über blockierte Programme (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie den Abschnitt **Protokolle und Meldungen** aus.
5. Klicken Sie im Block **Aufgabenprotokolle** auf **Anpassen**.

   Das Fenster **Aufgabenprotokolle** wird geöffnet.
6. Wählen Sie den Abschnitt **Kontrolle des Programmstarts** aus.
7. Aktivieren Sie in der Ereignisliste der Kontrolle des Programmstarts in der Spalte **Ereignisse an Kaspersky Security Center senden** die Kontrollkästchen für *Programmstart verboten* und *Programmstart im Testmodus verboten*.
8. Speichern Sie die vorgenommenen Änderungen.
9. Öffnen Sie die Registerkarte **Konfiguration von Ereignissen** der Richtlinie, die Sie gerade konfigurieren, und vergewissern Sie sich, dass die Speicherdauer für Ereignisse, die im Feld **In der Administrationsserver-Datenbank speichern für (Tage)** angegeben ist, länger als der Zeitraum ist, für den Sie Informationen über verweigerte Programmstarts erfassen möchten (der Standardwert beträgt 30 Tage).

   Sobald die Speicherdauer für Protokolle der Komponente Kontrolle des Programmstarts abläuft, werden die protokollierten Ereignisse gelöscht und erscheinen nicht mehr im Bericht.
10. Aktivieren Sie die Richtlinie, die die Erfassung von Daten über verweigerte Programmstarts festlegt.
11. Ändern Sie bei Bedarf den Betriebsmodus der Komponente Kontrolle des Programmstarts.
12. Nach dem Ende des Zeitraums für das Sammeln von Informationen über verhinderte Programmstarts können Sie Ereignisse aus *Programmstart verboten* und *Programmstart im Testmodus verboten* auswählen und in eine txt-Datei exportieren. Einzelheiten finden Sie im Abschnitt „Ereignisauswahlen“ in der Hilfe zu Kaspersky Security Center.
13. Öffnen Sie die exportierte txt-Datei.
14. Bearbeiten Sie bei Bedarf die Liste der Ereignisse.

Gruppenaufgabe zum Erstellen von Regeln zur Kontrolle des Programmstarts konfigurieren

So konfigurieren Sie die Gruppenaufgabe Erstellen von Regeln für die Kontrolle des Programmstarts (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Struktur der Kaspersky Security Center-Verwaltungskonsole den Knoten **Verwaltete Geräte**.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Öffnen Sie in der Liste der Gruppenaufgaben die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts*, indem Sie auf den Namen der Aufgabe doppelklicken.

   Das Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.

5. Wechseln Sie zum Abschnitt **Optionen**.

6. Geben Sie bei Bedarf auf der Registerkarte **Regeln** ein Präfix für Regelnamen ein.

7. Geben Sie unter **Gültigkeitsbereich der Erlaubnisregel** die Methode an, die Sie zum Erstellen von Erlaubnisregeln verwenden möchten:

   - **Erlaubnisregeln anhand von gestarteten Programmen erstellen**

   - **Erlaubnisregeln für Programme aus den Ordnern erstellen**

8. Wählen Sie auf der Registerkarte **Einstellungen** das Kriterium aus, das die Aufgabe beim Erstellen von Erlaubnisregeln zur Kontrolle des Programmstarts anwenden soll:

   - **Digitales Zertifikat verwenden**.

     Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts das Vorhandensein eines digitalen Zertifikats als Auslösekriterium für die Regel angegeben. Kaspersky Embedded Systems Security erlaubt Dateien, die über ein digitales Zertifikat verfügen. Diese Option wird empfohlen, wenn Sie den Start beliebiger Programme erlauben möchten, die im Betriebssystem als vertrauenswürdig eingestuft sind. Dieser Status gilt als Standard.

   - **Subjekt und Fingerabdruck für digitales Zertifikat verwenden**

   - **Falls kein Zertifikat vorhanden, verwende Folgendes**

   - **SHA256-Hash verwenden**.

     Wenn diese Option ausgewählt ist, wird in den Einstellungen der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts die Prüfsumme der Datei, auf deren Grundlage die Regel erstellt wird, als Auslösekriterium für die Regel angegeben. Kaspersky Embedded Systems Security erlaubt den Start von Programmen mithilfe von Dateien mit einer bestimmten Prüfsumme. Die Verwendung einer SHA256-Prüfsumme als Auslösekriterium für die Regel beschränkt den Gültigkeitsbereich der Regel auf eine Datei.

9. Konfigurieren Sie die Einstellung **Einen Dateipfad für Regeln hinzufügen, die auf Hash-Summen basieren**.

   Ist dieses Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security beim Export von Regeln die vollständigen Pfade der ausführbaren Dateien zu der xml-Datei hinzu. Anhand der vollständigen Pfade können Sie feststellen, zu welchem Programm eine ausführbare Datei gehört.

   Ist das Kontrollkästchen deaktiviert, enthält die xml-Datei nur die Namen und SHA256-Hashes von ausführbaren Dateien. Das Kontrollkästchen ist standardmäßig deaktiviert.

10. Fügen Sie Benutzer und/oder Benutzergruppen hinzu, die Programme starten dürfen, die den mit der Aufgabe erstellten Regeln entsprechen.

    a. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** die Methode zum Hinzufügen von Benutzern oder Gruppen aus.

    b. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Namen eines Benutzers bzw. einer Benutzergruppe ein oder wählen Sie einen Benutzer bzw. eine Gruppe aus.

    c. Klicken Sie auf **OK**.

    d. Führen Sie die Schritte a bis c für jeden Benutzer oder jede Benutzergruppe aus.

11. Konfigurieren Sie im Block **Nach Abschluss der Aufgabe** die folgenden Einstellungen:

    - **Erlaubnisregeln in die Liste der Regeln zur Kontrolle des Programmstarts aufnehmen**

- Prinzip für das Hinzufügen
- **Erlaubnisregeln in Datei exportieren**.
- Details über geschütztes Gerät zum Dateinamen hinzufügen

12. Geben Sie bei Bedarf auf der Registerkarte **Ausnahmen** die Objekte an, die Sie aus dem Aufgabenbereich ausschließen möchten.

13. Klicken Sie auf **OK** im Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts**.

So konfigurieren Sie die Gruppenaufgabe Erstellen von Regeln für die Kontrolle des Programmstarts (in der Kaspersky Security Center Web Console)

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

2. Öffnen Sie in der Liste der Gruppenaufgaben die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts.

   Das Fenster **Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.

3. Öffnen Sie die Registerkarte **Anwendungseinstellungen**.

4. Geben Sie bei Bedarf im Abschnitt **Gültigkeitsbereich der Erlaubnisregel** ein Präfix für Regelnamen ein.

5. Geben Sie unter **Gültigkeitsbereich der Erlaubnisregel** die Methode an, die Sie zum Erstellen von Erlaubnisregeln verwenden möchten:

   - Erlaubnisregeln anhand von gestarteten Programmen erstellen
   - Erlaubnisregeln für Programmeauf den Ordnern erstellen

6. Wählen Sie auf der Registerkarte **Einstellungen** das Kriterium aus, das die Aufgabe beim Erstellen von Erlaubnisregeln zur Kontrolle des Programmstarts anwenden soll:

   - Digitales Zertifikat verwenden
   - Subjekt und Fingerabdruck des digitalen Zertifikats verwenden
   - Falls kein Zertifikat vorhanden, verwende Folgendes
   - SHA256-Hash verwenden

7. Konfigurieren Sie die Einstellung **Einen Dateipfad für Regeln hinzufügen, die auf Hash-Summen basieren**.

   Ist dieses Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security beim Export von Regeln die vollständigen Pfade der ausführbaren Dateien zu der xml-Datei hinzu. Anhand der vollständigen Pfade können Sie feststellen, zu welchem Programm eine ausführbare Datei gehört.

   Ist das Kontrollkästchen deaktiviert, enthält die xml-Datei nur die Namen und SHA256-Hashes von ausführbaren Dateien. Das Kontrollkästchen ist standardmäßig deaktiviert.

8. Fügen Sie Benutzer und/oder Benutzergruppen hinzu, die Programme starten dürfen, die den mit der Aufgabe erstellten Regeln entsprechen.

   a. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**.

   b. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster den Namen eines Benutzers bzw. einer Benutzergruppe ein oder wählen Sie einen Benutzer bzw. eine Gruppe aus.

   c. Klicken Sie auf **Auswählen**.

   d. Führen Sie die Schritte a bis c für jeden Benutzer oder jede Benutzergruppe aus.

9. Konfigurieren Sie im Block **Nach Abschluss der Aufgabe** die folgenden Einstellungen:

   - **Erlaubnisregeln in die Liste der Regeln zur Kontrolle des Programmstarts aufnehmen**
   - **Prinzip für das Hinzufügen**
   - **Die Erlaubnisregeln werden in eine Datei exportiert**. Im Feld **Geben Sie den vollständigen Pfad zu einer Datei mit der Endung .xml an** können Sie den Pfad einer xml-Datei angeben, in die Kaspersky Embedded Systems Security die Erlaubnisregeln exportieren soll, sobald die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts abgeschlossen wird.
   - **Informationen über das geschützte Gerät zum Dateinamen hinzufügen**

10. Geben Sie bei Bedarf auf der Registerkarte **Ausnahmen** die Objekte an, die Sie aus dem Aufgabenbereich ausschließen möchten.

11. Klicken Sie im Fenster **Erstellen von Regeln für die Kontrolle des Programmstarts** auf **OK**.

Erstellen von Regeln mithilfe einer Gruppenaufgabe des Typs „Erstellen von Regeln zur Kontrolle des Programmstarts“

So erstellen Sie Regeln mithilfe der Gruppenaufgabe Erstellen von Regeln für die Kontrolle des Programmstarts:

1. Erstellen Sie die Gruppenaufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* oder wählen Sie eine vorhandene Aufgabe aus.

2. Konfigurieren Sie die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts.

3. Führen Sie die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts aus.

Gehen Sie nach Abschluss der Aufgabe je nach Aufgabeneinstellungen wie folgt vor:

- Wenn Sie festgelegt haben, dass nach Abschluss der Aufgabe die Aktion **Erlaubnisregeln in die Liste der Regeln zur Kontrolle des Programmstarts aufnehmen** ausgeführt wird, werden die Regeln, die zur Kontrolle des Programmstarts generiert wurden, zur Liste in den Einstellungen der Kontrolle des Programmstarts in der Anwendungskonsole hinzugefügt.

- Wenn Sie festgelegt haben, das nach Abschluss der Aufgabe die Aktion **Die Erlaubnisregeln werden in eine Datei exportiert** ausgeführt wird, werden die Regeln, die zur Kontrolle des Programmstarts generiert wurden, in einer xml-Datei unter dem in den Aufgabeneinstellungen angegebenen Pfad gespeichert.

Die Listen enthalten Erlaubnisregeln für den Start von Programmen, deren Typ den Einstellungen der Gruppenaufgabe „Erstellen von Regeln für die Kontrolle des Programmstarts“ entspricht.

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.

Die Gerätekontrolle bietet die folgende Funktionalität:

- Verwaltung von Benutzerzugriffsrechten für Speichergeräte (z. B. Wechseldatenträger, Mobiltelefone, und CD-/DVD-Laufwerke)
- Kontrolle der Verbindung von Geräten ohne ein Dateisystem (z. B. externe Modems, Bluetooth-Adapter und USB-Tastaturen)
- Verwaltung von WLAN-Verbindungen

Die Gerätekontrolle ist standardmäßig deaktiviert. Wenn Sie die Gerätekontrolle aktivieren, verweigert Kaspersky Embedded Systems Security standardmäßig den Zugriff auf die folgenden Gerätetypen:

- Wechseldatenträger (einschließlich USB-Sticks)
- Disketten
- CD-/DVD-Laufwerke
- Tragbare Geräte (MTP)
- Modems.
- Smartcard-Lesegeräte
- Externe Netzwerkadapter
- Bluetooth (außer Eingabegeräte)

Stufen der Gerätekontrolle

Kaspersky Embedded Systems Security kontrolliert den Gerätezugriff auf folgenden Ebenen:

1. **Gerätetyp**.

   Wenn ein Gerät an den Computer angeschlossen wird, ermittelt das Betriebssystem den Gerätetyp: Drucker, Wechseldatenträger, CD/DVD-Laufwerk usw. Auf dieser Stufe können Sie die Verbindung von Geräten nach Typ erlauben oder verbieten.

2. **Schnittstellen**.

   Eine *Verbindungsschnittstelle* ist eine Schnittstelle, über die Geräte an den Computer angeschlossen werden. Einige Gerätetypen verfügen über mehrere Verbindungsschnittstellen. Beispielsweise können Sie einen Drucker an den USB-Port oder den seriellen Port (COM) anschließen.

Auf dieser Stufe können Sie den Zugriff auf Geräte je nach Verbindungsschnittstelle erlauben oder verbieten.

Nehmen wir beispielsweise an, Sie haben den Zugriff über USB verweigert. Im Modus **Von Verbindungsschnittstelle abhängig** verweigert Kaspersky Embedded Systems Security den Zugriff auf alle Gerätetypen, wenn die Verbindung über USB erfolgt.

> Wenn der Zugriffsmodus **Erlauben** oder **Verbieten** für das Gerät ausgewählt ist, ignoriert die Zugriffskontrolle die Verbindungsschnittstelle des Geräts.

3. **Vertrauenswürdige Geräte**.

   Vertrauenswürdige Geräte sind Geräte, auf die jene Benutzer, die in den Einstellungen eines vertrauenswürdigen Gerätes angegeben sind, jederzeit vollständigen Zugriff besitzen.

Funktionsmodi der Gerätekontrolle

Die Gerätekontrolle bietet die folgenden Modi:

- **Aktiver Modus**.

  Kaspersky Embedded Systems Security verweigert oder erlaubt Geräte und berücksichtigt dazu die konfigurierten Zugriffsregeln für Geräte. Das Programm erlaubt auch den Zugriff auf vertrauenswürdige Geräte. Das Programm protokolliert Ereignisse, bei denen Geräte verbunden oder getrennt werden.

- **Informieren**.

  Kaspersky Embedded Systems Security erlaubt alle Geräte und protokolliert entsprechende Ereignisse. Alle Geräte sind zugelassen. Dieser Modus ist standardmäßig eingestellt. Sie können diesen Modus aktivieren, um ein Audit der Geräte in Ihrem Unternehmen durchzuführen und diese Informationen zum Erstellen einer Liste mit vertrauenswürdigen Geräten verwenden.

Regeln für den Zugriff auf Geräte

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, Lese- oder Schreibberechtigungen sowie andere Optionen. Die Auswahl der Einstellungen für eine Zugriffsregel ist vom Gerätetyp abhängig.

Einstellungen für eine Zugriffsregel

Geräte	Zuweisung von Benutzern / einer Benutzergruppe	Zeitplan für den Zugriff auf ein Gerät	Erlaubnis zum Lesen/Schreiben	Überwachung von Schnittstellen
Festplatten	✓	✓	✓	✓
Wechseldatenträger (einschließlich USB-Sticks)	✓	✓	✓	✓
Disketten	✓	✓	✓	✓
CD-/DVD-Laufwerke	✓	✓	✓	✓
Tragbare Geräte (MTP)	✓	✓	✓	✓
Lokale Drucker	✓	–	–	✓
Netzwerkdrucker	✓	–	–	–

Geräte	Zuweisung von Benutzern / einer Benutzergruppe	Zeitplan für den Zugriff auf ein Gerät	Erlaubnis zum Lesen/Schreiben	Überwachung von Schnittstellen
Modems	–	–	–	✓
Streamer	–	–	–	✓
Multifunktionsgeräte	–	–	–	✓
Smartcard-Lesegeräte	–	–	–	✓
Windows CE USB ActiveSync-Geräte	–	–	–	✓
Externe Netzwerkadapter	–	–	–	✓
Bluetooth	–	–	–	–
Kameras und Scanner	–	–	–	✓
WLAN	–	–	–	–
USB-Tastaturen	–	–	–	✓
USB-Mäuse	–	–	–	✓

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, Lese- oder Schreibberechtigungen sowie andere Optionen. Die Auswahl der Einstellungen für eine Zugriffsregel ist vom Gerätetyp abhängig.

Sie können den Zugriff auf Geräte wie folgt anpassen:

- **Erlauben**.

  Kaspersky Embedded Systems Security gewährt allen Benutzern uneingeschränkten Zugriff auf Geräte.

- **Verbieten**.

  Kaspersky Embedded Systems Security blockiert Verbindungen zu Geräten. Das Programm erlaubt nur Verbindungen mit vertrauenswürdigen Geräten.

- **Von Verbindungsschnittstelle abhängig**.

  Kaspersky Embedded Systems Security identifiziert die Verbindungsschnittstelle des Geräts und überwacht den Zugriff gemäß dem Zugriffsmodus der Verbindungsschnittstelle. Das Programm erlaubt auch Verbindungen mit vertrauenswürdigen Geräten.

- **Nach Regeln**.

  Für einige Gerätetypen können Sie die Benutzer oder eine Benutzergruppe auswählen, die zur Geräteverwendung berechtigt sind, und Sie können einen Zeitplan für den Gerätezugriff konfigurieren sowie Lese- und Schreibberechtigungen festlegen. 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 kontrollieren Sie den Zugriff auf Geräte nach Typ (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.
7. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.
8. Konfigurieren Sie die Regeln für den Zugriff auf mobile Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Verbieten**, **Von Verbindungsschnittstelle abhängig**, **Nach Regeln**.

   Zur Auswahl des Zugriffsmodus **Nach Regeln** müssen Sie doppelklicken, um die Eigenschaften der Zugriffsregeln zu öffnen.

   b. Wenn Sie den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** ausgewählt haben, gehen Sie zur Registerkarte **Verbindungsschnittstellen** und konfigurieren Sie die Zugriffsregeln für Verbindungsschnittstellen.

   c. Für Speichergeräte (z. B. Wechseldatenträger) können Sie Zugriffsrechte für einzelne Benutzer konfigurieren. Sie können einen Zeitplan für den Gerätezugriff konfigurieren sowie Lese- und Schreibberechtigungen festlegen.

   d. Konfigurieren Sie die Druckregeln (falls erforderlich).

   e. Falls erforderlich, konfigurieren Sie die Regeln für WLAN-Verbindungen.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So kontrollieren Sie den Zugriff auf Geräte nach Typ (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Gehen Sie zu **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Blockieren** oder **Informieren** aus.

7. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

8. Konfigurieren Sie die Regeln für den Zugriff auf mobile Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Von Verbindungsschnittstelle abhängig**, **Nach Regeln**.

      Wenn der Zugriffsmodus nicht im Dropdown-Menü verfügbar ist, öffnen Sie die Eigenschaften der Zugriffsregel durch Doppelklick auf den Gerätetyp.

   b. Wenn Sie den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** auswählen, müssen Sie zum Fenster mit den allgemeinen Gerätekontrolle-Einstellungen zurückkehren, auf **Verbindungsschnittstellen** klicken und Zugriffsregeln für Verbindungsschnittstellen konfigurieren.

   c. Für Speichergeräte (z. B. Wechseldatenträger) können Sie Zugriffsrechte für einzelne Benutzer konfigurieren. Sie können einen Zeitplan für den Gerätezugriff konfigurieren sowie Lese- und Schreibberechtigungen festlegen.

   d. Konfigurieren Sie die Druckregeln (falls erforderlich).

   e. Falls erforderlich, konfigurieren Sie die Regeln für WLAN-Verbindungen.

9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So kontrollieren Sie den Zugriff auf Geräte nach Typ (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

6. Konfigurieren Sie die Regeln für den Zugriff auf mobile Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Verbieten**, **Von Verbindungsschnittstelle abhängig**, **Nach Regeln**.

      Zur Auswahl des Zugriffsmodus **Nach Regeln** müssen Sie doppelklicken, um die Eigenschaften der Zugriffsregeln zu öffnen.

   b. Wenn Sie den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** auswählen, müssen Sie auf der Registerkarte **Verbindungsschnittstellen** die Zugriffsregeln für Verbindungsschnittstellen konfigurieren.

   c. Für Speichergeräte (z. B. Wechseldatenträger) können Sie Zugriffsrechte für einzelne Benutzer konfigurieren. Sie können einen Zeitplan für den Gerätezugriff konfigurieren sowie Lese- und Schreibberechtigungen festlegen.

   d. Konfigurieren Sie die Druckregeln (falls erforderlich).

   e. Falls erforderlich, konfigurieren Sie die Regeln für WLAN-Verbindungen.

7. Speichern Sie die vorgenommenen Änderungen.

Wenn ein Benutzer versucht, auf ein Gerät zuzugreifen, blockiert das Programm den Zugriff gemäß den Regeln. Außerdem protokolliert Kaspersky Embedded Systems Security das entsprechende Ereignis. Wenn Sie einzelnen Geräten Zugriff gewähren möchten, können Sie diese Geräte zur Liste der vertrauenswürdigen Geräte hinzufügen.

Kontrolle von WLAN-Verbindungen

Mit der Gerätekontrolle können Sie die WLAN-Verbindung des Computers (Terminals) 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 Embedded Systems Security die Verbindungen zu WLAN-Netzwerken nicht.

So beschränken Sie WLAN-Verbindungen (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

7. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.

8. Konfigurieren Sie eine Zugriffsregel für **WLAN**-Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Verbieten**, **Verbieten mit Ausnahmen**.

   b. Wenn Sie den Modus **Verbieten mit Ausnahmen** ausgewählt haben, müssen Sie eine Liste mit vertrauenswürdigen WLAN-Netzwerken erstellen:

      1. Doppelklicken Sie auf den Gerätetyp **WLAN**, um die Liste der vertrauenswürdigen WLAN-Netzwerke zu öffnen.

      2. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

      3. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster das vertrauenswürdige WLAN-Netzwerk:

         - **Netzwerkname**. Name oder SSID (Service Set Identifier) des WLAN-Netzwerks.
         - **Authentifizierungstyp**. Authentifizierungstyp, der zur Verbindung mit dem WLAN-Netzwerk verwendet wird.
         - **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. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So beschränken Sie WLAN-Verbindungen (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität → Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Blockieren** oder **Informieren** aus.

7. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

8. Doppelklicken Sie auf den Gerätetyp **WLAN**, um die Eigenschaften der Zugriffsregel zu öffnen.

9. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Verbieten mit Ausnahmen**.

10. Wenn Sie den Modus **Verbieten mit Ausnahmen** ausgewählt haben, müssen Sie eine Liste mit vertrauenswürdigen WLAN-Netzwerken erstellen:

    1. Klicken Sie im Block **Vertrauenswürdige WLAN-Netzwerke** auf **Hinzufügen**.

    2. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster das vertrauenswürdige WLAN-Netzwerk:

       - **Netzwerkname**. Name oder SSID (Service Set Identifier) des WLAN-Netzwerks.
       - **Authentifizierungstyp**. Authentifizierungstyp, der zur Verbindung mit dem WLAN-Netzwerk verwendet wird.
       - **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.

11. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So beschränken Sie WLAN-Verbindungen (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle → Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

6. Konfigurieren Sie eine Zugriffsregel für **WLAN**-Geräte:

   a. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Verbieten mit Ausnahmen**.

   b. Wenn Sie den Modus **Verbieten mit Ausnahmen** ausgewählt haben, müssen Sie eine Liste mit vertrauenswürdigen WLAN-Netzwerken erstellen:

      1. Doppelklicken Sie auf den Gerätetyp **WLAN**, um die Liste der vertrauenswürdigen WLAN-Netzwerke zu öffnen.

      2. Klicken Sie im angezeigten Fenster auf **Hinzufügen**.

      3. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster das vertrauenswürdige WLAN-Netzwerk:

         - **Netzwerkname**. Name oder SSID (Service Set Identifier) des WLAN-Netzwerks.
         - **Authentifizierungstyp**. Authentifizierungstyp, der zur Verbindung mit dem WLAN-Netzwerk verwendet wird.
         - **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.

Wenn ein Benutzer versucht, sich mit einem WLAN-Netzwerk zu verbinden, das nicht als vertrauenswürdig gilt, blockiert das Programm die Verbindung.

Druckerüberwachung

Mit der Gerätekontrolle können Sie den Benutzerzugriff auf lokale Drucker und Netzwerkdrucker konfigurieren.

Überwachung lokaler Drucker

Kaspersky Embedded Systems Security kontrolliert lokale Druckerverbindungen über die folgenden Schnittstellen: USB, Serielle Schnittstelle (COM), Paralleler Anschluss (LPT).

> Kaspersky Embedded Systems Security kontrolliert die Verbindung lokaler Drucker mit COM- und LPT-Ports nur auf Schnittstellenebene. Um Verbindungen von Druckern mit COM- und LPT-Ports zu verhindern, wählen Sie für den Gerätetyp **Lokale Drucker** den Modus **Von Verbindungsschnittstelle abhängig** aus und verbieten Sie das Verbinden von Geräten über COM- und LPT-Schnittstellen.

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 Embedded Systems Security gewährt allen Benutzern uneingeschränkten Zugriff auf lokale Drucker. Die Benutzer können Drucker anschließen und mit den vom Betriebssystem bereitgestellten Mitteln Dokumente drucken.
- **Blockieren**. Kaspersky Embedded Systems Security blockiert die Verbindung mit lokalen Druckern. Das Programm erlaubt nur Verbindungen mit vertrauenswürdigen Druckern.
- **Von Verbindungsschnittstelle abhängig**. Kaspersky Embedded Systems Security erlaubt Verbindungen zu lokalen Druckern abhängig vom Status der Verbindungsschnittstelle (**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 Embedded Systems 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 Embedded Systems Security nicht kontrolliert. Das Programm gewährt allen Benutzern Zugriff auf Drucker und speichert im Ereignisprotokoll keine Informationen über Druckvorgänge.
- **Erlauben**. Kaspersky Embedded Systems Security gewährt allen Benutzern Zugriff auf das Drucken auf Netzwerkdruckern.
- **Blockieren**. Kaspersky Embedded Systems Security beschränkt den Zugriff auf Netzwerkdrucker für alle Benutzer. Die App erlaubt nur den Zugriff auf vertrauenswürdige Drucker.
- **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 Netzwerkdruckern erlauben oder verbieten.

Druckerregeln für Drucker hinzufügen

So fügen Sie Druckregeln hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.
7. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.
8. Konfigurieren Sie die Zugriffsregeln für Drucker:

   a. Konfigurieren Sie für die Gerätetypen **Lokale Drucker** und **Netzwerkdrucker** die Zugriffsregeln: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren** (nur für Netzwerkdrucker), **Von Verbindungsschnittstelle abhängig** (nur für lokale Drucker), **Nach Regeln**.

   b. Wenn Sie den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** ausgewählt haben, gehen Sie zur Registerkarte **Verbindungsschnittstellen** und konfigurieren Sie die Zugriffsregeln für Verbindungsschnittstellen.

   c. Wenn Sie den Zugriffsmodus **Nach Regeln** auswählen, müssen Sie Druckregeln konfigurieren:

      1. Doppelklicken Sie auf den Gerätetyp **Lokale Drucker** und **Netzwerkdrucker**, um die Eigenschaften der Zugriffsregel zu öffnen.
      2. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Druckerregel gelten soll. Klicken Sie dazu auf **Hinzufügen**.

         Dadurch wird ein Fenster zum Hinzufügen einer neuen Druckerregel geöffnet.
      3. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

4. Konfigurieren Sie unter **Aktion** den Benutzerzugriff für das Drucken auf dem Drucker.

5. 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.

6. Klicken Sie auf **OK**.

9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So fügen Sie Druckregeln hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität → Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Blockieren** oder **Informieren** aus.

7. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

8. Konfigurieren Sie die Zugriffsregeln für Drucker:

   a. Wählen Sie für die Gerätetypen **Lokale Drucker** and **Netzwerkdrucker** einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren** (nur für Netzwerkdrucker), **Von Verbindungsschnittstelle abhängig** (nur für lokale Drucker), **Nach Regeln**.

   Wenn der Zugriffsmodus nicht im Dropdown-Menü verfügbar ist, öffnen Sie die Eigenschaften der Zugriffsregel durch Doppelklick auf den Gerätetyp.

   b. Wenn Sie den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** auswählen, müssen Sie zum Fenster mit den allgemeinen Einstellungen der Komponente Gerätekontrolle zurückkehren, auf **Verbindungsschnittstellen** klicken und Zugriffsregeln für Verbindungsschnittstellen konfigurieren.

c. Wenn Sie das Drucken konfigurieren möchten:

1. Doppelklicken Sie auf den Gerätetyp **Lokale Drucker** oder **Netzwerkdrucker**, um die Eigenschaften der Zugriffsregel zu öffnen.

2. Wählen Sie den Zugriffsmodus **Nach Regeln** aus.

3. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Druckerregel gelten soll. Klicken Sie dazu auf **Hinzufügen**.

   Dadurch wird ein Fenster zum Hinzufügen einer neuen Druckerregel geöffnet.

4. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

5. Konfigurieren Sie unter **Aktion** den Benutzerzugriff für das Drucken auf dem Drucker.

6. Klicken Sie unter **Benutzer und Gruppen** auf **Hinzufügen** 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.

7. Klicken Sie auf **OK**.

9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So fügen Sie Druckregeln hinzu (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle → Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

6. Konfigurieren Sie die Zugriffsregeln für Drucker:

    a. Konfigurieren Sie für die Gerätetypen **Lokale Drucker** und **Netzwerkdrucker** die Zugriffsregeln: **Erlauben**, **Verbieten**, **Erlauben und nicht protokollieren** (nur für Netzwerkdrucker), **Von Verbindungsschnittstelle abhängig** (nur für lokale Drucker), **Nach Regeln**.

    b. Wenn Sie den Zugriffsmodus **Von Verbindungsschnittstelle abhängig** ausgewählt haben, gehen Sie zur Registerkarte **Verbindungsschnittstellen** und konfigurieren Sie die Zugriffsregeln für Verbindungsschnittstellen.

    c. Wenn Sie den Zugriffsmodus **Nach Regeln** auswählen, müssen Sie Druckregeln konfigurieren:

        1. Doppelklicken Sie auf den Gerätetyp **Lokale Drucker** und **Netzwerkdrucker**, um die Eigenschaften der Zugriffsregel zu öffnen.

        2. Wählen Sie die Benutzer oder Benutzergruppen aus, für die die Druckerregel gelten soll. Klicken Sie dazu auf **Hinzufügen**.

            Dadurch wird ein Fenster zum Hinzufügen einer neuen Druckerregel geöffnet.

        3. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

        4. Konfigurieren Sie unter **Aktion** den Benutzerzugriff für das Drucken auf dem Drucker.

        5. 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.

        6. Klicken Sie auf **OK**.

7. Speichern Sie die vorgenommenen Änderungen.

Kontrolle von Eingabegeräten (HID)

Zu den Eingabegeräten gehören Tastaturen, Mäuse, Trackballs, Touchpads und ähnliche Geräte. Eingabegeräte können über die folgenden Schnittstellen angeschlossen werden: USB, Bluetooth, PS/2-Port, RS-232 (COM)-Port, IR-Port und andere.

Kaspersky Embedded Systems Security ermöglicht die Kontrolle von USB- und Bluetooth-Mäusen und -Tastaturen. Die Gerätekontrolle protokolliert das Anschließen und Trennen von Eingabegeräten.

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 Embedded Systems Security als separates Gerät verwaltet. Aus diesem Grund erstellt das Programm für jedes erkannte Gerät ein Ereignis.

In Kaspersky Embedded Systems Security können Sie die Verwendung eines Eingabegeräts erlauben oder verbieten sowie eine Liste mit vertrauenswürdigen Geräten erstellen.

So aktivieren Sie die Gerätekontrolle (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.
7. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.
8. Wählen Sie für den Gerätetyp **Bluetooth** einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

   Sie können alle Bluetooth-Geräte blockieren oder erlauben oder nur die Verbindung mit Bluetooth-Eingabegeräten (Eingabegeräte (HID)) zulassen.

   Das Anschließen von Eingabegeräten kann nur in der Kaspersky Security Center Web Console erlaubt werden. Es ist nicht möglich, das Anschließen von Eingabegeräten in der Verwaltungskonsole (MMC) oder in der Konsole für Kaspersky Embedded Systems Security zuzulassen.
9. Wählen Sie für die Gerätetypen **USB-Tastaturen** und **USB-Mäuse** einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Von Verbindungsschnittstelle abhängig**.
10. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren Sie die Gerätekontrolle (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Blockieren** oder **Informieren** aus.

7. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

8. Klicken Sie auf den Gerätetyp **Bluetooth**, um die Eigenschaften der Zugriffsregel zu öffnen.

9. Wählen Sie einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

   Sie können alle Bluetooth-Geräte blockieren oder erlauben oder nur die Verbindung mit Bluetooth-Eingabegeräten (Eingabegeräte (HID)) zulassen.

10. Wählen Sie für die Gerätetypen **USB-Tastaturen** und **USB-Mäuse** einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Von Verbindungsschnittstelle abhängig**.

11. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Gerätekontrolle (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

6. Wählen Sie für den Gerätetyp **Bluetooth** einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

   Sie können alle Bluetooth-Geräte blockieren oder erlauben oder nur die Verbindung mit Bluetooth-Eingabegeräten (Eingabegeräte (HID)) zulassen.

   > Das Anschließen von Eingabegeräten kann nur in der Kaspersky Security Center Web Console erlaubt werden. Es ist nicht möglich, das Anschließen von Eingabegeräten in der Verwaltungskonsole (MMC) oder in der Konsole für Kaspersky Embedded Systems Security zuzulassen.

7. Wählen Sie für die Gerätetypen **USB-Tastaturen** und **USB-Mäuse** einen Zugriffsmodus aus: **Erlauben**, **Blockieren**, **Von Verbindungsschnittstelle abhängig**.

8. Speichern Sie die vorgenommenen Änderungen.

Zugriff auf Mobilgeräte verwalten

Mit Kaspersky Embedded Systems 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 iTunes oder ähnliche Programme auf dem Computer Android Debug Bridge installiert sind (weitere Informationen über die ADB-Anwendung finden Sie in der Wissensdatenbank und auf der Website des technischen Supports für Android), erkennt das Betriebssystem Mobilgeräte 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 Embedded Systems 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 Embedded Systems Security gewährt uneingeschränkten Zugriff auf Mobilgeräte. Sie können Dateien auf Mobilgeräten mithilfe des Dateimanagers oder der ADB- und iTunes-Anwendungen 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 Embedded Systems Security schränkt den Zugriff auf Mobilgeräte im Dateimanager und in den ADB- und iTunes-Anwendungen ein. Das Programm 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 Embedded Systems Security erlaubt Verbindungen zu Mobilgeräten abhängig vom Status der USB-Busverbindung (**Erlauben** oder **Blockieren**).

- **Nach Regeln**. Kaspersky Embedded Systems Security beschränkt den Zugriff auf Mobilgeräte gemäß den Regeln. In den Regeln können Sie Zugriffsberechtigungen (Lesen/Schreiben) konfigurieren, Benutzer oder eine Benutzergruppe auswählen, die Zugriff auf Mobilgeräte haben, und einen Zeitplan für den Zugriff auf Mobilgeräte konfigurieren. Sie können den Zugriff auf Daten auf Mobilgeräten 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 Zugriffsregeln für Mobilgeräte (in der Kaspersky Security Center Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
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 **Tragbare Geräte (MTP)** den Zugriffsmodus für Mobilgeräte: **Erlauben**, **Blockieren** oder **Von Verbindungsschnittstelle abhängig**.
7. Um die Zugriffsregeln für Mobilgeräte zu konfigurieren, doppelklicken Sie zum Öffnen der Regelliste.
8. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems 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**.

9. 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.

10. Konfigurieren Sie die Zugriffsberechtigungen der Benutzer auf Mobilgeräte im Dateimanager (**Lesen**/**Schreiben**).

11. 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.

12. Konfigurieren Sie unter **Zugriff über iTunes** den Zugriff auf Daten auf dem Mobilgerät über die iTunes-App.

Kaspersky Embedded Systems Security wendet die Einstellungen für den Zugriff auf Mobilgeräte über die iTunes-App für alle Benutzer an. Für iTunes-Geräte kann kein separater Zugriffszeitplan konfiguriert werden.

13. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Zugriffsregeln für Mobilgeräte (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf den Link **Zugriffsregeln für 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**, **Von Verbindungsschnittstelle abhängig** oder **Nach Regeln**.

8. 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.

9. Wenn Sie den Modus **Nach Regeln** auswählen, müssen Sie Zugriffsregeln für Geräte hinzufügen. Klicken Sie dazu unter **Benutzer** 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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage einer beliebigen vorhandenen Blockierungsregel.

   b. 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.

   c. Konfigurieren Sie unter **Zeitplan für den Zugriff auf Geräte**, 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 Zugriffsregeln für Mobilgeräte (in der Programmkonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

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

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

4. Konfigurieren Sie im Kontextmenü für den Gerätetyp **Tragbare Geräte (MTP)** den Zugriffsmodus für Mobilgeräte: **Erlauben**, **Blockieren** oder **Von Verbindungsschnittstelle abhängig**.

5. Um die Zugriffsregeln für Mobilgeräte zu konfigurieren, doppelklicken Sie zum Öffnen der Regelliste.

6. 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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems 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**.

7. 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.

8. Konfigurieren Sie die Zugriffsberechtigungen der Benutzer auf Mobilgeräte im Dateimanager (**Lesen**/**Schreiben**).

9. 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. Konfigurieren Sie unter **Zugriff über iTunes** den Zugriff auf Daten auf dem Mobilgerät über die iTunes-App.

    Kaspersky Embedded Systems Security wendet die Einstellungen für den Zugriff auf Mobilgeräte über die iTunes-App für alle Benutzer an. Für iTunes-Geräte kann kein separater Zugriffszeitplan konfiguriert werden.

11. 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.

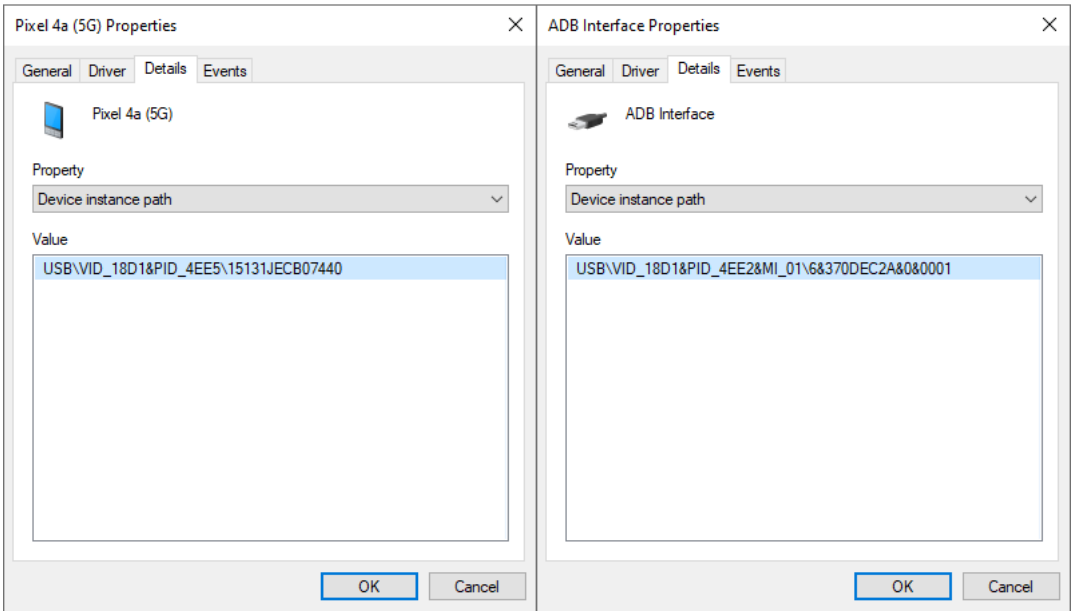
Vertrauenswürdige Mobilgeräte

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 Device 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 heißt, Kaspersky Embedded Systems Security erkennt dieses Gerät als neues Gerät. 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

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 Embedded Systems 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 *Informativ*.

So aktivieren Sie die Überwachung von Dateivorgängen auf Wechseldatenträgern (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

7. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.

8. Wählen Sie den Gerätetyp **Wechseldatenträger** aus und klicken Sie auf **Ereignisprotokollierung**.

   Dadurch wird das Fenster für die Ereignisprotokollierung geöffnet.

9. Aktivieren Sie das Kontrollkästchen **Protokollierung aktivieren**.

10. Markieren Sie im Block **Vorgänge mit Dateien** die Operationen, die Sie überwachen möchten: **Schreiben**, **Löschen**.

11. Wählen Sie im Block **Nach Dateiformaten filtern** die Formate von Dateien aus, deren zugehörige Operationen von der Gerätekontrolle protokolliert werden sollen.

12. Wählen Sie die Benutzer oder Benutzergruppen aus, deren Verwendung von Wechsellaufwerken Sie überwachen möchten.

13. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren Sie die Überwachung von Dateivorgängen auf Wechseldatenträgern (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität → Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Blockieren** oder **Informieren** aus.

7. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

8. Doppelklicken Sie auf den Gerätetyp **Wechseldatenträger**, um die Eigenschaften der Zugriffsregel zu öffnen.

9. Wählen Sie im folgenden Fenster die Registerkarte **Ereignisprotokollierung** aus.

10. Setzen Sie den Schalter **Ereignisprotokollierung AKTIVIERT**.

11. Markieren Sie im Block **Vorgänge mit Dateien** die Operationen, die Sie überwachen möchten: **Schreiben**, **Löschen**.

12. Wählen Sie im Block **Nach Dateiformaten filtern** die Formate von Dateien aus, deren zugehörige Operationen von der Gerätekontrolle protokolliert werden sollen.

13. Wählen Sie die Benutzer oder Benutzergruppen aus, deren Verwendung von Wechsellaufwerken Sie überwachen möchten.

14. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So aktivieren Sie die Überwachung von Dateivorgängen auf Wechseldatenträgern (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

6. Wählen Sie den Gerätetyp **Wechseldatenträger** aus und klicken Sie auf **Ereignisprotokollierung**.

   Dadurch wird das Fenster für die Ereignisprotokollierung geöffnet.

7. Aktivieren Sie das Kontrollkästchen **Protokollierung aktivieren**.

8. Markieren Sie im Block **Vorgänge mit Dateien** die Operationen, die Sie überwachen möchten: **Schreiben**, **Löschen**.

9. Wählen Sie im Block **Nach Dateiformaten filtern** die Formate von Dateien aus, deren zugehörige Operationen von der Gerätekontrolle protokolliert werden sollen.

10. Wählen Sie die Benutzer oder Benutzergruppen aus, deren Verwendung von Wechsellaufwerken Sie überwachen möchten.

11. Speichern Sie die vorgenommenen Änderungen.

Wenn daher Benutzer Dateien speichern, die sich auf Wechseldatenträgern befinden, oder Dateien von Wechseldatenträgern löschen, so speichert Kaspersky Embedded Systems 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-Konsole im Arbeitsbereich für den Knoten **Administrationsserver** auf der Registerkarte **Ereignisse** einsehen. Damit Ereignisse im lokalen Ereignisprotokoll von Kaspersky Embedded Systems Security angezeigt werden, muss das Kontrollkästchen **Dateivorgang ausgeführt** in den Benachrichtigungseinstellungen für die Komponente „Gerätekontrolle“ aktiviert werden.

Zugriff auf Bluetooth-Geräte verwalten

Mit Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems Security schränkt den Zugriff auf Bluetooth-Geräte ein. Sie können festlegen, dass nur die Verbindung von Bluetooth-Eingabegeräten (der Klasse „Human Interface Devices“) zugelassen wird. Zu diesen Geräten gehören z. B. 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.

Das Anschließen von Eingabegeräten kann nur in der Anwendungskonsole oder in der Kaspersky Security Center Web Console erlaubt werden. Es ist nicht möglich, das Anschließen von Eingabegeräten in der Kaspersky Security Center-Verwaltungskonsole zu erlauben.

So konfigurieren Sie Zugriffsregeln für Bluetooth-Geräte (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Kontrolle der lokalen Aktivität → Gerätekontrolle** aus und klicken Sie auf **Einstellungen**.
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 **Bluetooth** den Zugriffsmodus für Bluetooth-Geräte: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

   Wenn Sie den Zugriff auf Bluetooth-Geräte blockiert haben, können Sie die Verbindung von Eingabegeräten (Tastaturen, Mäuse usw.) nur in der Anwendungskonsole oder in der Kaspersky Security Center Web Console zulassen. Es ist nicht möglich, das Anschließen von Eingabegeräten in der Kaspersky Security Center-Verwaltungskonsole zu erlauben.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Zugriffsregeln für Bluetooth-Geräte (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie im Richtlinienfenster den Punkt **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** aus und klicken Sie auf **Einstellungen**.
5. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf den Link **Zugriffsregeln für 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** aus.

   Dadurch werden die Zugriffseinstellungen für Bluetooth-Geräte geöffnet.

7. Konfigurieren Sie den Zugriffsmodus für Bluetooth-Geräte: **Erlauben**, **Verbieten**, **Erlauben und nicht protokollieren**.
8. Wenn Sie den Modus **Verbieten** 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. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Zugriffsregeln für Bluetooth-Geräte (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Gerätekontrolle** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. 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.

4. Konfigurieren Sie unter **Zugriff** den Zugriffsmodus für Bluetooth-Geräte: **Erlauben**, **Blockieren**, **Erlauben und nicht protokollieren**.

5. 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)**.

6. Speichern Sie die vorgenommenen Änderungen.

Unterscheidung der Benutzerzugriffsrechte auf Geräte

Sie können die Benutzerzugriffsrechte nach Gerätetyp oder nach vertrauenswürdigen Geräten konfigurieren.

Differenzierung von Benutzerzugriffsrechten nach Gerätetyp

Die Gerätekontrolle ermöglicht die Konfiguration von Benutzerzugriffsrechten für die Daten auf *Speichergeräten*. Für solche Geräte können Sie Schreib- und Leseberechtigungen konfigurieren. Die Gerätekontrolle unterstützt die folgenden Arten von Speichergeräten:

- Festplatten
- Wechseldatenträger
- Disketten
- CD-/DVD-Laufwerke
- Tragbare Geräte (MTP). Zu den tragbaren Geräten (MTP) gehören beispielsweise mobile Geräte, Fotoapparate und Medienabspielgeräte.

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 Wechseldatenträgern (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.
7. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Die Registerkarte **Gerätetypen** enthält Zugriffsregeln für alle Geräte, die zur Klassifizierung der Gerätekontrolle gehören.

8. Um Zugriffsregeln für Speichergeräte zu konfigurieren, doppelklicken auf die Regelliste.

9. Konfigurieren Sie die Zugriffsregel für Speichergeräte:

   a. Klicken Sie im Block **Zugriffsregeln** auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel für Speichergeräte geöffnet.

   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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems 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**.

10. 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.

11. Konfigurieren Sie die Benutzerberechtigungen für den Zugriff auf Speichergeräte im Dateimanager (**Lesen**/**Schreiben**).

12. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Benutzerzugriffsrechte für Daten auf Speichergeräten (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Blockieren** oder **Informieren** aus.

7. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Zugriffsregeln für Geräte und WLAN-Netzwerke**.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

8. Öffnen Sie im Block **Zugriff auf Massenspeichergeräte** die Eigenschaften der Zugriffsregel für Speichergeräte.

9. Konfigurieren Sie die Zugriffsregel für Speichergeräte:

   a. Klicken Sie im Block **Benutzer** auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel für Speichergeräte geöffnet.

   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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems 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, 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 **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.

   e. Konfigurieren Sie die Benutzerberechtigungen für den Zugriff auf Speichergeräte im Dateimanager (**Lesen**/**Schreiben**).

   f. Klicken Sie auf **OK**.

10. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So konfigurieren Sie die Benutzerzugriffsrechte für Daten auf Speichergeräten (in der Konsole für Kaspersky Embedded Systems Security)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle → Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Punkt **Verbieten** oder **Informieren** aus.

5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Gerätetypen** aus.

   Ein Fenster wird geöffnet. Es enthält Zugriffsregeln für alle Geräte, in der Klassifizierung der Komponente Gerätekontrolle enthalten sind.

6. Um die Zugriffsregeln für Speichergeräte zu konfigurieren, doppelklicken Sie zum Öffnen der Regelliste.

7. Konfigurieren Sie die Zugriffsregel für Speichergeräte:

   a. Klicken Sie im Block **Zugriffsregeln** auf **Hinzufügen**.

      Dadurch wird ein Fenster zum Hinzufügen einer neuen Zugriffsregel für Speichergeräte geöffnet.

   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 Embedded Systems Security den Gerätezugriff auf der Grundlage der Regel mit der höchsten Priorität. Kaspersky Embedded Systems Security erlaubt die Zuweisung einer Priorität zwischen 0 und 10.000. 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 Embedded Systems 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 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**.

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. Speichern Sie die vorgenommenen Änderungen.

Unterscheidung der Benutzerzugriffsrechte 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.

Informationen zum Erstellen von Regeln für die Gerätekontrolle

Sie können mithilfe der Aufgaben und Richtlinien von Kaspersky Security Center gleichzeitig Regeln für die Gerätekontrolle für alle geschützten Geräte und Gruppen geschützter Geräte im Unternehmensnetzwerk erstellen. Um eine Liste mit vertrauenswürdigen Geräten zu erstellen, müssen Sie ein Audit von externen Geräten in Ihrem Unternehmen durchführen.

Um eine Liste mit Regeln auf Grundlage der Liste der Geräte zu erstellen, die mit einem einzelnen geschützten Gerät verbunden sind, können Sie die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* mithilfe der Programmkonsole lokal ausführen.

Sie haben folgende Möglichkeiten, um mit Kaspersky Security Center Regeln für die Gerätekontrolle zu erstellen:

- Mithilfe der Aufgabe *Erstellen von Regeln für die Gerätekontrolle*.

  Je nach Einstellungen kann die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* Informationen über alle Geräte erfassen, die jemals mit dem Computer verbunden waren und zu denen Informationen im Betriebssystem gespeichert sind, oder über Geräte, die beim Start der Aufgabe verbunden sind. Auf Grundlage der erfassten Informationen erstellt die Aufgabe eine Liste mit Erlaubnisregeln für die Komponente Gerätekontrolle. Sie können den automatischen Import der erstellten Regeln in die Liste der Regeln für die Komponente Gerätekontrolle konfigurieren oder die erstellten Regeln manuell importieren.

  Dieses Szenario kann beispielsweise verwendet werden, wenn Sie vor dem ersten Start der Komponente Gerätekontrolle schnell Erlaubnisregeln für vertrauenswürdige Geräte erstellen müssen, die Sie bereits zuvor verwendet haben.

  So führen Sie die Aufgabe Erstellen von Regeln für die Gerätekontrolle aus (in der Kaspersky Security Center-Verwaltungskonsole)

  1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

  2. Wählen Sie in der Konsolenstruktur den Punkt **Aufgaben** aus.

  3. Wählen Sie die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.

     Erstellen Sie bei Bedarf eine neue Aufgabe.

4. Wählen Sie im Abschnitt **Modus** einen Modus für die Aufgabe aus:

   - **Systemdaten über alle bisher verbundenen externen Geräte berücksichtigen**.

     Das Programm ruft Informationen über alle an den Computer angeschlossenen Geräte aus dem Speicher des Betriebssystems ab.

   - **Nur derzeit verbundene externe Geräte berücksichtigen**.

     Das Programm ruft Informationen über die angeschlossenen Geräte ab, wenn die Aufgabe gestartet wird.

5. Geben Sie den Pfad ein, unter dem Sie die Datei mit den Daten speichern möchten.

6. Wenn Sie die Aufgabe auf mehreren Computern ausführen, wird empfohlen, das Kontrollkästchen **Informationen über das geschützte Gerät zum Dateinamen hinzufügen** zu aktivieren.

7. Speichern Sie die vorgenommenen Änderungen.

8. Führen Sie die Aufgabe aus.

So führen Sie die Aufgabe Erstellen von Regeln für die Gerätekontrolle über die Web Console aus

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

   Die Aufgabenliste wird geöffnet.

2. Wählen Sie die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.

   Erstellen Sie bei Bedarf eine neue Aufgabe.

3. Wählen Sie im Abschnitt **Modus** einen Modus für die Aufgabe aus:

   - **Systemdaten für alle externen Geräten berücksichtigen, die jemals angeschlossen waren**.

     Das Programm ruft Informationen über alle an den Computer angeschlossenen Geräte aus dem Speicher des Betriebssystems ab.

   - **Nur momentan angeschlossene externe Geräte berücksichtigen**.

     Das Programm ruft Informationen über die angeschlossenen Geräte ab, wenn die Aufgabe gestartet wird.

4. Geben Sie den Pfad ein, unter dem Sie die Datei mit den Daten speichern möchten.

5. Wenn Sie die Aufgabe auf mehreren Computern ausführen, wird empfohlen, das Kontrollkästchen **Informationen über das geschützte Gerät zum Dateinamen hinzufügen** zu aktivieren.

6. Speichern Sie die vorgenommenen Änderungen.

7. Führen Sie die Aufgabe aus.

So führen Sie die Aufgabe Erstellen von Regeln für die Gerätekontrolle über die Web Console aus

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Automatisches Erstellen von Regeln → Erstellen von Regeln für die Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Erstellen von Regeln für die Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Erstellen von Regeln für die Gerätekontrolle** wird geöffnet.

3. Wählen Sie im Abschnitt **Modus** einen Modus für die Aufgabe aus:

   - **Systemdaten über alle bisher verbundenen externen Geräte berücksichtigen**.

     Das Programm ruft Informationen über alle an den Computer angeschlossenen Geräte aus dem Speicher des Betriebssystems ab.

   - **Nur derzeit verbundene externe Geräte berücksichtigen**.

     Das Programm ruft Informationen über die angeschlossenen Geräte ab, wenn die Aufgabe gestartet wird.

4. Wählen Sie im Abschnitt **Nach Abschluss der Aufgabe** aus, welche Aktionen das Programm nach der Aufgabe ausführen soll:

   - **Erlaubnisregeln zur Liste der Gerätekontrolle-Regeln hinzufügen**. Eine Liste der Gerätekontrolle-Regeln ist in den Einstellungen der Komponente Gerätekontrolle verfügbar.

     Ist das Kontrollkästchen aktiviert, fügt das Programm die von der Aufgabe generierten Regeln zur Liste der Gerätekontrolle-Regeln hinzu. Beim Hinzufügen der Regeln wird das ausgewählte Prinzip berücksichtigt.

     Ist das Kontrollkästchen nicht aktiviert, fügt das Programm die neu erstellten Erlaubnisregeln nicht zur Liste der Gerätekontrolle-Regeln hinzu. Das Programm exportiert Regeln nur in eine Datei.

   - **Prinzip für das Hinzufügen**. Methode, nach der die neu erstellten Erlaubnisregeln zur Liste der Gerätekontrolle-Regeln hinzugefügt werden:

     - **Zu vorhandenen Regeln hinzufügen**. Das Programm fügt eine Regel zur Liste der bestehenden Regeln hinzu. In diesem Fall dupliziert das Programm identische Regeln.

     - **Vorhandene Regeln ersetzen**. Das Programm fügt neue Regeln anstelle vorhandener Regeln hinzu.

     - **Mit vorhandenen Regeln zusammenführen**. Das Programm fügt eine Regel zur Liste der bestehenden Regeln hinzu. In diesem Fall führt das Programm identische Regeln zusammen.

   - **Erlaubnisregeln in Datei exportieren**. Das Programm exportiert Erlaubnisregeln in die Datei, die im Feld unten angegeben ist. Anschließend können Sie die Datei in den Programmeinstellungen auf anderen Computern importieren, um die Erlaubnisregeln zu verteilen. Die Datei kann auch verwendet werden, um ein Backup der Erlaubnisregeln anzulegen.

   - **Details über geschütztes Gerät zum Dateinamen hinzufügen**. Das Programm fügt dem Namen der exportierten Datei nicht nur Datum und Uhrzeit hinzu, sondern auch den Computernamen. Das ist praktisch, wenn Sie Erlaubnisregeln von mehreren Computern sammeln.

5. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security führt ein Audit der externen Geräte durch und speichert die Informationen in der Kaspersky Security Center-Registrierung. Die Liste der externen Geräte ist verfügbar, wenn vertrauenswürdige Geräte hinzugefügt wurden.

Die Aufgabe *Erstellen von Regeln für die Gerätekontrolle* erfasst keine Informationen über Netzwerkdrucker und WLAN-Netzwerke, die mit Geräten verbunden sind. Für Geräte dieser Typen müssen Sie Regeln manuell erstellen.

- Auf Basis des Ereignisberichts, der in Kaspersky Security Center für die Komponente Gerätekontrolle, die im **Informieren**-Modus läuft, generiert wird.

In diesem Szenario blockiert Kaspersky Embedded Systems Security den Zugriff auf Geräte nicht. Wenn die Komponente Gerätekontrolle im Modus **Informieren** ausgeführt wird, erlaubt das Programm die Verwendung aller Geräte und protokolliert Ereignisse beim Anschließen und Trennen externer Geräte.

So aktivieren Sie die Gerätekontrolle im Modus Informieren (in der Kaspersky Security Center Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.
6. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** den Punkt **Informieren** auswählen.
7. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren Sie die Gerätekontrolle im Modus Informieren (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kontrolle der lokalen Aktivität → Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.
5. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle aktivieren**.
6. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** den Punkt **Informieren** auswählen.
7. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So aktivieren Sie die Gerätekontrolle im Modus Informieren (in der Programmkonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle → Gerätekontrolle** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.
3. Aktivieren Sie das Kontrollkästchen **Gerätekontrolle**.

4. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** den Punkt **Informieren** auswählen.

5. Speichern Sie die vorgenommenen Änderungen.

Während die Komponente ausgeführt wird, müssen alle möglichen Szenarien für geschützte Geräte und geschützte Gerätegruppen ausgeführt werden. Anschließend können Sie die Informationen aus dem Ereignisbericht von Kaspersky Security Center in eine TXT-Datei importieren und nach der Überprüfung des Berichts vertrauenswürdige Geräte hinzufügen.

Dieses Szenario wird empfohlen, wenn das Unternehmensnetzwerk eine große Anzahl geschützter Geräte verschiedener Typen mit unterschiedlichen externen Geräten umfasst.

Vertrauenswürdige Geräte hinzufügen

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 1.000 vertrauenswürdige Geräte hinzuzufügen, da dies zu Systeminstabilität führen kann.

So fügen Sie ein vertrauenswürdiges Gerät hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.

4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.

5. Wählen Sie unter **Einstellungen der Geräteüberwachung** die Registerkarte **Vertrauenswürdige Geräte** aus.

   Dies öffnet die Liste der vertrauenswürdigen 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:

   - **Regeln auf Basis verbundenen Geräten erstellen**.
   - **Regeln auf Basis von Systemdaten erstellen**.
   - **Regeln auf Basis der Registrierung von Kaspersky Security Center erstellen**.

   Wenn die Geräteliste leer ist, müssen Sie ein Audit der externen Geräte durchführen. Starten Sie dazu die Aufgabe *Erstellen von Regeln für die Gerätekontrolle*.

   > Geräte des Typs **Disketten** können in Kaspersky Embedded Systems Security nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

8. Klicken Sie auf **Regeln für die ausgewählten Geräte hinzufügen**.
9. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So fügen Sie ein vertrauenswürdiges Gerät hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.
5. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Vertrauenswürdige Geräte**.

   Dies öffnet die Liste der vertrauenswürdigen 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 **Aus KSC-Registrierung**.

   Wenn die Geräteliste leer ist, müssen Sie ein Audit der externen Geräte durchführen. Starten Sie dazu die Aufgabe *Erstellen von Regeln für die Gerätekontrolle*.

Geräte des Typs **Disketten** können in Kaspersky Embedded Systems Security nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.

8. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser.

So fügen Sie ein vertrauenswürdiges Gerät hinzu (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle → Gerätekontrolle** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.
3. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Vertrauenswürdige Geräte** aus.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.
4. Klicken Sie auf **Hinzufügen** und wählen Sie die Methode aus, mit der das Gerät zur Liste der vertrauenswürdigen Geräte hinzugefügt werden soll:

   - **Regeln auf Basis verbundenen Geräten erstellen**.
   - **Regeln auf Basis von Systemdaten erstellen**.
   - **Regeln auf Basis der Registrierung von Kaspersky Security Center erstellen**.

   Wenn die Geräteliste leer ist, müssen Sie ein Audit der externen Geräte durchführen. Starten Sie dazu die Aufgabe *Erstellen von Regeln für die Gerätekontrolle*.

   Geräte des Typs **Disketten** können in Kaspersky Embedded Systems Security nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden.
5. Klicken Sie auf **Regeln für die ausgewählten Geräte hinzufügen**.
6. Speichern Sie die vorgenommenen Änderungen.

Liste mit vertrauenswürdigen Geräten exportieren und importieren

Um die Liste der vertrauenswürdigen Geräte an andere Computer des Unternehmens zu verteilen, können Sie die Liste exportieren bzw. importieren. Sie können die Liste der vertrauenswürdigen Geräte in eine xml-Datei exportieren. Dann können Sie die Datei ändern, um z. B. eine große Anzahl von Geräten desselben Typs hinzuzufügen. Mit der Export-/Importfunktion können Sie ein Backup für die Liste der Regeln der vertrauenswürdigen Geräte anlegen oder die Liste auf einen anderen Server migrieren.

Kaspersky Embedded Systems Security ermöglicht den Import der Liste der vertrauenswürdigen Geräte aus Kaspersky Endpoint Security für Windows. Das Format der xml-Dateien für diese Programme ist identisch.

So exportieren und importieren Sie eine Liste der vertrauenswürdigen Geräte (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Kontrolle der lokalen Aktivität** aus.
4. Klicken Sie im Abschnitt **Gerätekontrolle** auf **Einstellungen**.
5. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Vertrauenswürdige Geräte** aus.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.
6. Um die Liste der vertrauenswürdigen Geräte zu exportieren, gehen Sie wie folgt vor:

   a. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

   b. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

      1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.
      2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

      Kaspersky Embedded Systems Security exportiert die Liste der vertrauenswürdigen Geräte in die XML-Datei.
7. Um die Liste der vertrauenswürdigen Geräte zu importieren, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen → Regeln aus XML-Datei importieren** und wählen Sie einen Importmodus aus: Hinzufügen oder Ersetzen.

      Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der vertrauenswürdigen Geräte importieren möchten.

      Im Zusammenführen-Modus überprüft das Programm die Listen der vertrauenswürdigen Geräte und entfernt doppelte Einträge. Im Hinzufügen-Modus fügt das Programm Einträge zur Liste der vertrauenswürdigen Programme hinzu, ohne auf Duplikate zu prüfen.

   b. Öffnen Sie die Datei.

      Kaspersky Embedded Systems Security importiert vertrauenswürdige Geräte im ausgewählten Modus.
8. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So exportieren und importieren Sie eine Liste der vertrauenswürdigen Geräte (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Kontrolle der lokalen Aktivität** → **Gerätekontrolle** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Gerätekontrolle** wird geöffnet.

5. Klicken Sie im Block **Einstellungen der Gerätekontrolle** auf **Vertrauenswürdige Geräte**.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.

6. 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 die Schaltfläche **Export** und wählen Sie den Exportmodus aus: die gesamte Liste der vertrauenswürdigen Geräte oder nur ausgewählte vertrauenswürdige Geräte exportieren.

   c. Speichern Sie die Datei.

      Kaspersky Embedded Systems Security exportiert die Liste der Adressen von Webressourcen in eine XML-Datei.

7. Um die Liste der vertrauenswürdigen Geräte zu importieren, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Import** und wählen Sie einen Importmodus aus: Hinzufügen oder Ersetzen.

   b. Wählen Sie in dem sich öffnenden Fenster die XML-Datei aus, aus der Sie die Liste der Webressourcen importieren möchten.

   c. Öffnen Sie die Datei.

      Kaspersky Embedded Systems Security importiert vertrauenswürdige Geräte im ausgewählten Modus.

8. Speichern Sie die vorgenommenen Änderungen. Um die Richtlinie auf Computern anzuwenden, schließen Sie die Vorhängeschlösser .

So exportieren und importieren Sie eine Liste der vertrauenswürdigen Geräte (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Gerätekontrolle** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Gerätekontrolle** wird geöffnet.

3. Wählen Sie unter **Einstellungen der Gerätekontrolle** die Registerkarte **Vertrauenswürdige Geräte** aus.

   Dies öffnet die Liste der vertrauenswürdigen Geräte.

4. Um die Liste der vertrauenswürdigen Geräte zu exportieren, gehen Sie wie folgt vor:

   a. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

   b. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

      1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

      2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

      Kaspersky Embedded Systems Security exportiert die Liste der vertrauenswürdigen Geräte in die XML-Datei.

5. Um die Liste der vertrauenswürdigen Geräte zu importieren, gehen Sie wie folgt vor:

   a. Klicken Sie auf **Hinzufügen → Regeln aus XML-Datei importieren** und wählen Sie einen Importmodus aus: Hinzufügen oder Ersetzen.

      Wählen Sie in dem sich öffnenden Fenster die XML-Datei aus, aus der Sie die Liste der Webressourcen importieren möchten.

      Im Zusammenführen-Modus überprüft das Programm die Listen der vertrauenswürdigen Geräte und entfernt doppelte Einträge. Im Hinzufügen-Modus fügt das Programm Einträge zur Liste der vertrauenswürdigen Programme hinzu, ohne auf Duplikate zu prüfen.

   b. Öffnen Sie die Datei.

      Kaspersky Embedded Systems Security importiert vertrauenswürdige Geräte im ausgewählten Modus.

6. Speichern Sie die vorgenommenen Änderungen.

Firewall

Die Firewall-Komponente kann in den folgenden Modi ausgeführt werden:

- **Status der Windows-Firewall überwachen**. Dieser Modus dient einem reibungslosen Übergang von der Logik der Aufgabe zur Firewall-Verwaltung in der Programmversion 3.4 und älter zur vollwertigen Firewall in der Programmversion 4.0 und höher. Bei einem Upgrade von der Programmversion 3.4 und älter bleiben die Regeln der Aufgabe zur Firewall-Verwaltung, die in die Windows-Firewall integriert ist, beibehalten. Die Firewall-Komponente interagiert jedoch nicht mehr mit der Windows-Firewall, sondern überwacht nur die Datenverkehrsfilterung der Windows-Firewall und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Anschließend können Sie Firewall-Regeln erstellen und/oder Windows-Firewall-Regeln importieren und den Firewall-Betriebsmodus in **Informieren** ändern.

- **Informieren**. Das Programm überwacht nur die Ausführung der Firewall-Regeln und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Dieser Modus ist zum Testen der Firewall-Regeln vorgesehen. Sie können die Anwendbarkeit der Regeln anhand des Firewall-Protokolls bewerten. Anschließend können Sie bei Bedarf die Firewall-Regeln anpassen und den Firewall-Betriebsmodus in **Blockieren** ändern.

- **Blockieren**. Das Programm filtert den Netzwerkverkehr gemäß den Einstellungen der Komponente und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf.

Über Firewall-Regeln

Wenn der Modus **Blockieren** ausgewählt ist, filtert die Firewall-Komponente den Netzwerkverkehr anhand von Firewall-Regeln.

Firewall-Regeln für Programme kontrollieren Netzwerkverbindungen für bestimmte Programme. Das Auslösekriterium für diese Regeln basiert auf dem Pfad zu einer ausführbaren Anwendungsdatei.

Die Portregeln der Firewall kontrollieren Netzwerkverbindungen für die angegebenen Ports und Protokolle (TCP / UDP). Als Auslösekriterien für solche Regeln dienen der Protokolltyp und der Port bzw. Portbereich.

Die Regeln für Ports sind mit einem größeren Gültigkeitsbereich verbunden als die Regeln für Apps. Wenn Sie Netzwerkverbindungen auf der Grundlage von Portregeln zulassen, senken Sie die Sicherheitsstufe des geschützten Computers.

Firewall konfigurieren

Dieser Abschnitt enthält Anweisungen zum Konfigurieren von allgemeinen Einstellungen der Firewall-Komponente und zum Erstellen und Konfigurieren von Firewall-Regeln.

Allgemeine Firewall-Einstellungen konfigurieren

Allgemeine Einstellungen der Firewall-Komponente konfigurieren (in der Kaspersky Security Center-Verwaltungskonsole)

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. Klicken Sie im Abschnitt **Kontrolle der Netzwerkaktivität** im Unterabschnitt **Firewall** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Firewall** wird geöffnet.

4. Wählen Sie auf der Registerkarte **Allgemein** im Block **Funktionsmodus für Sperr-Regeln** den Betriebsmodus der Komponente aus:

   - **Status der Windows-Firewall überwachen**. Dieser Modus dient einem reibungslosen Übergang von der Logik der Aufgabe zur Firewall-Verwaltung in der Programmversion 3.4 und älter zur vollwertigen Firewall in der Programmversion 4.0 und höher. Bei einem Upgrade von der Programmversion 3.4 und älter bleiben die Regeln der Aufgabe zur Firewall-Verwaltung, die in die Windows-Firewall integriert ist, beibehalten. Die Firewall-Komponente interagiert jedoch nicht mehr mit der Windows-Firewall, sondern überwacht nur die Datenverkehrsfilterung der Windows-Firewall und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Anschließend können Sie Firewall-Regeln erstellen und/oder Windows-Firewall-Regeln importieren und den Firewall-Betriebsmodus in **Informieren** ändern.

   - **Informieren**. Das Programm überwacht nur die Ausführung der Firewall-Regeln und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Dieser Modus ist zum Testen der Firewall-Regeln vorgesehen. Sie können die Anwendbarkeit der Regeln anhand des Firewall-Protokolls bewerten. Anschließend können Sie bei Bedarf die Firewall-Regeln anpassen und den Firewall-Betriebsmodus in **Blockieren** ändern.

   - **Blockieren**. Das Programm filtert den Netzwerkverkehr gemäß den Einstellungen der Komponente und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf.

5. Passen Sie im Block **Eingehende Verbindungen** die Einstellungen für eingehende Netzwerkverbindungen an:

   - Geben Sie in der Dropdown-Liste **Aktion für eingehende Verbindungen** an, welche Aktion das Programm für alle eingehenden Netzwerkverbindungen ausführen soll, sofern in den Firewall-Regeln für eingehende Verbindungen nichts anderes festgelegt ist.

   - Fügen Sie bei Bedarf Firewall-Regeln für eingehende Verbindungen hinzu.

     Firewall-Regeln für eingehende Verbindungen haben die Rolle von Ausnahmen. Wenn Sie beispielsweise eine Erlaubnisregel für eingehende Netzwerkverbindungen konfigurieren und in der Dropdown-Liste **Blockieren** die Option **Aktion für eingehende Verbindungen** auswählen, lässt das Programm eingehende Netzwerkverbindungen zu, die den Regelkriterien entsprechen.

6. Passen Sie im Block **Ausgehende Verbindungen** die Einstellungen für ausgehende Netzwerkverbindungen an:

   - Legen Sie in der Dropdown-Liste **Aktion für ausgehende Verbindungen** fest, welche Aktion das Programm für alle ausgehenden Netzwerkverbindungen ausführen soll, sofern in den Firewall-Regeln für ausgehende Verbindungen nichts anderes festgelegt ist.

   - Fügen Sie bei Bedarf Firewall-Regeln für ausgehende Verbindungen hinzu.

     Firewall-Regeln für ausgehende Verbindungen haben die Rolle von Ausnahmen. Wenn Sie beispielsweise eine Verbotsregel für ausgehende Netzwerkverbindungen konfigurieren und in der Dropdown-Liste **Aktion für ausgehende Verbindungen** die Option **Erlauben** auswählen, blockiert das Programm ausgehende Netzwerkverbindungen, die den Regelkriterien entsprechen.

7. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen. Datum und Uhrzeit der Änderung der Einstellungen werden im System-Überwachungsprotokoll gespeichert.

Allgemeine Einstellungen der Firewall-Komponente konfigurieren (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Klicken Sie im Abschnitt **Kontrolle der Netzwerkaktivität** im Unterabschnitt **Firewall** auf die Schaltfläche **Anpassen**.

   Das Fenster **Firewall** wird geöffnet.

5. Setzen Sie den Schalter **Firewall AKTIVIERT**.

6. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Betriebsmodus der Komponente:

   - **Status der Windows-Firewall überwachen**. Dieser Modus dient einem reibungslosen Übergang von der Logik der Aufgabe zur Firewall-Verwaltung in der Programmversion 3.4 und älter zur vollwertigen Firewall in der Programmversion 4.0 und höher. Bei einem Upgrade von der Programmversion 3.4 und älter bleiben die Regeln der Aufgabe zur Firewall-Verwaltung, die in die Windows-Firewall integriert ist, beibehalten. Die Firewall-Komponente interagiert jedoch nicht mehr mit der Windows-Firewall, sondern überwacht nur die Datenverkehrsfilterung der Windows-Firewall und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Anschließend können Sie Firewall-Regeln erstellen und/oder Windows-Firewall-Regeln importieren und den Firewall-Betriebsmodus in **Informieren** ändern.

   - **Informieren**. Das Programm überwacht nur die Ausführung der Firewall-Regeln und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Dieser Modus ist zum Testen der Firewall-Regeln vorgesehen. Sie können die Anwendbarkeit der Regeln anhand des Firewall-Protokolls bewerten. Anschließend können Sie bei Bedarf die Firewall-Regeln anpassen und den Firewall-Betriebsmodus in **Blockieren** ändern.

   - **Blockieren**. Das Programm filtert den Netzwerkverkehr gemäß den Einstellungen der Komponente und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf.

7. Passen Sie im Block **Eingehende Verbindungen** die Einstellungen für eingehende Netzwerkverbindungen an:

   - Geben Sie in der Dropdown-Liste **Aktion für eingehende Verbindungen** an, welche Aktion das Programm für alle eingehenden Netzwerkverbindungen ausführen soll, sofern in den Firewall-Regeln für eingehende Verbindungen nichts anderes festgelegt ist.

   - Fügen Sie bei Bedarf Firewall-Regeln für eingehende Verbindungen hinzu.

     Firewall-Regeln für eingehende Verbindungen haben die Rolle von Ausnahmen. Wenn Sie beispielsweise eine Erlaubnisregel für eingehende Netzwerkverbindungen konfigurieren und in der Dropdown-Liste **Blockieren** die Option **Aktion für eingehende Verbindungen** auswählen, lässt das Programm eingehende Netzwerkverbindungen zu, die den Regelkriterien entsprechen.

8. Passen Sie im Block **Ausgehende Verbindungen** die Einstellungen für ausgehende Netzwerkverbindungen an:

   - Legen Sie in der Dropdown-Liste **Aktion für ausgehende Verbindungen** fest, welche Aktion das Programm für alle ausgehenden Netzwerkverbindungen ausführen soll, sofern in den Firewall-Regeln für ausgehende Verbindungen nichts anderes festgelegt ist.

   - Fügen Sie bei Bedarf Firewall-Regeln für ausgehende Verbindungen hinzu.

     Firewall-Regeln für ausgehende Verbindungen haben die Rolle von Ausnahmen. Wenn Sie beispielsweise eine Verbotsregel für ausgehende Netzwerkverbindungen konfigurieren und in der Dropdown-Liste **Aktion für ausgehende Verbindungen** die Option **Erlauben** auswählen, blockiert das Programm ausgehende Netzwerkverbindungen, die den Regelkriterien entsprechen.

9. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen. Datum und Uhrzeit der Änderung der Einstellungen werden im System-Überwachungsprotokoll gespeichert.

Allgemeine Einstellungen der Firewall-Komponente konfigurieren (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Firewall** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Firewall** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Firewall** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Firewall**.

4. Wählen Sie im Block **Funktionsmodus für Sperr-Regeln** den Betriebsmodus der Komponente:

   - **Status der Windows-Firewall überwachen**. Dieser Modus dient einem reibungslosen Übergang von der Logik der Aufgabe zur Firewall-Verwaltung in der Programmversion 3.4 und älter zur vollwertigen Firewall in der Programmversion 4.0 und höher. Bei einem Upgrade von der Programmversion 3.4 und älter bleiben die Regeln der Aufgabe zur Firewall-Verwaltung, die in die Windows-Firewall integriert ist, beibehalten. Die Firewall-Komponente interagiert jedoch nicht mehr mit der Windows-Firewall, sondern überwacht nur die Datenverkehrsfilterung der Windows-Firewall und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Anschließend können Sie Firewall-Regeln erstellen und/oder Windows-Firewall-Regeln importieren und den Firewall-Betriebsmodus in **Informieren** ändern.

   - **Informieren**. Das Programm überwacht nur die Ausführung der Firewall-Regeln und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf. Dieser Modus ist zum Testen der Firewall-Regeln vorgesehen. Sie können die Anwendbarkeit der Regeln anhand des Firewall-Protokolls bewerten. Anschließend können Sie bei Bedarf die Firewall-Regeln anpassen und den Firewall-Betriebsmodus in **Blockieren** ändern.

   - **Blockieren**. Das Programm filtert den Netzwerkverkehr gemäß den Einstellungen der Komponente und zeichnet die entsprechenden Ereignisse im Komponentenprotokoll auf.

5. Passen Sie im Block **Eingehende Verbindungen** die Einstellungen für eingehende Netzwerkverbindungen an:

   - Geben Sie in der Dropdown-Liste **Aktion für eingehende Verbindungen** an, welche Aktion das Programm für alle eingehenden Netzwerkverbindungen ausführen soll, sofern in den Firewall-Regeln für eingehende Verbindungen nichts anderes festgelegt ist.

   - Fügen Sie bei Bedarf Firewall-Regeln für eingehende Verbindungen hinzu.

     Firewall-Regeln für eingehende Verbindungen haben die Rolle von Ausnahmen. Wenn Sie beispielsweise eine Erlaubnisregel für eingehende Netzwerkverbindungen konfigurieren und in der Dropdown-Liste **Blockieren** die Option **Aktion für eingehende Verbindungen** auswählen, lässt das Programm eingehende Netzwerkverbindungen zu, die den Regelkriterien entsprechen.

6. Passen Sie im Block **Ausgehende Verbindungen** die Einstellungen für ausgehende Netzwerkverbindungen an:

   - Legen Sie in der Dropdown-Liste **Aktion für ausgehende Verbindungen** fest, welche Aktion das Programm für alle ausgehenden Netzwerkverbindungen ausführen soll, sofern in den Firewall-Regeln für ausgehende Verbindungen nichts anderes festgelegt ist.

   - Fügen Sie bei Bedarf Firewall-Regeln für ausgehende Verbindungen hinzu.

     Firewall-Regeln für ausgehende Verbindungen haben die Rolle von Ausnahmen. Wenn Sie beispielsweise eine Verbotsregel für ausgehende Netzwerkverbindungen konfigurieren und in der Dropdown-Liste **Aktion für ausgehende Verbindungen** die Option **Erlauben** auswählen, blockiert das Programm ausgehende Netzwerkverbindungen, die den Regelkriterien entsprechen.

7. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen. Datum und Uhrzeit der Änderung der Einstellungen werden im System-Überwachungsprotokoll gespeichert.

Firewall-Regeln erstellen und konfigurieren

Firewall-Regeln erstellen und konfigurieren (in der Kaspersky Security Center-Verwaltungskonsole)

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. Klicken Sie im Abschnitt **Kontrolle der Netzwerkaktivität** im Unterabschnitt **Firewall** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Firewall** wird geöffnet.
4. Klicken Sie im Block **Eingehende Verbindungen** auf **Regelliste**.

   Das Fenster **Regeln für eingehende Verbindungen** wird geöffnet.
5. **Erstellen und konfigurieren Sie Firewall-Regeln für eingehende Verbindungen**.

   1. Klicken Sie auf der Registerkarte **Programme** auf **Hinzufügen**.

      Das Fenster **Regel für eine Anwendung** wird geöffnet.
   2. Konfigurieren Sie die Regeleinstellungen:

      a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

      > Der Name der Regel darf unabhängig von der Groß-/Kleinschreibung nicht mit den folgenden reservierten Namen übereinstimmen: "Alle", "ICMPv4" und "ICMPv6". Der Name muss in der Liste aller Regeln für eingehende Netzwerkverbindungen eindeutig sein.

      b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm eingehende Netzwerkverbindungen für das Programm.
      - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm eingehende Netzwerkverbindungen für das Programm.

      c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

      d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

      e. Geben Sie im Feld **Programmpfad** manuell oder mithilfe der Schaltfläche **Durchsuchen** den Pfad zur ausführbaren Datei des Programms an, für das Sie die Regel konfigurieren.

      f. Geben Sie im Feld **Dienstname** bei Bedarf den Namen des Dienstes an, auf den die Regel angewendet werden soll.

g. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht eingehende Verbindungen von den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

> Für IP-Adressen wird nur das IPv4-Format unterstützt.

h. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

i. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

3. Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen**.

   Das Fenster **Regel für Ports** wird geöffnet.

4. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

   - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm eingehende Netzwerkverbindungen für die Ports.
   - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm eingehende Netzwerkverbindungen für die Ports.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

   e. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht eingehende Verbindungen von den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

   > Für IP-Adressen wird nur das IPv4-Format unterstützt.

   f. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

   g. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

5. Klicken Sie im Fenster **Regeln für eingehende Verbindungen** auf **OK**.

6. Klicken Sie im Block **Ausgehende Verbindungen** auf **Regelliste**.

   Das Fenster **Regeln für ausgehende Verbindungen** wird geöffnet.

7. **Erstellen und konfigurieren Sie Firewall-Regeln für ausgehende Verbindungen**.

   1. Klicken Sie auf der Registerkarte **Programme** auf **Hinzufügen**.

      Das Fenster **Regel für eine Anwendung** wird geöffnet.

2. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

      Der Name der Regel darf unabhängig von der Groß-/Kleinschreibung nicht mit den folgenden reservierten Namen übereinstimmen: "Alle", "ICMPv4" und "ICMPv6". Der Name muss in der Liste aller Regeln für ausgehende Netzwerkverbindungen eindeutig sein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm ausgehende Netzwerkverbindungen für das Programm.
      - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm ausgehende Netzwerkverbindungen für das Programm.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

   e. Geben Sie im Feld **Programmpfad** manuell oder mithilfe der Schaltfläche **Durchsuchen** den Pfad zur ausführbaren Datei des Programms an, für das Sie die Regel konfigurieren.

   f. Geben Sie im Feld **Dienstname** bei Bedarf den Namen des Dienstes an, auf den die Regel angewendet werden soll.

   g. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht ausgehende Verbindungen zu den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

      Für IP-Adressen wird nur das IPv4-Format unterstützt.

   h. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

   i. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

3. Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen**.

   Das Fenster **Regel für Ports** wird geöffnet.

4. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm ausgehende Netzwerkverbindungen für die Ports.
      - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm ausgehende Netzwerkverbindungen für die Ports.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

e. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht ausgehende Verbindungen zu den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

> Für IP-Adressen wird nur das IPv4-Format unterstützt.

f. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

g. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

5. Klicken Sie im Fenster **Regeln für ausgehende Verbindungen** auf **OK**.

8. Wenn Sie benutzerdefinierte Regeln aus einer xml-Datei importieren oder exportieren möchten, verwenden Sie die Schaltflächen **Import** oder **Export** im Block **Import und Export von Regeln**.

9. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen. Datum und Uhrzeit der Änderung der Einstellungen werden im System-Überwachungsprotokoll gespeichert.

Firewall-Regeln erstellen und konfigurieren (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Klicken Sie im Abschnitt **Kontrolle der Netzwerkaktivität** im Unterabschnitt **Firewall** auf die Schaltfläche **Anpassen**.

   Das Fenster **Firewall** wird geöffnet.

5. Setzen Sie den Schalter **Firewall AKTIVIERT**.

6. Klicken Sie im Block **Eingehende Verbindungen** auf **Anpassen**.

   Das Fenster **Regeln für eingehende Verbindungen** wird geöffnet.

7. **Erstellen und konfigurieren Sie Firewall-Regeln für eingehende Verbindungen**.

   1. Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen**.

      Das Fenster **Regel für Ports** wird geöffnet.

2. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm eingehende Netzwerkverbindungen für die Ports.
      - **Verweigern**. Wenn diese Option ausgewählt ist, blockiert das Programm eingehende Netzwerkverbindungen für die Ports.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Lokale Ports** und **Remote-Ports** einen Port oder Portbereich an.

   e. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht eingehende Verbindungen an die angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

      Für IP-Adressen wird nur das IPv4-Format unterstützt.

   f. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

   g. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

3. Klicken Sie auf der Registerkarte **Programme** auf **Hinzufügen**.

   Das Fenster **Regel für Programme** wird geöffnet.

4. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

      Der Name der Regel darf unabhängig von der Groß-/Kleinschreibung nicht mit den folgenden reservierten Namen übereinstimmen: "Alle", "ICMPv4" und "ICMPv6". Der Name muss in der Liste aller Regeln für eingehende Netzwerkverbindungen eindeutig sein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm eingehende Netzwerkverbindungen für das Programm.
      - **Verweigern**. Wenn diese Option ausgewählt ist, blockiert das Programm eingehende Netzwerkverbindungen für das Programm.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Lokale Ports** und **Remote-Ports** einen Port oder Portbereich an.

   e. Im Feld **Programmpfad** manuell Geben Sie den Pfad zur ausführbaren Datei des Programms an, für das Sie die Regel konfigurieren.

f. Geben Sie im Feld **Dienstname** bei Bedarf den Namen des Dienstes an, auf den die Regel angewendet werden soll.

g. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht eingehende Verbindungen von den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

> Für IP-Adressen wird nur das IPv4-Format unterstützt.

h. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

i. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

5. Klicken Sie im Fenster **Regeln für eingehende Verbindungen** auf **OK**.

8. Klicken Sie im Block **Ausgehende Verbindungen** auf **Anpassen**.

   Das Fenster **Regeln für ausgehende Verbindungen** wird geöffnet.

9. **Erstellen und konfigurieren Sie Firewall-Regeln für ausgehende Verbindungen**.

   1. Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen**.

      Das Fenster **Regel für Ports** wird geöffnet.

   2. Konfigurieren Sie die Regeleinstellungen:

      a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

      b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm ausgehende Netzwerkverbindungen für die Ports.
      - **Verweigern**. Wenn diese Option ausgewählt ist, blockiert das Programm ausgehende Netzwerkverbindungen für die Ports.

      c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

      d. Geben Sie in den Blöcken **Lokale Ports** und **Remote-Ports** einen Port oder Portbereich an.

      e. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht ausgehende Verbindungen zu den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

      > Für IP-Adressen wird nur das IPv4-Format unterstützt.

      f. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

      g. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

   3. Klicken Sie auf der Registerkarte **Programme** auf **Hinzufügen**.

      Das Fenster **Regel für Programme** wird geöffnet.

4. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   > Der Name der Regel darf unabhängig von der Groß-/Kleinschreibung nicht mit den folgenden reservierten Namen übereinstimmen: "Alle", "ICMPv4" und "ICMPv6". Der Name muss in der Liste aller Regeln für ausgehende Netzwerkverbindungen eindeutig sein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

   - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm ausgehende Netzwerkverbindungen für das Programm.
   - **Verweigern**. Wenn diese Option ausgewählt ist, blockiert das Programm ausgehende Netzwerkverbindungen für das Programm.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Lokale Ports** und **Remote-Ports** einen Port oder Portbereich an.

   e. Im Feld **Programmpfad** manuell Geben Sie den Pfad zur ausführbaren Datei des Programms an, für das Sie die Regel konfigurieren.

   f. Geben Sie im Feld **Dienstname** bei Bedarf den Namen des Dienstes an, auf den die Regel angewendet werden soll.

   g. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht ausgehende Verbindungen zu den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

   > Für IP-Adressen wird nur das IPv4-Format unterstützt.

   h. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

   i. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

5. Klicken Sie im Fenster **Regeln für ausgehende Verbindungen** auf **OK**.

10. Wenn Sie benutzerdefinierte Regeln aus einer xml-Datei importieren oder exportieren möchten, verwenden Sie die Schaltflächen **Import von Regeln** oder **Export von Regeln** im Block **Import und Export von Regeln**.

11. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen. Datum und Uhrzeit der Änderung der Einstellungen werden im System-Überwachungsprotokoll gespeichert.

Firewall-Regeln erstellen und konfigurieren (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Firewall** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Firewall** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Firewall** wird geöffnet.

3. Klicken Sie im Block **Eingehende Verbindungen** auf **Regelliste**.

   Das Fenster **Regeln für eingehende Verbindungen** wird geöffnet.

4. **Erstellen und konfigurieren Sie Firewall-Regeln für eingehende Verbindungen**.

   1. Klicken Sie auf der Registerkarte **Programme** auf **Hinzufügen**.

      Das Fenster **Regel für eine Anwendung** wird geöffnet.

   2. Konfigurieren Sie die Regeleinstellungen:

      a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

      > Der Name der Regel darf unabhängig von der Groß-/Kleinschreibung nicht mit den folgenden reservierten Namen übereinstimmen: "Alle", "ICMPv4" und "ICMPv6". Der Name muss in der Liste aller Regeln für eingehende Netzwerkverbindungen eindeutig sein.

      b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm eingehende Netzwerkverbindungen für das Programm.
      - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm eingehende Netzwerkverbindungen für das Programm.

      c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

      d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

      e. Geben Sie im Feld **Programmpfad** manuell oder mithilfe der Schaltfläche **Durchsuchen** den Pfad zur ausführbaren Datei des Programms an, für das Sie die Regel konfigurieren.

      f. Geben Sie im Feld **Dienstname** bei Bedarf den Namen des Dienstes an, auf den die Regel angewendet werden soll.

      g. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht eingehende Verbindungen von den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

      > Für IP-Adressen wird nur das IPv4-Format unterstützt.

      h. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

      i. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

   3. Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen**.

      Das Fenster **Regel für Ports** wird geöffnet.

4. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

   - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm eingehende Netzwerkverbindungen für die Ports.
   - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm eingehende Netzwerkverbindungen für die Ports.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

   e. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht eingehende Verbindungen von den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

   > Für IP-Adressen wird nur das IPv4-Format unterstützt.

   f. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

   g. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

5. Klicken Sie im Fenster **Regeln für eingehende Verbindungen** auf **OK**.

5. Klicken Sie im Block **Ausgehende Verbindungen** auf **Regelliste**.

   Das Fenster **Regeln für ausgehende Verbindungen** wird geöffnet.

6. **Erstellen und konfigurieren Sie Firewall-Regeln für ausgehende Verbindungen**.

   1. Klicken Sie auf der Registerkarte **Programme** auf **Hinzufügen**.

      Das Fenster **Regel für eine Anwendung** wird geöffnet.

   2. Konfigurieren Sie die Regeleinstellungen:

      a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

      > Der Name der Regel darf unabhängig von der Groß-/Kleinschreibung nicht mit den folgenden reservierten Namen übereinstimmen: "Alle", "ICMPv4" und "ICMPv6". Der Name muss in der Liste aller Regeln für ausgehende Netzwerkverbindungen eindeutig sein.

      b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

      - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm ausgehende Netzwerkverbindungen für das Programm.
      - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm ausgehende Netzwerkverbindungen für das Programm.

c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

e. Geben Sie im Feld **Programmpfad** manuell oder mithilfe der Schaltfläche **Durchsuchen** den Pfad zur ausführbaren Datei des Programms an, für das Sie die Regel konfigurieren.

f. Geben Sie im Feld **Dienstname** bei Bedarf den Namen des Dienstes an, auf den die Regel angewendet werden soll.

g. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht ausgehende Verbindungen zu den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

> Für IP-Adressen wird nur das IPv4-Format unterstützt.

h. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

i. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

3. Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen**.

   Das Fenster **Regel für Ports** wird geöffnet.

4. Konfigurieren Sie die Regeleinstellungen:

   a. Tragen Sie im Feld **Regelname** einen Namen für die Regel ein.

   b. Wählen Sie aus der Liste **Aktion** eine der Optionen aus:

   - **Erlauben**. Wenn diese Option ausgewählt ist, erlaubt das Programm ausgehende Netzwerkverbindungen für die Ports.
   - **Blockieren**. Wenn diese Option ausgewählt ist, blockiert das Programm ausgehende Netzwerkverbindungen für die Ports.

   c. Aktivieren Sie das Kontrollkästchen **Protokoll**, um den Protokolltyp auszuwählen, für den das Programm eingehende Netzwerkverbindungen kontrolliert.

   d. Geben Sie in den Blöcken **Ports** und **Ports** einen Port oder Portbereich an.

   e. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzwerkadressen an. Das Programm überwacht ausgehende Verbindungen zu den angegebenen Netzwerkadressen gemäß den Regeleinstellungen.

   > Für IP-Adressen wird nur das IPv4-Format unterstützt.

   f. Geben Sie im Block **Netzwerkadapter** die Liste der Netzwerkadapter an.

   g. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu speichern.

5. Klicken Sie im Fenster **Regeln für ausgehende Verbindungen** auf **OK**.

7. Wenn Sie benutzerdefinierte Regeln aus einer xml-Datei importieren oder exportieren möchten, verwenden Sie die Schaltflächen **Import** oder **Export** im Block **Import und Export von Regeln**.

8. Um Regeln aus der Windows-Firewall zu importieren, klicken Sie auf **Windows-Firewall-Regeln importieren**.

   Auf Computern mit Windows 11 24H2 überspringt das Programm möglicherweise bestimmte Regeln der Windows-Firewall. Aufgrund spezieller Funktionen dieser Betriebssystemversion erkennt Kaspersky Embedded Systems Security möglicherweise die Parameter einiger Regeln für Programmpakete nicht.

9. Speichern Sie die vorgenommenen Änderungen.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen. Datum und Uhrzeit der Änderung der Einstellungen werden im System-Überwachungsprotokoll gespeichert.

Firewall-Regeln aktivieren und deaktivieren

Firewall-Regeln aktivieren und deaktivieren (in der Kaspersky Security Center-Verwaltungskonsole)

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. Klicken Sie im Abschnitt **Kontrolle der Netzwerkaktivität** im Unterabschnitt **Firewall** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Firewall** wird geöffnet.

4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste** im Abschnitt **Eingehende Verbindungen** oder **Ausgehende Verbindungen**, abhängig vom Typ der Regel, deren Status Sie ändern möchten.

5. Wählen Sie im folgenden Fenster die Registerkarte **Programme** oder **Ports** aus.

   Suchen Sie in der Liste der Regeln die Regel aus, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

   - Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird aktiviert.

   - Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird deaktiviert.

6. Um Regeln aus der Liste zu löschen, wählen Sie die Regeln aus und klicken Sie auf **Löschen**.

7. Speichern Sie die vorgenommenen Änderungen.

Firewall-Regeln aktivieren und deaktivieren (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Klicken Sie im Abschnitt **Kontrolle der Netzwerkaktivität** im Unterabschnitt **Firewall** auf die Schaltfläche **Anpassen**.

   Das Fenster **Firewall** wird geöffnet.
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Anpassen** im Abschnitt **Eingehende Verbindungen** oder **Ausgehende Verbindungen**, abhängig vom Typ der Regel, deren Status Sie ändern möchten.
6. Wählen Sie im folgenden Fenster die Registerkarte **Ports** oder **Programme** aus.

   Suchen Sie in der Liste der Regeln die Regel aus, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

   - Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird aktiviert.
   - Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird deaktiviert.
7. Um Regeln aus der Liste zu löschen, wählen Sie die Regeln aus und klicken Sie auf **Löschen**.
8. Speichern Sie die vorgenommenen Änderungen.

Firewall-Regeln aktivieren und deaktivieren (in der Programmkonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Computer-Kontrolle** → **Firewall** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Firewall** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Firewall** wird geöffnet.
3. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste** im Abschnitt **Eingehende Verbindungen** oder **Ausgehende Verbindungen**, abhängig vom Typ der Regel, deren Status Sie ändern möchten.
4. Wählen Sie im folgenden Fenster die Registerkarte **Programme** oder **Ports** aus.

   Suchen Sie in der Liste der Regeln die Regel aus, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

   - Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird aktiviert.

- Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

  Die ausgewählte Regel wird deaktiviert.

5. Um Regeln aus der Liste zu löschen, wählen Sie die Regeln aus und klicken Sie auf **Löschen**.

6. Speichern Sie die vorgenommenen Änderungen.

Schutz vor modifizierten USB-Geräten

Die Komponente „Schutz vor BadUSB-Angriffen“ wird standardmäßig nicht installiert. Sie können eine Komponente während der Programminstallation hinzufügen oder die Auswahl der Programmkomponenten nach der Programminstallation ändern.

Bestimmte Viren verändern die in USB-Geräten eingebettete Software so, dass das USB-Gerät vom Betriebssystem als Tastatur erkannt wird. Infolgedessen kann der Virus unter Ihrem Benutzerkonto Befehle ausführen, um z. B. Malware herunterzuladen.

Die Komponente „Schutz vor BadUSB-Angriffen“ verhindert, dass modifizierte USB-Geräte, die eine Tastatur simulieren, mit dem PC verbunden werden.

Wenn ein USB-Gerät an den Computer angeschlossen und vom Betriebssystem als Tastatur erkannt wird, fordert das Programm den Benutzer auf, mit diesem Gerät oder mithilfe der Bildschirmtastatur (falls diese verfügbar ist) einen vom Programm generierten digitalen Code einzugeben. 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, 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.

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 konfigurieren Sie die Komponente „Schutz vor modifizierten USB-Geräten“ (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Kontrolle der lokalen Aktivität**.

4. Klicken Sie im Block **Schutz vor BadUSB-Angriffen** auf **Einstellungen**.

   Das Fenster **Schutz vor BadUSB-Angriffen** wird geöffnet.

5. Verwenden Sie das Kontrollkästchen **Schutz vor BadUSB-Angriffen**, um die Komponente zu aktivieren oder zu deaktivieren.

6. Konfigurieren Sie im Abschnitt **Autorisierung von USB-Geräten** die folgenden Einstellungen:

   - **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 Embedded Systems Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie wieder fünf Versuche, den Autorisierungscode einzugeben.

   - **Timeout, wenn maximale Anzahl der Versuche erreicht wird (Minuten)**. Dauer, für die das USB-Gerät gesperrt wird, nachdem die zulässige Anzahl der Eingabeversuche für den Autorisierungscode erreicht wurden. Mögliche Werte: 1 bis 180 (Minuten).

7. Konfigurieren Sie im Abschnitt **Autorisierung von USB-Geräten beim Anschließen** die folgenden Einstellungen:

   - **Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten**. Wenn das Kontrollkästchen aktiviert ist, verbietet das Programm die Verwendung einer Bildschirmtastatur für die Autorisierung von USB-Geräten, auf denen kein Autorisierungscode eingegeben werden kann (z. B. Strichcode-Scanner).

   - **Verwendung eines Strichcodes zur Autorisierung von USB-Geräten verbieten**. Wenn das Kontrollkästchen aktiviert ist, zeigt das Programm den Strichcode nicht in der Benachrichtigung zur Autorisierung via Strichcode-Scanner an.

8. Verriegeln Sie die Vorhängeschlösser, um die Richtlinie auf die Computer anzuwenden.

9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren und konfigurieren Sie die Komponente „Schutz vor modifizierten USB-Geräten“ (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Kontrolle der lokalen Aktivität** aus.

5. Klicken Sie im Block **Schutz vor BadUSB-Angriffen** auf **Anpassen**.

   Das Fenster **Schutz vor BadUSB-Angriffen** wird geöffnet.

6. Verwenden Sie den Schalter **Schutz vor BadUSB-Angriffen**, um die Komponente zu aktivieren oder zu deaktivieren.

7. Aktivieren oder deaktivieren Sie den Schalter **Verbot der Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten AKTIVIERT**, um zu erlauben oder zu verbieten, dass eine Bildschirmtastatur für die Autorisierung von USB-Geräten verwendet wird, auf denen kein Autorisierungscode eingegeben werden kann (z. B. Barcode-Scanner).

8. Aktivieren oder deaktivieren Sie den Schalter **Verbot der Verwendung eines Strichcodes zur Autorisierung von USB-Geräten AKTIVIERT**, um die Anzeige eines Strichcodes in der Autorisierungsbenachrichtigung des Barcode-Scanners zu erlauben oder zu verbieten.

9. Konfigurieren Sie im Abschnitt **Autorisierung von USB-Geräten** die folgenden Einstellungen:

   - **Maximale Anzahl der Autorisierungsversuche für USB-Geräte (1–10)**. 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 Embedded Systems Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie wieder fünf Versuche, den Autorisierungscode einzugeben.

   - **Timeout beim Erreichen der maximalen Anzahl von Versuchen, in Minuten (1–180)**. Dauer, für die das USB-Gerät gesperrt wird, nachdem die zulässige Anzahl der Eingabeversuche für den Autorisierungscode erreicht wurden. Mögliche Werte: 1 bis 180 (Minuten).

10. Verriegeln Sie die Vorhängeschlösser, um die Richtlinie auf die Computer anzuwenden.

11. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So aktivieren und konfigurieren Sie die Komponente „Schutz vor modifizierten USB-Geräten“ (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Computer-Kontrolle → Schutz vor BadUSB-Angriffen** aus.

2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Schutz vor BadUSB-Angriffen** wird geöffnet.

3. Verwenden Sie das Kontrollkästchen **Schutz vor BadUSB-Angriffen**, um die Komponente zu aktivieren oder zu deaktivieren.

4. Konfigurieren Sie im Abschnitt **Autorisierung von USB-Geräten** die folgenden Einstellungen:

   - **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 Embedded Systems Security zeigt die Sperrdauer für das USB-Gerät an. Nach Ablauf dieses Zeitraums haben Sie wieder fünf Versuche, den Autorisierungscode einzugeben.

   - **Timeout, wenn maximale Anzahl der Versuche erreicht wird (Minuten)**. Dauer, für die das USB-Gerät gesperrt wird, nachdem die zulässige Anzahl der Eingabeversuche für den Autorisierungscode erreicht wurden. Mögliche Werte: 1 bis 180 (Minuten).

5. Konfigurieren Sie im Abschnitt **Autorisierung von USB-Geräten beim Anschließen** die folgenden Einstellungen:

- **Verwendung der Bildschirmtastatur zur Autorisierung von USB-Geräten verbieten**. Wenn das Kontrollkästchen aktiviert ist, verbietet das Programm die Verwendung einer Bildschirmtastatur für die Autorisierung von USB-Geräten, auf denen kein Autorisierungscode eingegeben werden kann (z. B. Strichcode-Scanner).

- **Verwendung eines Strichcodes zur Autorisierung von USB-Geräten verbieten**. Wenn das Kontrollkästchen aktiviert ist, zeigt das Programm den Strichcode nicht in der Benachrichtigung zur Autorisierung via Strichcode-Scanner an.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Überwachung der Systemintegrität

In Kaspersky Embedded Systems Security 4.0 wurde die Komponente „Überwachung der Systemintegrität“ durch die Komponente „Überwachung der Systemintegrität“ ersetzt. Die Überwachung der Systemintegrität enthält alle Funktionen der Überwachung der Datei-Integrität 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 Embedded Systems 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

Sie können die Aufgabe zur Prüfung der Systemintegrität auf Befehl entweder manuell oder nach einem Zeitplan ausführen. Um die Aufgabe **Baseline-Überwachung 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. Eine Baseline wird erstellt, wenn die Aufgabe zum ersten Mal gestartet wird.

Migration der Einstellungen für die Überwachung der Datei-Integrität

Wenn Sie Kaspersky Embedded Systems Security Version 3.4 oder älter auf Version 4.1 aktualisieren, werden die Einstellungen für die Überwachung der Datei-Integrität und für die Überwachung des Registrierungszugriffs automatisch migriert. Im Rahmen der Migration werden die Überwachungsregeln in die Überwachung der Systemintegrität verschoben.

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 oder auf die Registrierung definieren. Die Überwachung der Systemintegrität erkennt Änderungen an Dateien oder 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.

Kaspersky Embedded Systems 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.

Das Programm generiert das Ereignis Objekt erstellen, wenn eine der folgenden Aktionen aufgezeichnet wird: Erstellen einer Datei, Vergrößern einer Datei, Ändern von Dateidaten oder Verkleinern einer Datei. Wenn die Kontrolle des Programmstarts Verbotsregeln anwendet und dabei das Ereignis Objekt erstellen für eine Datei generiert wird, sind verschiedene Gründe möglich: Es kann sein, dass das Erstellen oder das Ändern einer Datei verboten wurde (einschließlich Vorgängen wie Vergrößern einer Datei, Ändern von Daten oder Verkleinern einer Datei).

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

Der Schlüssel HKEY_CURRENT_USER wird von der Überwachung der Systemintegrität nicht unterstützt. 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 Programmkomponente 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 der 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.

So aktivieren und konfigurieren Sie die Echtzeitüberwachung der Systemintegrität (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **System-Inspektion** aus.
4. Klicken Sie im Abschnitt **Überwachung der Systemintegrität** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Überwachung der Systemintegrität**.
6. Konfigurieren Sie die Überwachung der Datei-Integrität:
   a. Aktivieren Sie das Kontrollkästchen **Dateien überwachen** auf der Registerkarte **Dateien**.
   b. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Überwachung der Datei-Integrität aus:
      - **Blockieren**. In diesem Modus verarbeitet das Programm die Dateien gemäß den Regeln für die Überwachung der Datei-Integrität und generiert entsprechende Ereignisse im Protokoll für die Überwachung der Systemintegrität.
      - **Informieren**. In diesem Modus generiert das Programm nur Ereignisse, die sich auf ausgelöste Regeln zur Überwachung der Datei-Integrität beziehen. Die Ereignisse werden ins Protokoll der Überwachung der Systemintegrität eingetragen.
   c. Fügen Sie manuell Regeln für die Überwachung der Datei-Integrität hinzu. Verwenden Sie dazu die Schaltfläche **Hinzufügen** oder importieren Sie die Regeln aus einer XML-Datei. Die Einstellungen für Regeln zur Überwachung der Datei-Integrität werden in der folgenden Tabelle beschrieben.
   d. Aktivieren Sie in der Liste der Regeln für die Überwachung der Datei-Integrität die Kontrollkästchen der Regeln, die aktiviert bleiben sollen.
7. Konfigurieren Sie die Überwachung des Registrierungszugriffs:
   a. Aktivieren Sie das Kontrollkästchen **Registrierung überwachen** auf der Registerkarte **Registrierung**.
   b. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Überwachung des Registrierungszugriffs aus:
      - **Blockieren**. In diesem Modus blockiert das Programm die Aktionen mit der Registrierung gemäß den Regeln für die Überwachung des Registrierungszugriffs und generiert entsprechende Ereignisse im Protokoll für die Überwachung der Systemintegrität.
      - **Informieren**. In diesem Modus generiert das Programm nur Ereignisse, die sich auf ausgelöste Regeln zur Überwachung des Registrierungszugriffs beziehen. Die Ereignisse werden ins Protokoll der Überwachung der Systemintegrität eingetragen.

c. Fügen Sie manuell Regeln für die Überwachung des Registrierungszugriffs hinzu. Verwenden Sie dazu die Schaltfläche **Hinzufügen** oder importieren Sie die Regeln aus einer XML-Datei. Die Einstellungen für Regeln zur Überwachung des Registrierungszugriffs werden in der folgenden Tabelle beschrieben.

d. Aktivieren Sie in der Liste der Regeln für die Überwachung des Registrierungszugriffs die Kontrollkästchen der Regeln, die aktiviert bleiben sollen.

8. Konfigurieren Sie die Überwachung externer Geräte:

a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen** auf der Registerkarte **Geräte**.

b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Wichtig*.

Nachdem die Einstellungen zur Überwachung externer Geräte übernommen wurden, merkt sich das Programm die aktuellen Verbindungen mit externen Geräten. Wenn künftig ein externes Gerät angeschlossen oder getrennt wird, generiert das Programm ein entsprechendes Ereignis im Protokoll für die Überwachung der Systemintegrität.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und konfigurieren Sie die Echtzeitüberwachung der Systemintegrität (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 Embedded Systems Security.

Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **System-Inspektion** → **Überwachung der Systemintegrität** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Aktivieren Sie das Kontrollkästchen **Überwachung der Systemintegrität**.

6. Konfigurieren Sie die Überwachung der Datei-Integrität:

a. Aktivieren Sie das Kontrollkästchen **Dateien überwachen** auf der Registerkarte **Dateien**.

b. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Überwachung der Datei-Integrität aus:

- **Blockieren**. In diesem Modus verarbeitet das Programm die Dateien gemäß den Regeln für die Überwachung der Datei-Integrität und generiert entsprechende Ereignisse im Protokoll für die Überwachung der Systemintegrität.

- **Informieren**. In diesem Modus generiert das Programm nur Ereignisse, die sich auf ausgelöste Regeln zur Überwachung der Datei-Integrität beziehen. Die Ereignisse werden ins Protokoll der Überwachung der Systemintegrität eingetragen.

c. Fügen Sie manuell Regeln für die Überwachung der Datei-Integrität hinzu. Verwenden Sie dazu die Schaltfläche **Hinzufügen** oder importieren Sie die Regeln aus einer XML-Datei. Die Einstellungen für Regeln zur Überwachung der Datei-Integrität werden in der folgenden Tabelle beschrieben.

d. Aktivieren Sie in der Liste der Regeln für die Überwachung der Datei-Integrität in der Spalte **Status** die Kontrollkästchen der Regeln, die aktiviert bleiben sollen.

7. Konfigurieren Sie die Überwachung des Registrierungszugriffs:

   a. Aktivieren Sie das Kontrollkästchen **Registrierung überwachen** auf der Registerkarte **Registrierung**.

   b. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Überwachung des Registrierungszugriffs aus:

      - **Blockieren**. In diesem Modus blockiert das Programm die Aktionen mit der Registrierung gemäß den Regeln für die Überwachung des Registrierungszugriffs und generiert entsprechende Ereignisse im Protokoll für die Überwachung der Systemintegrität.

      - **Informieren**. In diesem Modus generiert das Programm nur Ereignisse, die sich auf ausgelöste Regeln zur Überwachung des Registrierungszugriffs beziehen. Die Ereignisse werden ins Protokoll der Überwachung der Systemintegrität eingetragen.

   c. Fügen Sie manuell Regeln für die Überwachung des Registrierungszugriffs hinzu. Verwenden Sie dazu die Schaltfläche **Hinzufügen** oder importieren Sie die Regeln aus einer XML-Datei. Die Einstellungen für Regeln zur Überwachung des Registrierungszugriffs werden in der folgenden Tabelle beschrieben.

   d. Aktivieren Sie in der Liste der Regeln für die Überwachung des Registrierungszugriffs in der Spalte **Status** die Kontrollkästchen der Regeln, die aktiviert bleiben sollen.

8. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen** auf der Registerkarte **Geräte**.

   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Wichtig*.

      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.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren und konfigurieren Sie die Echtzeitüberwachung der Systemintegrität (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **System-Inspektion → Überwachung der Systemintegrität** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Überwachung der Systemintegrität** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Überwachung der Systemintegrität** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Überwachung der Systemintegrität**.

4. Konfigurieren Sie die Überwachung der Datei-Integrität:

   a. Aktivieren Sie das Kontrollkästchen **Dateien überwachen** auf der Registerkarte **Dateien**.

   b. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Überwachung der Datei-Integrität aus:

      - **Blockieren**. In diesem Modus verarbeitet das Programm die Dateien gemäß den Regeln für die Überwachung der Datei-Integrität und generiert entsprechende Ereignisse im Protokoll für die Überwachung der Systemintegrität.

      - **Informieren**. In diesem Modus generiert das Programm nur Ereignisse, die sich auf ausgelöste Regeln zur Überwachung der Datei-Integrität beziehen. Die Ereignisse werden ins Protokoll der Überwachung der Systemintegrität eingetragen.

   c. Fügen Sie manuell Regeln für die Überwachung der Datei-Integrität hinzu. Verwenden Sie dazu die Schaltfläche **Hinzufügen** oder importieren Sie die Regeln aus einer XML-Datei. Die Einstellungen für Regeln zur Überwachung der Datei-Integrität werden in der folgenden Tabelle beschrieben.

   d. Aktivieren Sie in der Liste der Regeln für die Überwachung der Datei-Integrität die Kontrollkästchen der Regeln, die aktiviert bleiben sollen.

5. Konfigurieren Sie die Überwachung des Registrierungszugriffs:

   a. Aktivieren Sie das Kontrollkästchen **Registrierung überwachen** auf der Registerkarte **Registrierung**.

   b. Wählen Sie unter **Funktionsmodus für Sperr-Regeln** einen Modus für die Überwachung des Registrierungszugriffs aus:

      - **Blockieren**. In diesem Modus blockiert das Programm die Aktionen mit der Registrierung gemäß den Regeln für die Überwachung des Registrierungszugriffs und generiert entsprechende Ereignisse im Protokoll für die Überwachung der Systemintegrität.

      - **Informieren**. In diesem Modus generiert das Programm nur Ereignisse, die sich auf ausgelöste Regeln zur Überwachung des Registrierungszugriffs beziehen. Die Ereignisse werden ins Protokoll der Überwachung der Systemintegrität eingetragen.

   c. Fügen Sie manuell Regeln für die Überwachung des Registrierungszugriffs hinzu. Verwenden Sie dazu die Schaltfläche **Hinzufügen** oder importieren Sie die Regeln aus einer XML-Datei. Die Einstellungen für Regeln zur Überwachung des Registrierungszugriffs werden in der folgenden Tabelle beschrieben.

   d. Aktivieren Sie in der Liste der Regeln für die Überwachung des Registrierungszugriffs die Kontrollkästchen der Regeln, die aktiviert bleiben sollen.

6. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen** auf der Registerkarte **Geräte**.

   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Ereigniskategorie für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Kritisch*.

      Nachdem die Einstellungen zur Überwachung externer Geräte übernommen wurden, merkt sich das Programm die aktuellen Verbindungen mit externen Geräten. Wenn künftig ein externes Gerät angeschlossen oder getrennt wird, generiert das Programm ein entsprechendes Ereignis im Protokoll für die Überwachung der Systemintegrität.

7. Speichern Sie die vorgenommenen Änderungen.

Einstellung	Beschreibung
Dateioperationen im folgenden Bereich überwachen	Bereich, auf den Sie die Überwachung der Datei-Integrität anwenden möchten. Dieses Feld ist obligatorisch. Verwenden Sie Masken: Kaspersky Embedded Systems 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.
Überwachte Objekte	Hier können Sie den Namen oder den Wert eines Registrierungsschlüssels angeben. Verwenden Sie Masken: Kaspersky Embedded Systems Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:
Vorgänge mit Dateien	• **Erkennen**. Das Programm erlaubt Aktionen mit Dateien im Überwachungsbereich. • **Erkennen und blockieren**. Die Aktionen des Programms hängen davon ab, welcher Modus für die Überwachung der Datei-Integrität ausgewählt ist. Wenn Sie den Modus *Blockieren* ausgewählt haben, verbietet die Überwachung der Systemintegrität Aktionen mit Dateien aus dem Überwachungsbereich. Wenn Sie den Modus *Informieren* ausgewählt haben, erlaubt die Überwachung der Systemintegrität Aktionen mit Dateien aus dem Überwachungsbereich.
Vertrauenswürdige Benutzer und/oder Benutzergruppen	Ein vertrauenswürdiger Benutzer ist ein Benutzer, der Aktionen mit Dateien und Registrierungsschlüsseln im Überwachungsbereich ausführen darf. Wenn Kaspersky Embedded Systems 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.
Markierungen für Dateivorgänge / Actions	Markierungen, die die Aktion mit Dateien oder Registrierungsschlüsseln charakterisieren, die von der App überwacht werden.
Dateivorgänge anhand aller registrierten Markierungen erkennen / Registrierungsvorgänge anhand aller erkannten Markierungen erkennen	Kaspersky Embedded Systems Security erkennt standardmäßig alle Markierungen für Datei-/Registrierungsvorgänge.
Dateivorgänge anhand der folgenden Markierungen erkennen / Registrierungsvorgänge anhand der folgenden Markierungen erkennen	Aktivieren Sie in der Liste der verfügbaren Datei-/Registrierungsvorgänge die Kontrollkästchen aller Vorgänge, die Sie überwachen möchten.
Bei Möglichkeit Prüfsumme nach einem Dateivorgang berechnen. Die Prüfsumme wird im Aufgabenprotokoll angegeben	Wenn das Kontrollkästchen aktiviert ist, ermittelt Kaspersky Embedded Systems Security die Prüfsumme der geänderten Datei, weine eine Dateioperation gefunden wurde, die mindestens einem ausgewählten Marker entspricht. Wenn für die Erkennung eines Dateivorgangs verschiedene Markierungen gelten, wird nur die Prüfsumme der endgültigen Datei berechnet, nachdem alle Änderungen vorgenommen wurden. Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security keine Prüfsumme der geänderten Dateien. In den folgenden Fällen wird keine Berechnung der Prüfsumme vorgenommen: • Wenn infolge der Dateioperation die Datei nicht mehr verfügbar ist (weil z. B. die Zugriffsrechte für die Datei geändert wurden) • Wenn in der Datei eine Dateioperation gefunden wurde, die daraufhin gelöscht wurde Das Kontrollkästchen ist standardmäßig deaktiviert.
Algorithmus zur Prüfsummenberechnung	Wählen Sie aus der Dropdown-Liste einen Algorithmus zur Berechnung der Prüfsumme aus: • MD5-Hash • SHA256-Hash

Einstellung	Beschreibung
Ausnahmen	Auf der Registerkarte **Ausnahmen** können Sie Objekte hinzufügen, die Sie aus dem Überwachungsbereich ausschließen möchten: • Für eine Regel zur Überwachung der Datei-Integrität können Sie eine Liste mit Ordnern angeben. • Für eine Regel zur Überwachung von Registrierungszugriffen können Sie Registrierungsschlüssel oder Werte angeben. Verwenden Sie Masken: **Dateien** Liste der Dateien und Ordner, die von der Komponente überwacht werden. Kaspersky Embedded Systems 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. **Registrierung** Kaspersky Embedded Systems Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske: Einträge für Ausnahmen haben eine höhere Priorität als Einträge des Überwachungsbereichs.
Ereignis-Signifikanz	Kaspersky Embedded Systems Security protokolliert Dateiänderungsereignisse, wenn eine Datei oder ein Registrierungsschlüssel im Überwachungsbereich geändert wird. Die folgenden Ereignisschweregrade sind verfügbar: **Informativ**, **Warnung**, **Kritisch**.

Prüfung der Systemintegrität auf Befehl

Die Aufgabe zur Prüfung der Systemintegrität auf Befehl können Sie manuell oder nach einem Zeitplan ausführen. Wenn die Aufgabe *Baseline-Überwachung der Systemintegrität* ausgeführt wird, vergleicht die App den aktuellen Status der Objekte, die zum Überwachungsbereich gehören, mit ihrem *Baseline*-Status. Eine Baseline wird erstellt, wenn die Aufgabe zum ersten Mal gestartet wird.

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.

Überwachungsbereich für die Aufgabe Baseline-Überwachung der Systemintegrität konfigurieren

Standardmäßig ist der Überwachungsbereich der Aufgabe *Baseline-Überwachung der Systemintegrität* identisch mit dem Überwachungsbereich der Überwachung 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 einen anderen Überwachungsbereich für die Aufgabe Baseline-Überwachung der Systemintegrität (in der Kaspersky Security Center-Verwaltungskonsole)

1. Wählen Sie in der Verwaltungskonsolenstruktur von Kaspersky Security Center den Punkt **Aufgaben** aus.
2. Wählen Sie die erforderliche Aufgabe *Baseline-Überwachung der Systemintegrität* aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.
3. Wählen Sie im folgenden Fenster den Punkt **Einstellungen** aus.
4. Konfigurieren Sie die Dateiüberwachung:
   a. Aktivieren Sie das Kontrollkästchen **Dateien überwachen** auf der Registerkarte **Dateien**.
   b. Wählen Sie in der Liste mithilfe der Kontrollkästchen Regeln aus.
   c. Fügen Sie bei Bedarf über die Schaltfläche **Hinzufügen** eine neue Regel hinzu. Die Einstellungen einer Regel für die Baseline-Überwachung der Systemintegrität werden in der folgenden Tabelle beschrieben.
   d. Sie können auch Regeln aus einer anderen Quelle importieren.
5. Konfigurieren Sie die Überwachung der Registrierung:
   a. Aktivieren Sie das Kontrollkästchen **Registrierung überwachen** auf der Registerkarte **Registrierung**.
   b. Wählen Sie in der Liste mithilfe der Kontrollkästchen Regeln aus.
   c. Fügen Sie bei Bedarf über die Schaltfläche **Hinzufügen** eine neue Regel hinzu. Die Einstellungen einer Regel für die Baseline-Überwachung der Systemintegrität werden in der folgenden Tabelle beschrieben.
   d. Sie können auch Regeln aus einer anderen Quelle importieren.
6. Konfigurieren Sie die Überwachung externer Geräte:
   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen** auf der Registerkarte **Geräte**.
   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Prioritätsstufe für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Wichtig*.

      Die Baseline-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 ausgeführt wird, wird das Trennen externer Geräte nicht überwacht.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die Web Console einen anderen Überwachungsbereich für die Aufgabe Baseline-Überwachung der Systemintegrität

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Aufgaben** aus.
2. Wählen Sie die erforderliche Aufgabe *Baseline-Überwachung der Systemintegrität* aus und öffnen Sie durch Doppelklick das Fenster mit den Aufgabeneigenschaften.
3. Wählen Sie im folgenden Fenster den Punkt **Anwendungseinstellungen** aus.

4. Konfigurieren Sie die Dateiüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien überwachen**.

   b. Wählen Sie in der Liste mithilfe der Kontrollkästchen Regeln aus.

   c. Fügen Sie bei Bedarf über die Schaltfläche **Hinzufügen** eine neue Regel hinzu. Die Einstellungen einer Regel für die Baseline-Überwachung der Systemintegrität werden in der folgenden Tabelle beschrieben.

   d. Sie können auch Regeln aus einer anderen Quelle importieren.

5. Konfigurieren Sie die Überwachung der Registrierung:

   a. Aktivieren Sie das Kontrollkästchen **Registrierung überwachen**.

   b. Wählen Sie in der Liste mithilfe der Kontrollkästchen Regeln aus.

   c. Fügen Sie bei Bedarf über die Schaltfläche **Hinzufügen** eine neue Regel hinzu. Die Einstellungen einer Regel für die Baseline-Überwachung der Systemintegrität werden in der folgenden Tabelle beschrieben.

   d. Sie können auch Regeln aus einer anderen Quelle importieren.

6. Konfigurieren Sie die Überwachung externer Geräte:

   a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen**.

   b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Ereigniskategorie für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Kritisch*.

      Die Aufgabe *Baseline-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 ausgeführt wird, wird das Trennen externer Geräte nicht überwacht.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie über die Programmkonsole einen anderen Überwachungsbereich für die Aufgabe Baseline-Überwachung der Systemintegrität

Die Eigenschaften der Aufgabe **Baseline-Überwachung der Systemintegrität** können in der Konsole für Kaspersky Embedded Systems Security bearbeitet werden, wenn die Aufgabe lokal erstellt wurde oder wenn das Kontrollkästchen **Verwendung lokaler Aufgaben erlauben** im Abschnitt **Programmeinstellungen → Lokale Systemaufgaben ausführen** der Richtlinieneigenschaften aktiviert ist.

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **System-Inspektion → Baseline-Überwachung der Systemintegrität** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Baseline-Überwachung der Systemintegrität** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Baseline-Überwachung der Systemintegrität** wird geöffnet.

3. Konfigurieren Sie die Dateiüberwachung:

   a. Aktivieren Sie das Kontrollkästchen **Dateien überwachen** auf der Registerkarte **Dateien**.

   b. Wählen Sie in der Liste mithilfe der Kontrollkästchen Regeln aus.

c. Fügen Sie bei Bedarf über die Schaltfläche **Hinzufügen** eine neue Regel hinzu. Die Einstellungen einer Regel für die Baseline-Überwachung der Systemintegrität werden in der folgenden Tabelle beschrieben.

d. Sie können auch Regeln aus einer anderen Quelle importieren.

4. Konfigurieren Sie die Überwachung der Registrierung:

a. Aktivieren Sie das Kontrollkästchen **Registrierung überwachen** auf der Registerkarte **Registrierung**.

b. Wählen Sie in der Liste mithilfe der Kontrollkästchen Regeln aus.

c. Fügen Sie bei Bedarf über die Schaltfläche **Hinzufügen** eine neue Regel hinzu. Die Einstellungen einer Regel für die Baseline-Überwachung der Systemintegrität werden in der folgenden Tabelle beschrieben.

d. Sie können auch Regeln aus einer anderen Quelle importieren.

5. Konfigurieren Sie die Überwachung externer Geräte:

a. Aktivieren Sie das Kontrollkästchen **Geräte überwachen** auf der Registerkarte **Geräte**.

b. Wählen Sie in der Dropdown-Liste **Ereignis-Signifikanz** die Ereigniskategorie für Ereignisse bei der Überwachung externer Geräte aus: *Informativ*, *Warnung*, *Kritisch*.

Die Baseline-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 ausgeführt wird, wird das Trennen externer Geräte nicht überwacht.

6. Speichern Sie die vorgenommenen Änderungen.

Einstellungen einer Regel für die Aufgabe Baseline-Überwachung der Systemintegrität

Einstellung	Beschreibung
Dateioperationen im folgenden Bereich überwachen	Bereich, auf den Sie die Überwachung der Datei-Integrität anwenden möchten. Dieses Feld ist obligatorisch. Verwenden Sie Masken: Kaspersky Embedded Systems 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.
Überwachte Objekte	Hier können Sie den Namen oder den Wert eines Registrierungsschlüssels angeben. Verwenden Sie Masken: Kaspersky Embedded Systems Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske:

Einstellung	Beschreibung
Ausnahmen	Auf der Registerkarte **Ausnahmen** können Sie Objekte hinzufügen, die Sie aus dem Überwachungsbereich ausschließen möchten: • Für eine Regel zur Überwachung der Datei-Integrität können Sie eine Liste mit Ordnern angeben. • Für eine Regel zur Überwachung von Registrierungszugriffen können Sie Registrierungsschlüssel oder Werte angeben. Verwenden Sie Masken: **Dateien** Liste der Dateien und Ordner, die von der Komponente überwacht werden. Kaspersky Embedded Systems 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. **Registrierung** Kaspersky Embedded Systems Security unterstützt die Zeichen `*` und `?` bei der Eingabe einer Maske: Einträge für Ausnahmen haben eine höhere Priorität als Einträge des Überwachungsbereichs.
Ereignis-Signifikanz	Kaspersky Embedded Systems Security protokolliert Dateiänderungsereignisse, wenn eine Datei oder ein Registrierungsschlüssel im Überwachungsbereich geändert wird. Die folgenden Ereignisschweregrade sind verfügbar: **Informativ**, **Warnung**, **Kritisch**.

Aufgabe Baseline-Überwachung der Systemintegrität starten

Die Aufgabe **Baseline-Überwachung 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 **Baseline-Überwachung der Systemintegrität** in den folgenden Modi ausführen:

- **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.

Der Ausführungsmodus der Aufgabe hat keinen Einfluss auf die Überprüfung der Registrierung oder externer Geräte.

So führen Sie die Aufgabe Baseline-Überwachung der Systemintegrität aus (in der Kaspersky Security Center-Verwaltungskonsole)

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.

3. Wählen Sie das **Kaspersky Embedded Systems 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.

4. 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.

   - Die Auswahl der Geräte angeben, 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.

5. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Embedded Systems Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.

6. Konfigurieren Sie einen Zeitplan für die Aufgabe, beispielsweise manuell oder an einem bestimmten Wochentag.

7. Geben Sie einen Namen für die Aufgabe ein.

8. 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 Baseline-Überwachung der Systemintegrität über die Web Console aus

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.

3. Passen Sie die Einstellungen der Aufgabe an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option Kaspersky Embedded Systems Security aus.

   b. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Baseline-Überwachung der Systemintegrität**.

   c. Geben Sie im Feld **Aufgabenname** eine kurze Beschreibung ein, beispielsweise *Wöchentliche Prüfung der Systemintegrität*.

4. Wählen Sie im Block **Geräte, denen die Aufgabe zugewiesen wird** den Aufgabenbereich aus.

5. Wählen Sie die Geräte aus. Berücksichtigen Sie dabei die ausgewählte Variante für den Gültigkeitsbereich der Aufgabe. Weiter zum nächsten Schritt

6. Wählen Sie den Algorithmus zur Berechnung der Prüfsumme aus.
7. Wählen Sie eine Benutzerkonto für den Start der Aufgabe aus. Kaspersky Embedded Systems Security startet die Aufgabe standardmäßig mit den Rechten des lokalen Benutzerkontos.
8. Schließen Sie den Assistenten ab.

   Die neue Aufgabe wird in der Aufgabenliste angezeigt.
9. Klicken Sie auf die neue Aufgabe.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.
10. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
11. Wählen Sie einen Modus für die Prüfung 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.
12. Speichern Sie die vorgenommenen Änderungen.
13. Aktivieren Sie das Kontrollkästchen neben der Aufgabe.
14. Klicken Sie auf **Starten**.

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*.

So exportieren und importieren Sie eine Liste der Regeln zur Überwachung der Systemintegrität (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **System-Inspektion** aus.
4. Klicken Sie im Abschnitt **Überwachung der Systemintegrität** auf **Einstellungen**.

5. Wechseln Sie je nachdem, welche Regeln Sie exportieren oder importieren möchten, zur Registerkarte **Dateien** oder **Registrierung**.

6. So exportieren Sie eine Liste mit Datei- und Registrierungsregeln:

   a. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

   b. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

      1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

      2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

   c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

      Kaspersky Embedded Systems Security exportiert die Liste der Regeln in die XLM-Datei.

7. So importieren Sie die Regeln für Dateien/Registrierung:

   a. Klicken Sie auf **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 Embedded Systems 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 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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **System-Inspektion** → **Überwachung der Systemintegrität** und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Einstellungen der Überwachung der Systemintegrität** wird geöffnet.

5. So exportieren Sie die Regeln für Dateien/Registrierung:

   a. Wählen Sie auf der Registerkarte **Datei** or **Registrierung** die Regeln aus, die Sie exportieren möchten.

   b. Klicken Sie auf die Schaltfläche **Export**. Dadurch wir ein Fenster geöffnet. Geben Sie in diesem Fenster an, ob Sie nur die ausgewählten Regeln oder alle Regeln exportieren möchten, und klicken Sie dann auf **Export**.

      Wenn Sie keine Regel ausgewählt haben, exportiert Kaspersky Embedded Systems Security alle Regeln.

6. Kaspersky Embedded Systems Security exportiert die Liste der Regeln in die XLM-Datei.

7. So importieren Sie die Regeln für Dateien/Registrierung:

    a. Klicken Sie auf der Registerkarte **Datei** oder **Registrierung** auf die Schaltfläche **Aus vorheriger Version importieren**, wenn Sie Regeln aus einer xml-Datei importieren möchten, die in der Programmversion 3.4 oder älter erstellt wurde.

    Wenn Sie Regeln aus einer xml-Datei importieren, die in Version 4.0 oder höher erstellt wurde, klicken Sie auf **Import**.

    b. Wenn es auf dem Computer bereits eine Liste mit Regeln gibt, fragt Kaspersky Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

    c. Wählen Sie im folgenden Fenster die XML-Datei aus, aus der Sie die Liste der Regeln importieren möchten.

    d. Klicken Sie auf **Import**.

8. Speichern Sie die vorgenommenen Änderungen.

So exportieren und importieren Sie eine Liste mit Regeln für die Überwachung der Systemintegrität (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **System-Inspektion → Überwachung der Systemintegrität** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Überwachung der Systemintegrität** auf **Eigenschaften**.

    Das Fenster **Eigenschaften: Überwachung der Systemintegrität** wird geöffnet.

3. Wechseln Sie je nachdem, welche Regeln Sie exportieren oder importieren möchten, zur Registerkarte **Dateien** oder **Registrierung**.

4. So exportieren Sie eine Liste mit Datei- und Registrierungsregeln:

    a. Wenn Sie die gesamte Liste exportieren möchten, klicken Sie auf die Schaltfläche und wählen Sie **Exportieren** aus.

    b. Wenn Sie nur einen Teil der Liste exportieren möchten, gehen Sie folgendermaßen vor:

        1. Wählen Sie mithilfe der Tasten **STRG** oder **UMSCHALT** die Listenelemente aus, die Sie exportieren möchten. Um alle Elemente auszuwählen, drücken Sie **STRG+A**.

        2. Klicken Sie auf die Schaltfläche und wählen Sie **Ausgewählte exportieren** aus.

    c. Geben Sie im folgenden Fenster den Namen der XML-Datei an, in die Sie exportieren möchten, und wählen Sie den Ordner aus, in dem die Datei gespeichert werden soll. Klicken Sie auf die Schaltfläche **Speichern**.

    Kaspersky Embedded Systems Security exportiert die Liste der Regeln in die XLM-Datei.

5. So importieren Sie die Regeln für Dateien/Registrierung:

    a. Klicken Sie auf **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 Embedded Systems Security, ob die vorhandene Liste gelöscht oder durch die Einträge aus der XLM-Datei ergänzt werden soll.

6. 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 Embedded Systems Security erstellt die folgenden Berichte über die Komponente:

- Bericht über Computer, auf denen Überwachungsregeln am häufigsten ausgelöst wurden
- Bericht über die Überwachungsregeln, die am häufigsten ausgelöst wurden

  Um einen Bericht über die am häufigsten ausgelösten Überwachungsregeln zu erstellen, protokolliert das Programm die folgenden Ereignisse:

  - *Änderung einer Datei oder eines Ordners wurde erkannt*
  - *Nur Statistik: Dateivorgang im Kontrollbereich verboten*
  - *Erlaubter Dateivorgang im Kontrollbereich von einem vertrauenswürdigen Benutzer ausgeführt*
  - *Dateivorgang im Kontrollbereich nicht kontrolliert*.

  Um die Speicherdauer dieser Ereignisse zu konfigurieren, geben Sie im Abschnitt **Konfiguration von Ereignissen** der Richtlinie die Dauer für das allgemeine Ereignis der Überwachung der Systemintegrität: *Änderung einer Datei oder eines Ordners wurde erkannt* an.

Standardmäßig umfasst ein Bericht die letzten 30 Tage, einschließlich des Datums der Berichterstellung.

So zeigen Sie Berichte zur Überwachung der Systemintegrität an (in der Kaspersky Security Center-Verwaltungskonsole)

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 **Vorlage** im Abschnitt **Andere** 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.

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.

Kaspersky Embedded Systems 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*.

Wenn Sie die Protokollanalyse verwenden möchten, stellen Sie sicher, dass die Sicherheitsüberwachungsrichtlinie konfiguriert ist und das System die relevanten Ereignisse protokolliert (Einzelheiten finden Sie in der Website des Technischen Supports von Microsoft.).

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.

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 mehrere Regeln, die von Kaspersky-Experten erstellt wurden.

So fügen Sie eine benutzerdefinierte Regel hinzu (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **System-Inspektion** aus.

4. Klicken Sie im Abschnitt **Protokollanalyse** auf **Einstellungen**.

5. Aktivieren Sie das Kontrollkästchen **Protokollanalyse**.

6. Aktivieren Sie auf der Registerkarte **Benutzerdefinierte Regeln** das Kontrollkästchen **Benutzerdefinierte Regeln zur Protokollanalyse anwenden**.

7. Aktivieren Sie die Kontrollkästchen neben den benutzerdefinierten Regeln, die Sie aktivieren möchten.

8. Klicken Sie ggf. auf **Hinzufügen**, um Ihre eigenen benutzerdefinierten Regeln zu erstellen.

9. 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.

10. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine benutzerdefinierte Regel hinzu (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **System-Inspektion → Protokollanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Aktivieren Sie das Kontrollkästchen **Protokollanalyse aktivieren**.

6. Aktivieren Sie auf der Registerkarte **Benutzerdefinierte Regeln** das Kontrollkästchen **Benutzerdefinierte Regeln zur Protokollanalyse anwenden**.

7. Konfigurieren Sie die benutzerdefinierten Regeln mithilfe der Schalter:

8. Klicken Sie ggf. auf **Hinzufügen**, um Ihre eigenen benutzerdefinierten Regeln zu erstellen.

9. Dadurch wird ein Fenster geöffnet. Konfigurieren Sie in diesem Fenster die benutzerdefinierte Regel:

   - **Regelname**.

   - **Name des Windows-Ereignisprotokolls**. 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.

10. Speichern Sie die vorgenommenen Änderungen.

So fügen Sie eine benutzerdefinierte Regel hinzu (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **System-Inspektion** → **Protokollanalyse** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Protokollanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Protokollanalyse** geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Protokollanalyse**.

4. Aktivieren Sie auf der Registerkarte **Benutzerdefinierte Regeln** das Kontrollkästchen **Benutzerdefinierte Regeln zur Protokollanalyse anwenden**.

5. Aktivieren Sie die Kontrollkästchen neben den 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-IDs**. 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 Embedded Systems Security ein *Kritisch* Ereignis.

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 Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **System-Inspektion** aus.
4. Klicken Sie im Abschnitt **Protokollanalyse** auf **Einstellungen**.
5. Aktivieren Sie das Kontrollkästchen **Protokollanalyse**.
6. Aktivieren Sie auf der Registerkarte **Vordefinierte Regeln** das Kontrollkästchen **Vordefinierte Regeln zur Protokollanalyse anwenden**.
7. 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**.
8. Konfigurieren Sie ggf. die Regel **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**:
   a. Klicken Sie auf die Schaltfläche **Einstellungen** neben 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**.
9. 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** neben der Regel.
   b. Geben Sie im folgenden Fenster im Block **Erkennung von Netzwerkanmeldungen** den Beginn und das Ende des Intervalls ein.

Kaspersky Embedded Systems 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 Embedded Systems Security überwacht die Anmeldeversuche dieser Benutzer und Computer nicht.

> Das Ausschließen vertrauenswürdiger Computer anhand der IP-Adresse funktioniert im Programm unter Windows XP nicht.

d. Klicken Sie auf **OK**.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie vordefinierte Regeln (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **System-Inspektion** → **Protokollanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Aktivieren Sie das Kontrollkästchen **Protokollanalyse aktivieren**.
6. Aktivieren Sie auf der Registerkarte **Vordefinierte Regeln** das Kontrollkästchen **Vordefinierte Regeln zur Protokollanalyse anwenden**.
7. Konfigurieren Sie die vordefinierten Regeln mithilfe der Schalter:

   - **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**.
   - **Verdächtige Änderungen in der privilegierten integrierten Administratorgruppe wurden erkannt**.

8. Konfigurieren Sie auf der Registerkarte **Erweitert** die folgenden Einstellungen:

   - Anzahl der Versuche sowie Zeitraum, innerhalb dessen Versuche zur Eingabe eines Passworts erfolgen müssen, damit die Regel **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden** ausgelöst wird.

   - Geben Sie als Auslösebedingung für die Regel **Es wurde eine ungewöhnliche Aktivität während einer Netzwerkanmeldesitzung erkannt** den Beginn und das Ende des Zeitintervalls an, in dem das Programm alle Anmeldeversuche als abnormale Aktivität betrachten soll.

     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.

9. Erstellen Sie auf den entsprechenden Registerkarten die Liste der vertrauenswürdigen Benutzer und die Liste der vertrauenswürdigen IP-Adressen (IPv4 und IPv6).

   Sie können Benutzer aus der Liste mit Benutzerkonten auswählen oder einen lokalen Benutzernamen manuell eingeben.

   > Das Ausschließen vertrauenswürdiger Computer anhand der IP-Adresse funktioniert im Programm unter Windows XP nicht.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie vordefinierte Regeln (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **System-Inspektion → Protokollanalyse** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Protokollanalyse** auf **Eigenschaften**.

   Dadurch wird das Fenster **Eigenschaften: Protokollanalyse** geöffnet.

3. Aktivieren Sie das Kontrollkästchen **Protokollanalyse**.

4. Aktivieren Sie auf der Registerkarte **Vordefinierte Regeln** das Kontrollkästchen **Vordefinierte Regeln zur Protokollanalyse anwenden**.

5. 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**.

6. Konfigurieren Sie ggf. die Regel **Anzeichen eines Brute-Force-Angriffs wurden im System gefunden**:

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

7. 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** neben der Regel.

   b. Geben Sie im folgenden Fenster im Block **Erkennung von Netzwerkanmeldungen** den Beginn und das Ende des Intervalls ein.

   Kaspersky Embedded Systems 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. Erstellen Sie die Liste der Benutzer aus Active Directory. Kaspersky Embedded Systems Security überwacht die Anmeldeversuche dieser Benutzer und Computer nicht.

   > Das Ausschließen vertrauenswürdiger Computer anhand der IP-Adresse funktioniert im Programm unter Windows XP nicht.

   d. Klicken Sie auf **OK**.

8. Speichern Sie die vorgenommenen Änderungen.

Wenn die Regel ausgelöst wird, erstellt Kaspersky Embedded Systems Security daher ein *kritisches* Ereignis.

Untersuchung auf Befehl

Dieser Abschnitt enthält Informationen über die Aufgaben zur Untersuchung auf Befehl und erläutert das Anpassen der Aufgaben zur Untersuchung auf Befehl und der Sicherheitseinstellungen des geschützten Geräts.

Über Aufgaben zur Untersuchung auf Befehl

Kaspersky Embedded Systems Security untersucht den angegebenen Bereich auf Viren und andere Bedrohungen der Computersicherheit. Kaspersky Embedded Systems Security überprüft Daten des geschützten Geräts, den Arbeitsspeicher sowie Autostart-Objekte.

Kaspersky Embedded Systems Security enthält die folgenden Aufgaben zur Untersuchung auf Befehl:

- Die Aufgabe *Untersuchung wichtiger Bereiche* wird standardmäßig wöchentlich nach Zeitplan ausgeführt. Kaspersky Embedded Systems Security untersucht Objekte, die sich in kritischen Bereichen des Betriebssystems befinden: Autostart-Objekte, Bootsektoren und Master-Bootsektoren von Festplatten und Wechseldatenträgern, Systemspeicher und Prozess-Speicher. Kaspersky Embedded Systems Security verwendet die Sicherheitseinstellungen, die der Stufe **Inform** entsprechen. Sie können die Parameter für die Aufgabe *Untersuchung wichtiger Bereiche* ändern.

- Die Aufgabe *Kontrolle der Anwendungsintegrität* wird täglich ausgeführt. Sie gewährleistet die Untersuchung der Module von Kaspersky Embedded Systems Security auf Beschädigungen oder Änderungen. Es wird der Installationsordner des Programms geprüft. Die Statistiken über die Aufgabenausführung geben Auskunft über die Anzahl der geprüften Module und die Anzahl der als beschädigt bewerteten Module. Die Parameterwerte einer Aufgabe werden vom Programm vorgegeben und lassen sich nicht ändern. Die Einstellungen im Zeitplan für den Aufgabenstart lassen sich dagegen für so eine Aufgabe ändern.

- Die Aufgabe zur *Untersuchung von Wechseldatenträgern* untersucht alle Dateien, die Sie ausführen oder kopieren, selbst wenn sich eine Datei auf einem Wechseldatenträger befindet. 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.

- Die Aufgabe *Vollständige Untersuchung* wird wöchentlich ausgeführt. Diese Aufgabe gewährleistet eine gründliche Untersuchung des geschützten Geräts, einschließlich des System-Backup-Speichers, der Bootsektoren und der Mail-Datenbanken.

Zusätzlich können Sie benutzerdefinierte Aufgaben zur Untersuchung auf Befehl erstellen, beispielsweise eine Aufgabe zur Untersuchung freigegebener Ordner auf dem geschützten Gerät.

Kaspersky Embedded Systems Security kann gleichzeitig mehrere Aufgaben zur Untersuchung auf Befehl ausführen.

Über den Untersuchungsbereich von Aufgaben und Sicherheitseinstellungen

In der Anwendungskonsole wird der Untersuchungsbereich der ausgewählten Aufgabe zur Untersuchung auf Befehl als eine Liste der geschützten Geräte-Dateiressourcen angezeigt, die Kaspersky Embedded Systems Security kontrollieren kann.

Die Elemente oder Knoten werden als Listenansicht der Dateiressourcen des geschützten Geräts wie folgt dargestellt:

☑ Der Knoten gehört zum Untersuchungsbereich.

☐ Der Knoten gehört nicht zum Untersuchungsbereich.

Parameter für Sicherheit

In der ausgewählten Aufgabe zur Untersuchung auf Befehl können Sie die standardmäßigen Sicherheitseinstellungen ändern. Dabei können Sie entweder einheitliche Werte für den gesamten Schutzbereich bzw. Untersuchungsbereich oder individuelle Werte für bestimmte Knoten oder Elemente in der Liste der Geräteressourcen festlegen.

> Wenn dasselbe Objekt in mehreren Schutzbereichseinträgen enthalten ist und diese Einträge unterschiedliche Sicherheitsstufen haben, ist die letzte Regel in der Liste vorrangig. Stellen Sie sich beispielsweise einen Schutzbereich vor, der zwei Einträge enthält: **Alle Festplatten** (Sicherheitsstufe **Inform**) und `*\Users\*\Downloads\*` (Sicherheitsstufe **Custom**). Das Programm untersucht Festplatten mit der Stufe „Informieren", unter Ausnahme des Ordners `Downloads`. Das Programm untersucht den Ordner `Downloads` nach den manuell festgelegten Einstellungen, da dieser Eintrag in der Liste der Schutzbereiche an letzter Stelle steht.

Die Sicherheitseinstellungen, die für den ausgewählten übergeordneten Knoten konfiguriert wurden, werden automatisch für alle untergeordneten Knotens übernommen. Die Sicherheitseinstellungen des übergeordneten Knotens werden für untergeordnete Knoten, die gesondert konfiguriert werden, nicht übernommen.

Sie können die Parameter eines ausgewählten Schutzbereichs bzw. Untersuchungsbereichs auf eine der folgenden Weisen anpassen:

- Durch Auswahl einer der drei vordefinierten Sicherheitsstufen (**Maximale Leistung**, **Empfohlen** oder **Maximaler Schutz**).
- Durch manuelle Änderung der Sicherheitseinstellungen für die ausgewählten Knoten oder Elemente in der Liste der Dateiressourcen des geschützten Geräts (die Sicherheitsstufe ändert sich in **Benutzerdefiniert**).

Vordefinierte Untersuchungsbereiche

Die Liste der Dateiressourcen des geschützten Geräts für die ausgewählte Aufgabe zur Untersuchung auf Befehl wird im Fenster **Untersuchungsbereich** angezeigt.

> Die Liste der Dateiressourcen enthält die Knoten, für die Sie gemäß den Microsoft Windows-Sicherheitseinstellungen über Leserechte verfügen.

Kaspersky Embedded Systems Security enthält die folgenden vordefinierten Untersuchungsbereiche:

- **Alle Festplatten**. Kaspersky Embedded Systems Security untersucht Objekte auf den Festplatten des geschützten Geräts. Sie können alle Festplatten sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.

- **Alle Wechseldatenträger**. Kaspersky Embedded Systems Security untersucht Dateien auf externen Geräten, z. B. auf CDs oder Wechseldatenträgern. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.

- **Alle Netzlaufwerke**. Sie können dem Untersuchungsbereich Netzwerkordner oder Dateien hinzufügen, indem Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) angeben. Das für den Aufgabenstart verwendete Benutzerkonto muss über Zugriffsrechte für die hinzugefügten Netzwerkordner oder Dateien verfügen. Standardmäßig werden die Aufgaben zur Untersuchung auf Befehl unter dem Systemkonto ausgeführt.

  Verbundene Netzlaufwerke werden nicht in der Dateistruktur des geschützten Geräts angezeigt. Um Objekte auf einem Netzlaufwerk in den Untersuchungsbereich aufzunehmen, geben Sie den Pfad des Ordners an, der dem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

- **Kernel-Speicher**. Kaspersky Embedded Systems Security untersucht ausführbare Dateien und Module von Prozessen, die während der Untersuchung im Betriebssystem ausgeführt werden.

- **Aktive Prozesse und Autostart-Objekte**. Kaspersky Embedded Systems Security untersucht Objekte, auf die sich Registrierungsschlüssel und Konfigurationsdateien beziehen, beispielsweise WIN.INI oder SYSTEM.INI, sowie die Programm-Module, die beim Hochfahren des geschützten Geräts automatisch gestartet werden.

- **Laufwerksbootsektoren**. Kaspersky Embedded Systems Security untersucht die Bootsektoren von Festplatten und Wechseldatenträgern.

- **System-Backup**. Kaspersky Embedded Systems Security untersucht den Inhalt des Ordners „System Volume Information“.

  In Kaspersky Embedded Systems Security 4.1 sind E-Mail-Nachrichten aus dem Untersuchungsbereich des Programms ausgeschlossen. 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.

Standardmäßige Untersuchungsbereiche werden standardmäßig in der Struktur der Netzwerkdateiressourcen angezeigt. Sie können bei der Erstellung in den Einstellungen des Untersuchungsbereichs zur Liste der Ressourcen für Netzwerkdateien hinzugefügt werden.

Standardmäßig werden die Aufgaben zur Untersuchung auf Befehl in den folgenden Bereichen ausgeführt:

- Aufgabe für die *Untersuchung wichtiger Bereiche*:

  - **Alle Festplatten** (unter Ausnahme von Windows-Ordnern)

  - **Alle Wechseldatenträger**.

- **Kernel-Speicher**.
- **Aktive Prozesse und Autostart-Objekte**.

- Aufgabe für die *Untersuchung auf Befehl*:
  - **Alle Festplatten** (unter Ausnahme von Windows-Ordnern)
  - **Alle Wechseldatenträger**.
  - **Kernel-Speicher**.
  - **Aktive Prozesse und Autostart-Objekte**.
- Aufgabe für die *Vollständige Untersuchung*:
  - **Alle Festplatten** (unter Ausnahme von Windows-Ordnern)
  - **Alle Wechseldatenträger**.
  - **Kernel-Speicher**.
  - **Aktive Prozesse und Autostart-Objekte**.
  - **System-Backup**.
  - **Laufwerksbootsektoren**.

Untersuchung von Dateien im Online-Speicher

Über Cloud-Dateien

Kaspersky Embedded Systems Security kann mit Dateien in der Microsoft OneDrive Cloud interagieren. Das Programm unterstützt die neue Funktion OneDrive Files On-Demand.

> Kaspersky Embedded Systems Security unterstützt keine anderen Online-Speicher.

OneDrive Files On-Demand ermöglicht Ihnen den Zugriff auf all Ihre OneDrive-Dateien, ohne dass sie heruntergeladen werden müssen und Speicherplatz auf Ihrem Gerät belegen. Sie können die Dateien bei Bedarf auf Ihre Festplatte herunterladen.

Wenn die Funktion "OneDrive Files On-Demand" aktiviert ist, werden im Datei-Explorer neben jeder Datei in der Spalte **Status** Statussymbole angezeigt. Jede Datei besitzt eine der folgenden Statusvarianten:

Dieses Statussymbol zeigt an, dass die Datei *nur online verfügbar* ist. Dateien, die nur online verfügbar sind, werden nicht physisch auf Ihrer Festplatte gespeichert. Sie können solche Dateien nicht öffnen, wenn Ihr Gerät keine Internetverbindung hat.

Dieses Statussymbol zeigt an, dass die Datei *lokal verfügbar* ist. Dies ist der Fall, wenn Sie eine nur online verfügbare Datei öffnen und auf Ihr Gerät herunterladen. Sie können eine lokal verfügbare Datei jederzeit auch ohne Internetzugang öffnen. Um Speicherplatz freizugeben, können Sie die Datei wieder nur online verfügbar machen ( ).

Dieses Statussymbol zeigt an, dass die Datei *auf Ihrer Festplatte gespeichert und immer verfügbar* ist.

Untersuchung von Cloud-Dateien

Kaspersky Embedded Systems Security kann nur Cloud-Dateien untersuchen, die lokal auf einem geschützten Gerät gespeichert sind. Solche OneDrive-Dateien besitzen die Status und . Die Dateien mit dem Status werden bei der Untersuchung übersprungen, da sie sich nicht physisch auf dem geschützten Gerät befinden.

> Kaspersky Embedded Systems Security lädt Dateien mit dem Status während der Untersuchung nicht automatisch aus der Cloud herunter, selbst wenn sie zum Untersuchungsbereich gehören.

Cloud-Dateien werden je nach Aufgabetyp von mehreren Aufgaben von Kaspersky Embedded Systems Security in unterschiedlichen Szenarien verarbeitet:

- Untersuchung von Cloud-Dateien in Echtzeit: Sie können Ordner mit Cloud-Dateien zum Schutzbereich der Aufgabe „Echtzeitschutz für Dateien“ hinzufügen. Eine Datei wird untersucht, wenn der Benutzer auf sie zugreift. Wenn der Benutzer auf eine Datei mit dem Status zugreift, wird sie heruntergeladen und lokal verfügbar gemacht und ihr Status wechselt zu . Dann kann die Datei durch die Komponente Echtzeitschutz für Dateien bearbeitet werden.

- Untersuchung von Cloud-Dateien auf Befehl: Sie können Ordner mit Cloud-Dateien zum Untersuchungsbereich der Aufgabe zur Untersuchung auf Befehl hinzufügen. Die Aufgabe untersucht Dateien mit dem Status und . Wenn Dateien mit dem Status im Untersuchungsbereich gefunden werden, werden sie bei der Untersuchung übersprungen. Im Protokoll der Aufgabenausführung wird ein informatives Ereignis gespeichert, das darauf hinweist, dass die untersuchte Datei nur ein Platzhalter für eine Cloud-Datei ist und nicht auf einer lokalen Festplatte verfügbar ist.

- Generierung und Verwendung von Regeln für die Kontrolle des Programmstarts: Mit der Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* können Sie Erlaubnisregeln und Verbotsregeln für die Dateien mit dem Status und erstellen. Die Komponente „Kontrolle des Programmstarts“ wendet das Prinzip des standardmäßigen Verbots (Default Deny) an und erstellt Regeln zum Verarbeiten und Blockieren von Cloud-Dateien.

  > Die Komponente „Kontrolle des Programmstarts“ blockiert den Start aller Cloud-Dateien unabhängig von ihrem Status. Dateien mit dem Status werden nicht in den Gültigkeitsbereich der Erstellung von Regeln aufgenommen, da sie nicht physisch auf Ihrer Festplatte gespeichert sind. Da für solche Dateien keine Erlaubnisregeln erstellt werden können, gilt für sie das Prinzip des standardmäßigen Verbots (Default Deny).

Wenn in einer OneDrive Cloud-Datei eine Bedrohung gefunden wird, wendet das Programm die Aktion an, die in den Einstellungen der Aufgabe festgelegt ist, welche die Untersuchung ausführt. Auf diese Weise kann die Datei gelöscht, desinfiziert, in Quarantäne oder ins Backup verschoben werden.

Änderungen an lokalen Dateien werden mit den in OneDrive gespeicherten Kopien synchronisiert, wobei die Prinzipien zur Anwendung kommen, die in der entsprechenden Dokumentation zu Microsoft OneDrive beschrieben sind.

Über vordefinierte Sicherheitsstufen

Die Sicherheitseinstellung **Heuristische Analyse verwenden** gehört nicht zu den Einstellungen für die vordefinierten Sicherheitsstufen. Wenn Sie diese Einstellung ändern, wird die von Ihnen ausgewählte Standardsicherheitsstufe nicht geändert.

Sie können eine der folgenden vier vordefinierten Sicherheitsstufen für einen in der Struktur der Geräte-Dateiressourcen ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen**, **Maximaler Schutz** oder **Informieren**. Jede dieser Stufen besitzt eigene vordefinierte Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird empfohlen, wenn Ihr Netzwerk über zusätzliche Sicherheitsmaßnahmen verfügt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien, die über die Verwendung von Kaspersky Embedded Systems Security auf geschützten Geräten und Workstations hinausgehen.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Geräte. Die Experten von Kaspersky empfehlen diese Stufe als ausreichenden Schutz von Geräten in den meisten Unternehmensnetzwerken. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximaler Schutz

Die Sicherheitsstufe **Maximaler Schutz** wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Gerätesicherheit hat.

Informieren

Die Sicherheitsstufe **Informieren** wird empfohlen, wenn sich im Unternehmensnetzwerk möglicherweise viele infizierte Computer befinden und deren Blockierung den Betrieb des Unternehmens erheblich stören könnte.

Vordefinierte Sicherheitsstufen und entsprechende Werte für die Sicherheitsparameter

Einstellungen	Sicherheitsstufe			
	Maximale Leistung	Empfohlen	Maximaler Schutz	Informieren
Object types	Objekte, die nach Format untersucht werden	Alle Objekte	Alle Objekte	Alle Objekte
Scan only new and modified files	Aktiviert	Deaktiviert	Deaktiviert	Deaktiviert

Einstellungen	Sicherheitsstufe			
	Maximale Leistung	Empfohlen	Maximaler Schutz	Informieren
Action to perform on infected and other objects	Desinfizieren. Löschen, wenn Desinfektion fehlschlägt	Führen Sie die von Kaspersky-Experten empfohlene Aktion aus	Desinfizieren. Löschen, wenn Desinfektion fehlschlägt	Informieren
Scan of compound files	Untersuchung von Programmpaketen und Dateien in Microsoft Office-Formaten	Untersuchung aller Archive, Programmpakete und Dateien in den Microsoft Office-Formaten	Untersuchung aller Archive, Programmpakete und Dateien in den Microsoft Office-Formaten	Untersuchung aller Archive, Programmpakete und Dateien in den Microsoft Office-Formaten
Systemkritische Objekte sind Dateien, die für die Ausführung des Betriebssystems und von Kaspersky Embedded Systems Security erforderlich sind. Diese Dateien können nicht gelöscht werden. Prozesse, die mit solchen Objekten verknüpft sind, können nicht beendet werden.				
Aktion auf die ausgewählten Objekttypen anwenden	Standardmäßig werden alle Objekttypen untersucht	Standardmäßig werden alle Objekttypen untersucht	Standardmäßig werden alle Objekttypen untersucht	Standardmäßig werden alle Objekttypen untersucht
Entirely remove the compound file that cannot be modified by the application in case of embedded object detection	Nein	Nein	Nein	Nein
Dateien ausschließen	Nein	Nein	Nein	Nein
Do not detect objects by type	Nein	Nein	Nein	Nein
Stop scanning if it takes longer than (sec)	60 Sek.	Nein	Nein	Nein
Do not scan compound objects larger than (MB)	8 MB	Nein	Nein	Nein
iSwift-Technologie verwenden	Ja	Ja	Ja	Ja
iChecker-Technologie verwenden	Ja	Ja	Ja	Ja

Untersuchung von Wechseldatenträgern

Sie können die Untersuchung von Wechseldatenträgern anpassen, die über USB an das geschützte Gerät angeschlossen werden.

Kaspersky Embedded Systems Security startet die Untersuchung von Wechseldatenträgern, wenn diese im Betriebssystem als externe USB-Geräte registriert werden. Das Programm führt keine Untersuchung des Wechseldatenträgers durch, wenn sein Anschluss von der Aufgabe zur Gerätekontrolle blockiert wird.

Kaspersky Embedded Systems Security erlaubt den Zugriff auf Wechseldatenträger während der Untersuchung.

Die Ergebnisse der Untersuchung jedes Wechseldatenträgers werden im Protokoll der Aufgabe zur Untersuchung auf Befehl gespeichert, wenn der jeweilige Datenträger angeschlossen wird.

Sie können die Einstellungswerte der Komponente Untersuchung von Wechseldatenträgern bearbeiten (s. Tabelle unten).

Einstellungen für die Untersuchung von Wechseldatenträgern

Einstellung	Standardwert	Beschreibung
Wechseldatenträger bei USB-Verbindung untersuchen	Deaktiviert	Sie können die Untersuchung von Wechseldatenträgern, die über USB an das geschützte Gerät angeschlossen werden, aktivieren und deaktivieren.
Wechseldatenträger untersuchen, maximale Größe (MB)	4096 MB	Sie können den Bereich, in dem die Komponente aktiviert wird, reduzieren, indem Sie die Höchstmenge der Daten auf dem Wechseldatenträger angeben. Kaspersky Embedded Systems Security wird einen Wechseldatenträger nicht untersuchen, wenn die Menge der darauf gespeicherten Daten den angegebenen Wert übersteigt.
Untersuchen mit Sicherheitsstufe	Maximale Sicherheit	Sie können die Einstellungen der zu erstellenden Aufgaben zur Untersuchung auf Befehl anpassen, indem Sie eine der folgenden drei Sicherheitsstufen wählen: • **Maximaler Schutz** • **Empfohlen** • **Maximale Leistung** • **Informieren**. Der Algorithmus der Aktionen beim Entdecken infizierter, möglicherweise infizierter und anderer Objekte, sowie andere Untersuchungseinstellungen für jede Sicherheitsstufe entsprechen den vorinstallierten Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl.

Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl

Die Standardeinstellungen von Aufgaben zur Untersuchung auf Befehl werden in folgender Tabelle beschrieben. Lokale Systemaufgaben und benutzerdefinierte Aufgaben zur Untersuchung auf Befehl lassen sich konfigurieren.

Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl

Einstellung	Standardwert	Beschreibung
Untersuchungsbereich	Wird in den folgenden lokalen Systemaufgaben und benutzerdefinierten Aufgaben verwendet: • **Untersuchung wichtiger Bereiche**: das gesamte geschützte Gerät mit Ausnahme der freigegebenen Ordner und einiger Dateien des Betriebssystems. • **Untersuchung auf Befehl** (benutzerdefinierte Aufgabe): das gesamte geschützte Gerät. • **Vollständige Untersuchung**: ausführliche Untersuchung des geschützten Geräts.	Sie können den Untersuchungsbereich ändern. Der Untersuchungsbereich für die lokalen Systemaufgaben zur **Untersuchung von Wechseldatenträgern** und **Kontrolle der Anwendungsintegrität** kann nicht konfiguriert werden.
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Für die ausgewählten Knoten können Sie in der Liste der Dateiressourcen des geschützten Geräts folgende Aktionen ausführen: • eine andere vordefinierte Sicherheitsstufe auswählen • die Sicherheitseinstellungen manuell ändern
Heuristische Analyse verwenden	Angewendet mit der Analysestufe **Mittel** für die Aufgaben *Untersuchung wichtiger Bereiche*, *Untersuchung auf Befehl* und *Vollständige Untersuchung*.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
Einstellungen zum Start der Aufgabe mit spezifischen Rechten	Die Aufgabe wird mit den Rechten des Systemkontos gestartet.	Sie können Einstellungen für den Start mit Berechtigungen spezieller Benutzerkonten für alle Systemaufgaben und benutzerdefinierten Aufgaben zur Untersuchung auf Befehl ändern, unter Ausnahme der Aufgabe „*Kontrolle der Anwendungsintegrität*“.
Aufgabe im Hintergrundmodus ausführen	Wird nicht verwendet	Sie können die Priorität der Aufgaben für die Untersuchung auf Befehl festlegen.

Einstellung	Standardwert	Beschreibung
Aufgabe als Untersuchung wichtiger Bereiche betrachten	Angewendet für die Aufgaben *Untersuchung auf Befehl*, *Untersuchung wichtiger Bereiche* und *Vollständige Untersuchung*.	Sie können die Priorität der Aufgaben für die Untersuchung auf Befehl festlegen.
Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen	Wird nicht verwendet	Sie können die Priorität der Aufgaben für die Untersuchung auf Befehl festlegen.
Zeitplan für den Aufgabenstart	Angewendet in lokalen Systemaufgaben: *Untersuchung wichtiger Bereiche*, *Kontrolle der Anwendungsintegrität* und *Vollständige Untersuchung* – **Monatlich**.	Sie können die Einstellungen für die Ausführung von geplanten Aufgaben anpassen.

Aufgaben zur Untersuchung auf Befehl verwalten

In diesem Abschnitt wird beschrieben, wie die Aufgabe *Untersuchung auf Befehl* auf dem geschützten Gerät erstellt und konfiguriert wird.

Erstellen einer Aufgabe zur Untersuchung auf Befehl

Aufgabe zur Untersuchung auf Befehl erstellen (in der Kaspersky Security Center-Verwaltungskonsole)

1. Starten Sie den Assistenten für neue Aufgaben.
2. Wählen Sie im Fenster **Aufgabentyp auswählen** den Punkt **Untersuchung auf Befehl** aus und klicken Sie auf **Weiter**.
3. Erstellen Sie im Fenster **Untersuchungsbereich** einen Untersuchungsbereich:

   Standardmäßig gehören zum Untersuchungsbereich wichtige Bereiche des geschützten Geräts. Untersuchungsbereiche sind in der Tabelle mit dem Symbol ☑ gekennzeichnet. Bereiche, die vom Untersuchungsbereich ausgenommen sind, werden in der Tabelle mit dem Symbol ☐ markiert. Sie können den Untersuchungsbereich ändern: Einzelne vordefinierte Bereiche, Datenträger, Ordner, Netzwerkobjekte oder Dateien in den Untersuchungsbereich aufnehmen und individuelle Sicherheitseinstellungen für die hinzugefügten Bereiche festlegen.

   - Um einen Bereich von der Untersuchung auszuschließen, wählen Sie das entsprechende Listenelement aus und klicken Sie auf **Löschen**.
   - Um einen vordefinierten Untersuchungsbereich, ein Laufwerk, einen Ordner, ein Netzwerkobjekt oder eine Datei zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

     a. Klicken Sie auf **Hinzufügen**.

     b. Wählen Sie im Fenster **Untersuchungsbereich auswählen** den vordefinierten Untersuchungsbereich aus der Liste aus und klicken Sie auf **OK**.

- So schließen Sie Unterordner oder Dateien vom Untersuchungsbereich aus:

  a. Wählen Sie im Fenster **Untersuchungsbereich** einen hinzugefügten Ordner (oder Datenträger) aus.

  b. Klicken Sie auf **Ändern**.

  c. Deaktivieren Sie das Kontrollkästchen **Unterordner einschließen**.

- Um die Sicherheitseinstellungen des Untersuchungsbereichs zu ändern, gehen Sie wie folgt vor:

  a. Wählen Sie den Untersuchungsbereich aus, dessen Einstellungen Sie ändern möchten, und klicken Sie auf **Konfigurieren**.

  b. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster eine der vordefinierten Sicherheitsstufen aus oder klicken Sie auf die Schaltfläche **Einstellungen**, um die Sicherheitseinstellungen manuell zu konfigurieren.

  Die Sicherheitseinstellungen werden auf die gleiche Weise wie bei der Aufgabe Echtzeitschutz für Dateien konfiguriert.

4. Konfigurieren Sie die heuristische Analyse und die Integration in andere Komponenten:

   - Konfigurieren Sie die Verwendung der heuristischen Analyse.

   - Aktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**, wenn Sie dem Arbeitsprozess, in dem die Aufgabe ausgeführt wird, die Priorität *Niedrig* zuweisen möchten.

     Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

   - Aktivieren Sie das Kontrollkästchen **Aufgabe als Untersuchung wichtiger Bereiche betrachten**, wenn Sie die Aufgabe als Aufgabe zur *Untersuchung wichtiger Bereiche* verwenden möchten.

   - Aktivieren Sie das Kontrollkästchen **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**, um die Auslastung des Computers zu optimieren.

5. Geben Sie im Fenster **Geräte auswählen, denen die Aufgabe zugewiesen wird** die Liste der Geräte an und klicken Sie auf **Weiter**.

6. Geben Sie im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** ein Benutzerkonto an und klicken Sie auf **Weiter**.

7. Konfigurieren Sie im Fenster **Aufgabenzeitplan anpassen** den Aufgabenzeitplan und klicken Sie auf **Weiter**.

8. Geben Sie einen Namen für die Aufgabe ein.

   Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

9. Das Fenster **Erstellung der Aufgabe abschließen** wird geöffnet. Klicken Sie auf die Schaltfläche **Fertig**, um die Erstellung der Aufgabe fertigzustellen.

Die neue Aufgabe zur *Untersuchung auf Befehl* wird für das ausgewählte geschützte Gerät oder eine Gruppe von geschützten Geräten erstellt.

Aufgabe zur Untersuchung auf Befehl erstellen (in der Kaspersky Security Center Web Console)

1. Starten Sie den Assistenten für neue Aufgaben.
2. Wählen Sie im Fenster **Neue Aufgabe** in der Dropdown-Liste **Anwendung** den Punkt **Kaspersky Embedded Systems Security** aus.
3. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Punkt **Untersuchung auf Befehl** aus und klicken Sie auf **Weiter**.
4. Wählen Sie den Aufgabenbereich aus und klicken Sie auf **Weiter**.
5. Geben Sie im Fenster **Benutzerkonto für die Ausführung der Aufgabe auswählen** ein Benutzerkonto an und klicken Sie auf **Weiter**.
6. Geben Sie einen Namen für die Aufgabe ein.

   Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |
7. Das Fenster **Erstellung der Aufgabe abschließen** wird geöffnet. Klicken Sie auf die Schaltfläche **Fertig**, um die Erstellung der Aufgabe fertigzustellen.

Die neue Aufgabe zur *Untersuchung auf Befehl* wird für das ausgewählte geschützte Gerät oder eine Gruppe von geschützten Geräten erstellt.

Aufgabe „Untersuchung auf Befehl“ erstellen (in der Anwendungskonsole)

Sie können im Knoten **Untersuchung auf Befehl** benutzerdefinierte Aufgaben für ein einzelnes geschütztes Gerät erstellen.

Um eine neue Aufgabe zur Untersuchung auf Befehl zu erstellen und anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Untersuchung auf Befehl**.
2. Wählen Sie die Option **Aufgabe erstellen** aus.

   Das Fenster **Aufgabe erstellen** wird geöffnet.
3. Geben Sie einen Namen für die Aufgabe ein und klicken Sie auf **OK**.

Die Aufgabe „*Untersuchung auf Befehl*“ wird für ein einzelnes geschütztes Gerät erstellt.

Ausführung einer Aufgabe im Hintergrund zur Untersuchung auf Befehl

Prozesse, in denen Aufgaben von Kaspersky Embedded Systems Security ausgeführt werden, besitzen die Priorität *Mittel (Normal)*.

Sie können einem Prozess, in dem eine Aufgabe zur *Untersuchung auf Befehl* ausgeführt wird, die Priorität *Niedrig* (Low) zuweisen. Wenn die Priorität eines Prozesses gesenkt wird, erhöht sich dadurch die Ausführungsdauer der Aufgabe und die Leistung der Prozesse anderer aktiver Anwendungen wird gesteigert.

In einem aktiven Prozess mit niedriger Priorität können mehrere Aufgaben im Hintergrundmodus ausgeführt werden.

Um die Priorität einer vorhandenen Aufgabe zur *Untersuchung auf Befehl* zu ändern, aktivieren oder deaktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen** in den Aufgabeneinstellungen.

Die Einstellungen der Aufgabe werden gespeichert und unverzüglich auf eine ausgeführte Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Registrierung der Ausführung der Untersuchung wichtiger Bereiche

Standardmäßig wird der Schutzstatus des Geräts im Ergebnisbereich des Knotens **Kaspersky Embedded Systems Security** angezeigt und wöchentlich nach Abschluss der Aufgabe *Untersuchung wichtiger Bereiche* aktualisiert.

Der Zeitpunkt, zu dem der Schutzstatus des Geräts aktualisiert wird, ist mit dem Zeitplan der Aufgabe zur Untersuchung auf Befehl verknüpft, für die das Kontrollkästchen **Aufgabe als Untersuchung wichtiger Bereiche betrachten** aktiviert ist.

Untersuchungsbereich für die Aufgabe „Untersuchung auf Befehl“ konfigurieren

Wenn Sie den Untersuchungsbereich in den Aufgaben „*Untersuchung beim Start des Betriebssystems*“ und „*Untersuchung wichtiger Bereiche*“ geändert haben, können Sie den standardmäßigen Untersuchungsbereich für diese Aufgaben wiederherstellen. Verwenden Sie dafür den Setup-Assistenten.

Untersuchungsbereich für die Aufgabe „Untersuchung auf Befehl“ konfigurieren (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
4. Wechseln Sie zum Abschnitt **Aufgaben**.
5. Doppelklicken Sie, um das Eigenschaftenfenster der Aufgabe **Untersuchung auf Befehl** zu öffnen.
6. Wählen Sie den Abschnitt **Untersuchungsbereich** aus.
7. Um dem Untersuchungsbereich weitere Bereiche hinzuzufügen, aktivieren Sie die entsprechenden Kontrollkästchen.

8. So fügen Sie einen Untersuchungsbereich hinzu, der nicht auf der Liste steht:

    a. Klicken Sie auf **Hinzufügen**.

    b. Wählen Sie im angezeigten Fenster einen Bereich, eine einzelne Festplatte, einen Ordner oder einen Netzwerkspeicherort aus.

    c. Wenn Sie Unterordner in den Untersuchungsbereich aufnehmen möchten, aktivieren Sie das Kontrollkästchen **Unterordner einschließen**.

9. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten.

10. Um einen Untersuchungsbereich zu bearbeiten, wählen Sie den Untersuchungsbereich in der Liste aus und klicken Sie auf **Bearbeiten**.

11. Um einen bereits hinzugefügten Untersuchungsbereich aus der Liste der Ressourcen für Netzwerkdateien zu auszublenden, wählen Sie den Untersuchungsbereich aus und klicken Sie auf **Löschen**.

    Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

12. Klicken Sie auf **OK**.

Das Fenster Untersuchungsbereich - Einstellungen wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Untersuchungsbereich für die Aufgabe „Untersuchung auf Befehl“ konfigurieren (in der Kaspersky Security Center 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 Aufgabe konfigurieren möchten.

3. Wählen Sie den Abschnitt **Aufgaben** aus.

4. Dadurch wird ein Fenster geöffnet. Doppelklicken Sie in diesem Fenster, um die Eigenschaften der Aufgabe **Untersuchung auf Befehl** zu öffnen.

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

6. Um dem Untersuchungsbereich weitere Bereiche hinzuzufügen, aktivieren Sie die entsprechenden Schalter.

7. So fügen Sie einen Untersuchungsbereich hinzu, der nicht auf der Liste steht:

    a. Klicken Sie auf **Hinzufügen**.

    b. Wählen Sie im angezeigten Fenster einen Bereich, eine einzelne Festplatte, einen Ordner oder einen Netzwerkspeicherort aus.

    c. Wenn Sie Unterordner in den Untersuchungsbereich aufnehmen möchten, aktivieren Sie das Kontrollkästchen **Unterordner**.

8. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten.

9. Um einen Untersuchungsbereich zu bearbeiten, wählen Sie den Untersuchungsbereich in der Liste aus und klicken Sie auf **Bereich bearbeiten**.

10. Um einen bereits hinzugefügten Untersuchungsbereich aus der Liste der Ressourcen für Netzwerkdateien zu auszublenden, wählen Sie den Untersuchungsbereich aus und klicken Sie auf **Löschen**.

    Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

11. Klicken Sie auf **Speichern**.

Das Fenster Untersuchungsbereich - Einstellungen wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Untersuchungsbereich für die Aufgabe „Untersuchung auf Befehl“ konfigurieren (in der Anwendungskonsole)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe zur Untersuchung auf Befehl entspricht, deren Einstellungen Sie konfigurieren möchten.

3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf den Link **Schutzbereich konfigurieren**.

4. Um dem Untersuchungsbereich weitere Bereiche hinzuzufügen, aktivieren Sie im angezeigten Fenster die entsprechenden Kontrollkästchen.

5. So fügen Sie einen Untersuchungsbereich hinzu, der nicht auf der Liste steht:

   a. Klicken Sie auf **Hinzufügen**.

   b. Wählen Sie im angezeigten Fenster einen Bereich, eine einzelne Festplatte, einen Ordner oder einen Netzwerkspeicherort aus.

   c. Wenn Sie Unterordner in den Untersuchungsbereich aufnehmen möchten, aktivieren Sie das Kontrollkästchen **Unterordner einschließen**.

6. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten.

7. Um einen Untersuchungsbereich zu bearbeiten, wählen Sie den Untersuchungsbereich in der Liste aus und klicken Sie auf **Bereich bearbeiten**.

8. Um einen bereits hinzugefügten Untersuchungsbereich aus der Liste der Ressourcen für Netzwerkdateien zu auszublenden, wählen Sie den Untersuchungsbereich aus und klicken Sie auf **Löschen**.

   Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

9. Klicken Sie auf **OK**.

Das Fenster Untersuchungsbereich - Einstellungen wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Einstellungen für die Aufgabe „Untersuchung auf Befehl“ konfigurieren

So konfigurieren Sie die Aufgabe Untersuchung auf Befehl (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
4. Wechseln Sie zum Abschnitt **Aufgaben**.
5. Doppelklicken Sie, um das Eigenschaftenfenster der Aufgabe **Untersuchung auf Befehl** zu öffnen.
6. Wählen Sie den Abschnitt **Optionen** aus.
7. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.
8. Ändern Sie bei Bedarf die Analysestufe.
9. Aktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**, wenn Sie dem Arbeitsprozess, in dem die Aufgabe ausgeführt wird, die Priorität *Niedrig* zuweisen möchten.

   Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

10. Aktivieren Sie das Kontrollkästchen **Aufgabe als Untersuchung wichtiger Bereiche betrachten**, wenn Sie die Aufgabe als Aufgabe zur *Untersuchung wichtiger Bereiche* verwenden möchten.
11. Aktivieren Sie das Kontrollkästchen **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**, um die Auslastung des Computers zu optimieren.
12. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Aufgabe Untersuchung auf Befehl (in der Kaspersky Security Center 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 Aufgabe konfigurieren möchten.
3. Wählen Sie den Abschnitt **Aufgaben** aus.
4. Dadurch wird ein Fenster geöffnet. Doppelklicken Sie in diesem Fenster, um die Eigenschaften der Aufgabe **Untersuchung auf Befehl** zu öffnen.
5. Wählen Sie den Abschnitt **Anwendungseinstellungen** aus.

6. Wechseln Sie zum Abschnitt **Einstellungen**.
7. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.
8. Legen Sie bei Bedarf in der Dropdown-Liste **Stufe der heuristischen Analyse** die Analysestufe fest.
9. Aktivieren Sie das Kontrollkästchen **Nur ausführen, wenn der Computer inaktiv ist**, wenn Sie dem Arbeitsprozess, in dem die Aufgabe ausgeführt wird, die Priorität *Niedrig* zuweisen möchten.

   Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

10. Aktivieren Sie das Kontrollkästchen **Aufgabe als Untersuchung wichtiger Bereiche betrachten**, wenn Sie die Aufgabe als Aufgabe zur *Untersuchung wichtiger Bereiche* verwenden möchten.
11. Aktivieren Sie das Kontrollkästchen **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**, um die Auslastung des Computers zu optimieren.
12. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Aufgabe Untersuchung auf Befehl (in der Programmkonsole)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe zur Untersuchung auf Befehl entspricht, deren Einstellungen Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf **Eigenschaften**.
4. Wählen Sie die Registerkarte **Aufgabeneinstellungen** aus.
5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.
6. Ändern Sie bei Bedarf die Analysestufe.
7. Aktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**, wenn Sie dem Arbeitsprozess, in dem die Aufgabe ausgeführt wird, die Priorität *Niedrig* zuweisen möchten.

   Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

8. Aktivieren Sie das Kontrollkästchen **Aufgabe als Untersuchung wichtiger Bereiche betrachten**, wenn Sie die Aufgabe als Aufgabe zur *Untersuchung wichtiger Bereiche* verwenden möchten.
9. Aktivieren Sie das Kontrollkästchen **Nicht mehrere Untersuchungsaufgaben gleichzeitig ausführen**, um die Auslastung des Computers zu optimieren.
10. Speichern Sie die vorgenommenen Änderungen.

Untersuchung von Wechseldatenträgern anpassen

Untersuchung von Wechseldatenträgern konfigurieren (in der Kaspersky Security Center-Verwaltungskonsole)

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Kaspersky Security Center Verwaltungskonsole.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

   Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Zusätzlich**.
5. Klicken Sie im Unterabschnitt **Untersuchung von Wechseldatenträgern** auf **Einstellungen**.

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.
6. Führen Sie folgende Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Wechseldatenträger bei USB-Verbindung untersuchen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Wechseldatenträger untersuchen, maximale Größe (MB)** und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste **Untersuchen mit Sicherheitsstufe** die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.
7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und übernommen.

Untersuchung von Wechseldatenträgern konfigurieren (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Zusätzlich**.
5. Klicken Sie auf **Anpassen** unter **Untersuchung von Wechseldatenträgern**.

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.

6. Führen Sie folgende Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Wechseldatenträger bei USB-Verbindung untersuchen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Wechseldatenträger untersuchen, maximale Größe (MB)** und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste **Untersuchen mit Sicherheitsstufe** die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.

7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und übernommen.

Untersuchung von Wechseldatenträgern konfigurieren (in der Anwendungskonsole)

1. Öffnen Sie in der Struktur der Anwendungskonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security** und wählen Sie den Punkt **Untersuchung von Wechseldatenträgern** aus.

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.

2. Führen Sie folgende Aktionen aus:

   - Aktivieren Sie das Kontrollkästchen **Wechseldatenträger bei USB-Verbindung untersuchen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Wechseldatenträger untersuchen, maximale Größe (MB)** und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste **Untersuchen mit Sicherheitsstufe** die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.

3. Klicken Sie auf **OK**.

Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen

Sie können eine der folgenden drei vordefinierten Sicherheitsstufen für einen in der Liste der Dateiressourcen des geschützten Geräts ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen** und **Maximaler Schutz**.

Eine der vordefinierten Sicherheitsstufen auswählen (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
4. Wechseln Sie zum Abschnitt **Aufgaben**.

5. Doppelklicken Sie, um das Eigenschaftenfenster der Aufgabe **Untersuchung auf Befehl** zu öffnen.

6. Wählen Sie den Abschnitt **Untersuchungsbereich** aus.

7. Wählen Sie in der Liste des geschützten Geräts ein Element aus dem Untersuchungsbereich aus, um eine vordefinierte Sicherheitsstufe festzulegen.

8. Klicken Sie auf **Konfigurieren**.

9. Ein Fenster wird geöffnet. Aktivieren Sie in diesem Fenster auf der Registerkarte **Sicherheitsstufe** die gewünschte Sicherheitsstufe.

10. Klicken Sie auf **OK**.

11. Klicken Sie im Fenster **Eigenschaften: Untersuchung auf Befehl** auf die Schaltfläche **OK**.

Die Einstellungen der Aufgabe werden gespeichert und unverzüglich auf eine ausgeführte Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Eine der vordefinierten Sicherheitsstufen auswählen (in der Anwendungskonsole)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe zur Untersuchung auf Befehl entspricht, deren Einstellungen Sie konfigurieren möchten.

3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf **Schutzbereich konfigurieren**.

4. Wählen Sie in der Liste der Netzwerk-Dateiressourcen des geschützten Geräts einen Knoten oder ein Element aus, für den bzw. das Sie die vordefinierte Sicherheitsstufe festlegen möchten.

5. Vergewissern Sie sich, dass der ausgewählte Knoten bzw. das Element zum Untersuchungsbereich gehört.

6. Klicken Sie auf **Konfigurieren**.

7. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die passende Sicherheitsstufe aus.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.

8. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe werden gespeichert und unverzüglich während der Ausführung der Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Sicherheitseinstellungen manuell anpassen

Standardmäßig werden in den Aufgaben zur Untersuchung auf Befehl die gleichen Sicherheitsparameter verwendet wie für den gesamten Untersuchungsbereich.

Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**.

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Untersuchungsbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des geschützten Geräts oder den Nodes in der Struktur festlegen.

Sicherheitseinstellungen manuell verwalten (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie in der Verwaltungskonsolenstruktur im Ordner **Verwaltete Geräte** den Ordner mit dem Namen der Administrationsgruppe, zu welcher der betreffende Client-Computer gehört.
2. Wählen Sie im Arbeitsbereich die Registerkarte **Geräte** aus.
3. Öffnen Sie durch Doppelklick das Fenster mit den Computereigenschaften.
4. Wechseln Sie zum Abschnitt **Aufgaben**.
5. Doppelklicken Sie, um das Eigenschaftenfenster der Aufgabe **Untersuchung auf Befehl** zu öffnen.
6. Wählen Sie den Abschnitt **Untersuchungsbereich** aus.
7. Wählen Sie in der Liste der geschützten Geräte ein Element des Untersuchungsbereichs, um die Sicherheitseinstellungen zu verwalten.
8. Klicken Sie auf **Konfigurieren**.
9. Ein Fenster wird geöffnet. Aktivieren Sie in diesem Fenster auf der Registerkarte **Sicherheitsstufe** die gewünschte Sicherheitsstufe.
10. Wählen Sie die Ressource aus, deren Sicherheitseinstellungen Sie konfigurieren möchten.
11. Klicken Sie auf **Konfigurieren**.
12. Wählen Sie im folgenden Fenster die erforderliche Sicherheitsstufe aus und klicken Sie auf **Einstellungen**.
13. Nehmen Sie im Abschnitt auf der Registerkarte **Allgemein** die folgenden Einstellungen vor:
    - Objekte, die in den Schutzbereich aufgenommen werden sollen:
      - **Alle Objekte**. Kaspersky Embedded Systems Security untersucht alle Objekte.
      - **Objekte nach Format untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats. Die Liste der Dateiformate wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
      - **Objekte nach Erweiterungsliste der Antiviren-Datenbanken untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Erweiterungsliste wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
      - **Objekte nach angegebener Erweiterungsliste untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Liste der Erweiterungen wird vom Benutzer manuell angegeben.
    - Aktivieren oder deaktivieren Sie im Block **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien schützen**.

- Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:
  - Archive untersuchen
  - Programmpakete untersuchen
  - Dateien in Microsoft Office-Formaten untersuchen
  - Dateien in E-Mail-Formaten untersuchen

14. Nehmen Sie im Abschnitt auf der Registerkarte **Aktionen** die folgenden Einstellungen vor:
    - Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
      - **Desinfizieren**
      - **Disinfect. Delete if disinfection fails**
      - Löschen
      - Empfohlen
      - Informieren
    - Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
      a. Deaktivieren oder aktivieren Sie das Kontrollkästchen Aktion auf die ausgewählten Objekttypen anwenden.
      b. Klicken Sie auf **Einstellungen** und wählen Sie die zu erkennenden Objekttypen aus.
    - Konfigurieren Sie die Aktionen für zusammengesetzte Dateien, die nicht geändert werden können: Deaktivieren oder aktivieren Sie das Kontrollkästchen Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann.

15. Nehmen Sie im Abschnitt auf der Registerkarte **Optimierung** die folgenden Einstellungen vor:
    - Im Abschnitt **Ausnahmen**:
      - Deaktivieren oder aktivieren Sie das Kontrollkästchen Dateien ausschließen.
      - Deaktivieren oder aktivieren Sie das Kontrollkästchen Objekte nicht nach Typ erkennen.
        Klicken Sie für jede Einstellung auf die Schaltfläche **Ändern**, um Ausnahmen hinzuzufügen.
    - Im Abschnitt **Erweiterte Einstellungen**:
      - Untersuchung beenden, wenn sie länger dauert als (Sek.)
      - Limit für Untersuchung zusammengesetzter Objekte (MB)
      - iSwift-Technologie verwenden

- iChecker-Technologie verwenden

16. Speichern Sie die neuen Sicherheitseinstellungen.

Sicherheitseinstellungen manuell verwalten (in der Kaspersky Security Center 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 Aufgabe konfigurieren möchten.
3. Wählen Sie den Abschnitt **Aufgaben** aus.
4. Dadurch wird ein Fenster geöffnet. Doppelklicken Sie in diesem Fenster, um die Eigenschaften der Aufgabe **Untersuchung auf Befehl** zu öffnen.
5. Wählen Sie den Abschnitt **Anwendungseinstellungen** aus.
6. Wechseln Sie zum Abschnitt **Untersuchungsbereich**.
7. Wählen Sie in der Liste der Netzwerk-Dateiressourcen des geschützten Geräts ein Element aus, für das Sie die Sicherheitseinstellungen verwalten möchten. Vergewissern Sie sich, dass das ausgewählte Element zum Untersuchungsbereich gehört.
8. Klicken Sie auf **Ändern**.
9. Wählen Sie in der Dropdown-Liste einen Schutzmodus für Objekte aus:
   - **Alle Objekte**. Kaspersky Embedded Systems Security untersucht alle Objekte.
   - **Objekte nach Format untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats. Die Liste der Dateiformate wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
   - **Objekte nach Erweiterungsliste der Antiviren-Datenbanken untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Erweiterungsliste wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
   - **Objekte nach angegebener Erweiterungsliste untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Liste der Erweiterungen wird vom Benutzer manuell angegeben.
10. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Nur neue und veränderte Dateien schützen** und geben Sie an, ob Sie Unterordner in die Untersuchung einschließen möchten.
11. Verwalten Sie die Einstellungen für den Schutz zusammengesetzter Objekte:
    - Archive untersuchen
    - Programmpakete untersuchen
    - Dateien in Microsoft Office-Formaten untersuchen
    - Dateien in E-Mail-Formaten untersuchen

12. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:

    - **Desinfizieren**
    - **Disinfect. Delete if disinfection fails**
    - **Löschen**
    - **Empfohlen**
    - **Informieren**

13. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

    a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Aktion auf die ausgewählten Objekttypen anwenden**.

    b. Klicken Sie auf **Einstellungen** und wählen Sie die zu erkennenden Objekttypen aus.

14. Konfigurieren Sie die Aktionen für zusammengesetzte Dateien, die nicht geändert werden können: Deaktivieren oder aktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann**.

15. Im Abschnitt **Ausnahmen**:

    - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
    - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Objekte nicht nach Typ erkennen**.

16. Im Abschnitt **Schlüssel hinzufügen**:

    - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
    - **Limit für Untersuchung zusammengesetzter Objekte (MB)**
    - **iSwift-Technologie verwenden**
    - **iChecker-Technologie verwenden**

17. Speichern Sie die neuen Sicherheitseinstellungen.

Sicherheitseinstellungen manuell verwalten (in der Anwendungskonsole)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe zur Untersuchung auf Befehl entspricht, deren Einstellungen Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf **Schutzbereich konfigurieren**.
4. Wählen Sie in der Liste der Netzwerk-Dateiressourcen des geschützten Geräts ein Element aus, für das Sie die Sicherheitseinstellungen verwalten möchten.
5. Vergewissern Sie sich, dass das ausgewählte Element zum Untersuchungsbereich gehört.
6. Klicken Sie auf **Konfigurieren**.

7. Wählen Sie im folgenden Fenster die erforderliche Sicherheitsstufe aus und klicken Sie auf **Einstellungen**.

8. Nehmen Sie im Abschnitt auf der Registerkarte **Allgemein** die folgenden Einstellungen vor:

- Objekte, die in den Schutzbereich aufgenommen werden sollen:
  - **Alle Objekte**. Kaspersky Embedded Systems Security untersucht alle Objekte.
  - **Objekte nach Format untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats. Die Liste der Dateiformate wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
  - **Objekte nach Erweiterungsliste der Antiviren-Datenbanken untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Erweiterungsliste wird von Kaspersky zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
  - **Objekte nach angegebener Erweiterungsliste untersuchen**. Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung. Die Liste der Erweiterungen wird vom Benutzer manuell angegeben.
- Aktivieren oder deaktivieren Sie im Block **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien schützen**.
- Geben Sie im Abschnitt **Untersuchung von zusammengesetzten Dateien** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:
  - **Archive untersuchen**
  - **Programmpakete untersuchen**
  - **Dateien in Microsoft Office-Formaten untersuchen**
  - **Dateien in E-Mail-Formaten untersuchen**

9. Nehmen Sie im Abschnitt auf der Registerkarte **Aktionen** die folgenden Einstellungen vor:

- Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
  - **Desinfizieren**
  - **Disinfect. Delete if disinfection fails**
  - **Löschen**
  - **Empfohlen**
  - **Informieren**

- Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

  a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Aktion auf die ausgewählten Objekttypen anwenden**.

  b. Klicken Sie auf **Einstellungen** und wählen Sie die zu erkennenden Objekttypen aus.

- Konfigurieren Sie die Aktionen für zusammengesetzte Dateien, die nicht geändert werden können: Deaktivieren oder aktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn ein erkanntes eingebettetes Objekt nicht von der App geändert werden kann**.

10. Nehmen Sie im Abschnitt auf der Registerkarte **Optimierung** die folgenden Einstellungen vor:

    - Im Abschnitt **Ausnahmen**:

      - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
      - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Objekte nicht nach Typ erkennen**.

      Klicken Sie für jede Einstellung auf die Schaltfläche **Ändern**, um Ausnahmen hinzuzufügen.

    - Im Abschnitt **Erweiterte Einstellungen**:

      - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
      - **Limit für Untersuchung zusammengesetzter Objekte (MB)**
      - **iSwift-Technologie verwenden**
      - **iChecker-Technologie verwenden**

11. Speichern Sie die neuen Sicherheitseinstellungen.

Statistik von Aufgaben zur Untersuchung auf Befehl

Während eine Aufgabe zur *Untersuchung auf Befehl* ausgeführt wird, können Sie Informationen über Anzahl der Objekte, die Kaspersky Embedded Systems Security seit dem Aufgabenstart verarbeitet hat, anzeigen.

Diese Informationen stehen auch zur Verfügung, wenn Sie eine Aufgabe anhalten. Sie können die Aufgabenstatistik im Bericht über Aufgabenausführung aufrufen.

So zeigen Sie Untersuchung auf Befehl-Statistik an:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie die Aufgabe zur Untersuchung auf Befehl, deren Statistik Sie anzeigen möchten.

   Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Informationen über Objekte, die Kaspersky Embedded Systems Security seit dem Aufgabenstart verarbeitet hat, werden in der nachfolgenden Tabelle angezeigt.

Feld	Beschreibung
Gefunden	Anzahl der Objekte, die von Kaspersky Embedded Systems Security gefunden wurden. Findet Kaspersky Embedded Systems Security beispielsweise in fünf Dateien ein und dasselbe schädliche Objekt, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Infizierte und andere Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security als infiziert eingestuft hat, oder der gefundenen legalen Softwaredateien, die nicht aus dem Untersuchungsbereich ausgeschlossen wurden und die als legitime Software klassifiziert wurden, die von Eindringlingen verwendet werden kann, um das Gerät oder persönliche Daten zu beschädigen.
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security aus folgenden Gründen nicht desinfiziert wurden: • Das erkannte Objekt ist von einem Typ, der nicht desinfiziert werden kann. • Bei der Desinfektion ist eine Störung aufgetreten.
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden.
Entfernte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security erfolgreich gelöscht wurden.
Nicht untersuchte Objekte	Anzahl der zum Schutzbereich gehörenden Objekte, die Kaspersky Embedded Systems Security nicht untersuchen konnte, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Archive	Anzahl der Archive, die von Kaspersky Embedded Systems Security untersucht wurden.
Gepackte Objekte	Anzahl der gepackten Objekte, die von Kaspersky Embedded Systems Security untersucht wurden.
Kennwortgeschützte Objekte	Anzahl der Objekte (z. B. Archive), die von Kaspersky Embedded Systems Security übersprungen wurden, weil sie kennwortgeschützt sind.
Beschädigte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security übersprungen wurden, da ihr Format beschädigt war.
Bearbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Nicht entfernte Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos zu entfernen versucht hat, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht verarbeitete Objekte	Gesamtzahl der Objekte, die nicht von Kaspersky Embedded Systems Security verarbeitet wurden.

Sie können auch eine Statistik der Aufgaben zur Untersuchung auf Befehl im Bericht über die Ausführung der gewählten Aufgabe über den Link **Aufgabenprotokoll öffnen** im Abschnitt **Verwaltung** des Ergebnisbereichs anzeigen.

Wir empfehlen, dass Sie nach Aufgabenabschluss die im Protokoll der Aufgabenausführung registrierten Ereignisse auf der Registerkarte **Ereignisse** manuell bearbeiten.

Datenbanken-Update und Update der Programm-Module für Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen über die Update-Aufgaben und das Rollback von Kaspersky Embedded Systems Security-Updates sowie Anweisungen zur Konfiguration von Aufgaben.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) ist in der Software in den USA möglicherweise nicht verfügbar.

Update der Datenbanken und Programm-Module

Das Update der Datenbanken und Programm-Module von Kaspersky Embedded Systems 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 Embedded Systems Security enthalten. Damit neue Bedrohungen rechtzeitig erkannt werden können, müssen Sie die Datenbanken und Programm-Module regelmäßig aktualisieren.

Für ein regelmäßiges Update ist eine aktuelle Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Für den Download von Updates der Programm-Datenbanken und Programm-Module verwendet Kaspersky Embedded Systems Security die HTTP- oder FTP-Update-Server von Kaspersky, den Kaspersky Security Center Administrationsserver oder andere Update-Quellen.

Sie können Updates auf die einzelnen geschützten Geräte herunterladen oder ein geschütztes Gerät als Verteiler verwenden. Die Updates werden darauf kopiert und dann auf die geschützten Geräte verteilt. Wenn Sie die Gerätesicherheit Ihres Unternehmens zentral mit Kaspersky Security Center verwalten, können Sie den Administrationsserver als Proxy für den Download von Updates nutzen.

Wenn der Update-Download unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zu den Datenbanken aus den zuletzt installierten Updates zurück. Wenn die Datenbanken von Kaspersky Embedded Systems Security beschädigt werden, kann ein manuelles Rollback auf zuvor installierte Updates: durchgeführt werden.

Bei einer Aktualisierung werden folgende Objekte auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Embedded Systems 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 Embedded Systems Security werden auch die Netzwerktreiber aktualisiert, die gewährleisten, dass die Schutzkomponenten den Netzwerkverkehr abfangen können.

- Programm-Module. Updates für Programm-Module beheben Schwachstellen von Kaspersky Embedded Systems 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 Embedded Systems 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 Update-Ergebnisse und über alle Ereignisse, die bei der Ausführung der Update-Aufgabe eintreten, werden im Bericht der Update-Aufgabe protokolliert.

Über Update-Aufgaben

Kaspersky Embedded Systems Security bietet zwei Update-Aufgaben: *Update* und *Update-Rollback*.

Update

Standardmäßig kopiert Kaspersky Embedded Systems Security die Datenbanken und (sofern verfügbar) die Programm-Module aus der Update-Quelle auf das Gerät und verwendet diese sofort in den Schutzkomponenten. Die Aufgaben zur Untersuchung auf Befehl verwenden beim nächsten Aufgabenstart die aktualisierten Programm-Datenbanken.

Sie können die Einstellungen der Aufgabe *Update* konfigurieren. Nachdem Sie die Aufgabeneinstellungen geändert haben, übernimmt Kaspersky Embedded Systems Security die neuen Werte beim nächsten Aufgabenstart.

Standardmäßig ist die Aufgabe *Update* auf den Modus **Manuell** eingestellt. Update-Aufgaben können nicht angehalten und wieder fortgesetzt werden.

Update-Rollback

Aufgrund dieser Aufgabe kehrt Kaspersky Embedded Systems Security zu den vorherigen Datenbanken und Programm-Modulen zurück.

Die Aufgabe *Update-Rollback* wird standardmäßig nicht ausgeführt.

Update-Schemata für die Datenbanken und Module von Kaspersky Embedded Systems Security

Die Wahl der Update-Quelle in *Update*-Aufgaben hängt vom Update-Schema für Datenbanken und Programm-Module ab, die im Unternehmen verwendet werden.

Sie können die Datenbanken und Module von Kaspersky Embedded Systems Security auf den geschützten Geräten nach folgendem Schemata aktualisieren:

- Download von Updates direkt aus dem Internet auf jedes der geschützten Geräte (Schema 1).
- Download von Updates aus dem Internet auf ein zwischengeschaltetes Gerät und Verteilung des Updates von diesem Gerät aus auf die geschützten Geräte.

  Jedes Gerät, auf dem die folgenden Programme installiert sind, kann als Zwischengerät dienen:

  - Kaspersky Embedded Systems Security (Schema 2).
  - Kaspersky Security Center Administrationsserver (Schema 3).

  > Das Update über ein zwischengeschaltetes Gerät spart nicht nur Internet-Datenverkehr ein, sondern bietet den geschützten Geräten auch zusätzliche Sicherheit.

- Laden Sie Datenbank-Updates über einen sicheren Wechseldatenträger auf jedes geschützte Gerät herunter (Schema 4).

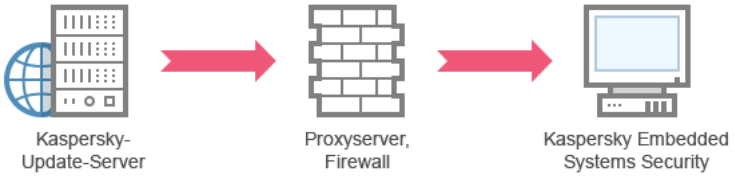
Die Update-Schemata werden im Folgenden beschrieben.

Schema 1. Direktes Aktualisieren von Datenbanken und Modulen aus dem Internet

Um Updates für Kaspersky Embedded Systems Security direkt aus dem Internet anzupassen, gehen Sie wie folgt vor:

Geben Sie auf jedem geschützten Gerät in den Einstellungen der *Update*-Aufgabe als Update-Quelle die Kaspersky-Update-Server an.

Als Update-Quelle können auch andere HTTPS- oder HTTP-Server gewählt werden, auf denen sich ein Ordner mit den Update-Dateien befindet.



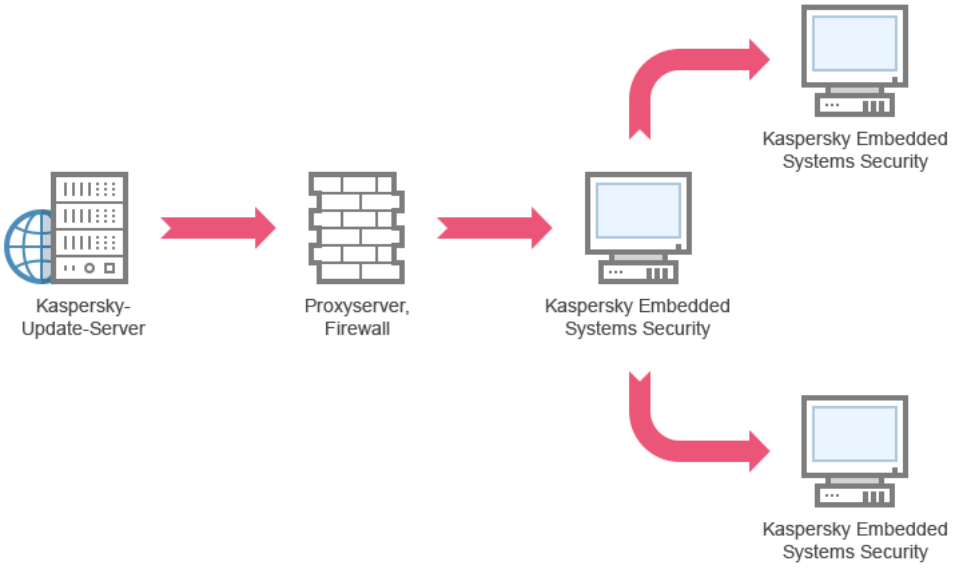
Schema 1: Direktes Aktualisieren von Datenbanken und Modulen aus dem Internet

Schema 2. Aktualisieren von Datenbanken und Modulen über eines der geschützten Geräte

So konfigurieren Sie den Empfang von Updates für Kaspersky Embedded Systems Security über eines der geschützten Geräte:

1. Kopieren Sie die Updates auf das ausgewählte geschützte Gerät.
   - Konfigurieren Sie auf dem ausgewählten geschützten Gerät die Einstellungen der *Update*-Aufgabe:
     a. Geben Sie als Update-Quelle den Kaspersky-Update-Server an.
     b. Geben Sie als Ordner, in dem die Updates gespeichert werden sollen, einen freigegebenen Ordner an.
2. Verteilen Sie die Updates auf die übrigen geschützten Geräte:
   - Konfigurieren Sie die *Update*-Aufgabe auf jedem geschützten Gerät.
     Geben Sie als Update-Quelle den Ordner auf dem Laufwerk des zwischengeschalteten Geräts an, in den die Updates kopiert werden.

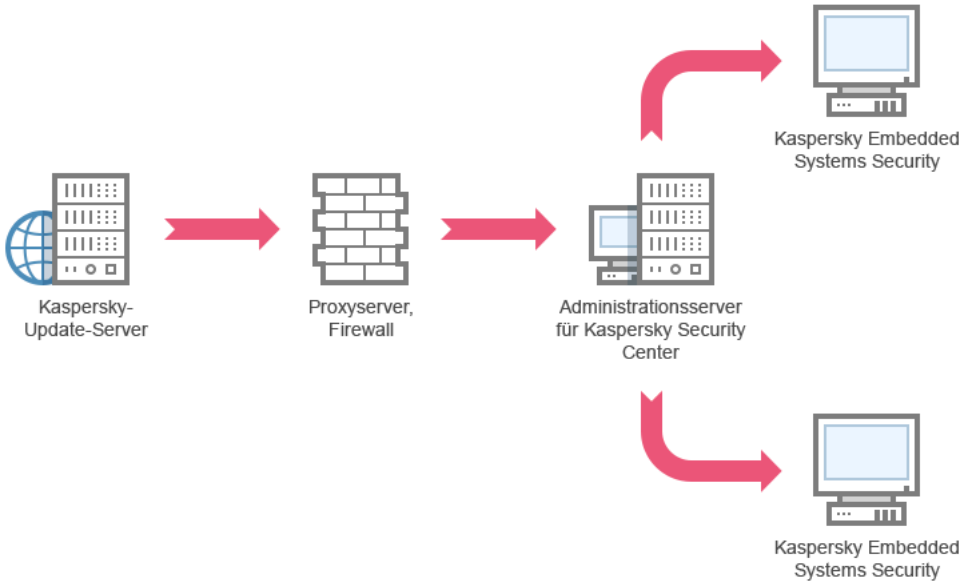
Kaspersky Embedded Systems Security erhält die Updates dann über eines der geschützten Geräte.



Schema 2: Aktualisieren von Datenbanken und Modulen über eines der geschützten Geräte

Schema 3. Aktualisieren von Datenbanken und Modulen über den Kaspersky Security Center Administrationsserver

Wenn Sie Kaspersky Security Center verwenden, um den Antiviren-Schutz für Geräte zentral zu verwalten, können Sie Updates über den Kaspersky Security Center Administrationsserver herunterladen, der in Ihrem lokalen Netzwerk installiert ist.



Schema 3: Aktualisieren von Datenbanken und Modulen über einen Kaspersky Security Center Administrationsserver

So konfigurieren Sie den Empfang von Updates für Kaspersky Embedded Systems Security über den Kaspersky Security Center Administrationsserver:

1. Installieren Sie den Administrationsagenten auf jedem geschützten Gerät. Der Administrationsagent ist eine Programmkomponente, die zum Lieferumfang von Kaspersky Security Center gehört. Er gewährleistet die Interaktion zwischen dem Administrationsserver und Kaspersky Embedded Systems Security auf dem geschützten Gerät. Ausführliche Informationen zum Administrationsagenten und seiner Konfiguration mithilfe von Kaspersky Security Center finden Sie in der *Hilfe für Kaspersky Security Center*.

2. Laden Sie die Updates von einem Kaspersky-Update-Server auf den Kaspersky Security Center Administrationsserver herunter.

   - Konfigurieren Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* für die angegebene Auswahl von geschützten Geräten.

     Geben Sie als Update-Quelle den Kaspersky-Update-Server an.

3. Verteilen Sie die Updates auf die geschützten Geräte. Führen Sie hierzu eine der folgenden Aktionen aus:

   - Passen Sie in Kaspersky Security Center eine Gruppenaufgabe zum Update der Antiviren-Datenbanken (Programm-Modul) für die Verteilung der Updates an die geschützten Geräte an:
   - Konfigurieren Sie die Aufgabe *Update* auf jedem geschützten Gerät:

     a. Geben Sie den Kaspersky Security Center Administrationsserver als Update-Quelle an.

     b. Passen Sie den Zeitplan für die Aufgabe bei Bedarf an.

Kaspersky Embedded Systems Security erhält die Updates dann über den Kaspersky Security Center Administrationsserver.

Schema 4. Programm-Datenbanken von einem sicheren Wechseldatenträger aktualisieren

So aktualisieren Sie die Datenbanken von Kaspersky Embedded Systems Security mithilfe eines sicheren Wechseldatenträgers:

1. Verbinden Sie den sicheren Wechseldatenträger mit dem Gerät, auf dem Kaspersky Embedded Systems Security installiert ist und das Zugriff auf die Updates der Programm-Datenbanken hat.
2. Fügen Sie für den angeschlossenen Wechseldatenträger eine Erlaubnisregel der Komponente Gerätekontrolle hinzu.
3. Konfigurieren und starten Sie in der Programmkonsole die Aufgabe *Sicheres Kopieren von Programm-Datenbanken*.
4. Verbinden Sie den sicheren Wechseldatenträger, der die Datenbanken-Updates enthält, mit dem Gerät, auf dem Sie die Programm-Datenbanken aktualisieren möchten.
5. Konfigurieren und starten Sie in der Programmkonsole die Aufgabe *Sicheres Update der Programm-Datenbanken*.

Kaspersky Embedded Systems Security erhält die aktualisierten Programm-Datenbanken vom sicheren Wechseldatenträger.

Einstellung von Update-Aufgaben

So konfigurieren Sie die Aufgabe Update (in der Kaspersky Security Center-Verwaltungskonsole)

1. Gehen Sie in der Kaspersky Security Center-Verwaltungskonsole zu der lokalen Update-Aufgabe oder Update-Gruppenaufgabe, die Sie konfigurieren möchten.
2. Öffnen Sie den Abschnitt **Einstellungen**.

3. Konfigurieren Sie unter **Update-Einstellungen für den lokalen Modus** die Update-Quellen für Kaspersky Embedded Systems Security, das mit dem Kaspersky Security Center Administrationsserver verbunden ist:

   a. Klicken Sie auf **Einstellungen**.

      Das Fenster **Update der Datenbanken und Programm-Module** wird geöffnet.

   b. Aktivieren Sie das Kontrollkästchen neben den Update-Quellen, die Sie verwenden möchten:

      - Kaspersky Security Center Administrationsserver
      - Kaspersky-Update-Server

      Klicken Sie bei Bedarf auf die Schaltfläche **Hinzufügen**, um eine benutzerdefinierte Update-Quelle hinzuzufügen.

   c. Wenn Sie mehrere Update-Quellen auswählen, können Sie die Update-Quellen mit den Schaltflächen **Nach oben** und **Nach unten** nach Priorität sortieren. Kaspersky Embedded Systems Security greift genau in der festgelegten Reihenfolge auf die Update-Quellen zu und führt die Update-Aufgabe mit dem Update-Paket aus der ersten verfügbaren Update-Quelle aus.

      Standardmäßig verwendet Kaspersky Embedded Systems 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*-Aufgabe die Kaspersky-Server als primäre Update-Quelle ausgewählt, da das Programm möglicherweise keinen Zugriff auf Kaspersky Security Center hat.

   d. Wenn Sie **Kaspersky-Update-Server** als Update-Quelle ausgewählt haben, legen Sie die Methode fest, nach der Kaspersky Embedded Systems Security einen Kaspersky-Update-Servers auswählen soll:

      - **Automatisch ermitteln**. Das Programm verwendet den nächstgelegenen verfügbaren Kaspersky-Update-Server.
      - **Aus der Liste wählen**. Das Programm verwendet den Kaspersky-Update-Server in dem aus der Liste ausgewählten Land.

   e. Klicken Sie im Fenster **Update der Datenbanken und Programm-Module** auf die Schaltfläche **OK**.

4. Update der Programm-Datenbanken konfigurieren:

   a. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Updates für Programm-Datenbanken herunterladen**.

   b. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern**. Dieses Kontrollkästchen aktiviert oder deaktiviert den Prozess zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher. Das Kontrollkästchen ist standardmäßig deaktiviert.

   c. Wenn das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern** ausgewählt haben, geben Sie im Feld **Für die Optimierung genutzter Arbeitsspeicher (MB)** die Größe des Arbeitsspeichers in Megabyte an. Das Betriebssystem stellt dieses Arbeitsspeichervolumen temporär für die Speicherung der Update-Dateien während der Aufgabenausführung zur Verfügung. Standardmäßig ist ein Arbeitsspeichervolumen von 640 MB eingestellt. Das minimale Arbeitsspeichervolumen beträgt 400 MB.

Wenn die *Update*-Aufgabe mit aktivierter Optimierung für Datenträgersubsysteme ausgeführt wird, kann eines der folgenden Ereignisse auftreten:

- Wenn der Wert zu klein ist, reicht die zugewiesene RAM-Größe möglicherweise nicht aus, um die Aufgabe zum Update der Programm-Datenbanken abzuschließen (z. B. während der ersten Aktualisierung), wodurch die Aufgabe mit einem Fehler abgeschlossen wird.

  In diesem Fall wird empfohlen, mehr RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

- Wenn der Wert zu Beginn der Aufgabe zur Aktualisierung der Datenbank zu groß ist, kann es vorkommen, dass es unmöglich ist, ein virtuelles Laufwerk mit der ausgewählten Größe im RAM zu erstellen. Die Funktion zur Optimierung des Festplattensubsystems wird daher automatisch deaktiviert und die Aufgabe zur Aktualisierung der Datenbank wird ohne die Funktion zur Optimierung ausgeführt.

  In diesem Fall wird empfohlen, weniger RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

5. Konfigurieren Sie die Updates für Programm-Module:

   a. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen**.

   Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Embedded Systems Security den Benutzer über verfügbare Updates für Programm-Module und aktualisiert im Verlauf von *Update*-Vorgängen die Programm-Module. Die Art der Updates für Programm-Module, die angewendet werden, wird separat konfiguriert. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   b. Wählen Sie aus, welche Updates für Programm-Module Sie installieren möchten.

   - **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Embedded Systems 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 Embedded Systems Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.

   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.

6. Konfigurieren Sie das Kopieren von Updates in einen lokalen Ordner:

   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Updates in einen lokalen Ordner kopieren**.

b. Wählen Sie aus, welche Update-Inhalte das Programm in den lokalen Ordner kopieren soll:

- **Datenbanken-Updates verteilen**. Das Programm lädt nur Datenbanken-Updates herunter.
- **Kritische Updates für Programm-Module verteilen**. Das Programm lädt nur wichtige Updates für Programm-Module herunter.
- **Datenbanken-Updates und kritische Updates für Programm-Module verteilen**. Das Programm lädt Datenbanken-Updates und wichtige Updates für Programm-Module herunter.

c. Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Kaspersky Embedded Systems Security die erhaltenen Updates kopieren soll.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Aufgabe Update (in der Programmkonsole)

1. Öffnen Sie in der Struktur der Anwendungskonsole den Knoten **Update → Update der Datenbanken und Programm-Module**.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Eigenschaften: Update der Datenbanken und Programm-Module** wird geöffnet.
3. Konfigurieren Sie unter **Update-Einstellungen für den lokalen Modus** die Update-Quellen für Kaspersky Embedded Systems Security, das mit dem Kaspersky Security Center Administrationsserver verbunden ist:

   a. Klicken Sie auf **Einstellungen**.

   Das Fenster **Update der Datenbanken und Programm-Module** wird geöffnet.

   b. Aktivieren Sie das Kontrollkästchen neben den Update-Quellen, die Sie verwenden möchten:

   - Kaspersky Security Center Administrationsserver
   - Kaspersky-Update-Server

   Klicken Sie bei Bedarf auf die Schaltfläche **Hinzufügen**, um eine benutzerdefinierte Update-Quelle hinzuzufügen.

   c. Wenn Sie mehrere Update-Quellen auswählen, können Sie die Update-Quellen mit den Schaltflächen **Nach oben** und **Nach unten** nach Priorität sortieren. Kaspersky Embedded Systems Security greift genau in der festgelegten Reihenfolge auf die Update-Quellen zu und führt die Update-Aufgabe mit dem Update-Paket aus der ersten verfügbaren Update-Quelle aus.

   Standardmäßig verwendet Kaspersky Embedded Systems 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*-Aufgabe die Kaspersky-Server als primäre Update-Quelle ausgewählt, da das Programm möglicherweise keinen Zugriff auf Kaspersky Security Center hat.

d. Wenn Sie **Kaspersky-Update-Server** als Update-Quelle ausgewählt haben, legen Sie die Methode fest, nach der Kaspersky Embedded Systems Security einen Kaspersky-Update-Servers auswählen soll:

- **Automatisch ermitteln**. Das Programm verwendet den nächstgelegenen verfügbaren Kaspersky-Update-Server.
- **Aus der Liste wählen**. Das Programm verwendet den Kaspersky-Update-Server in dem aus der Liste ausgewählten Land.

e. Klicken Sie im Fenster **Update der Datenbanken und Programm-Module** auf die Schaltfläche **OK**.

4. Update der Programm-Datenbanken konfigurieren:

a. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Updates für Programm-Datenbanken herunterladen**.

b. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern**. Dieses Kontrollkästchen aktiviert oder deaktiviert den Prozess zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher. Das Kontrollkästchen ist standardmäßig deaktiviert.

c. Wenn das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern** ausgewählt haben, geben Sie im Feld **Für die Optimierung genutzter Arbeitsspeicher (MB)** die Größe des Arbeitsspeichers in Megabyte an. Das Betriebssystem stellt dieses Arbeitsspeichervolumen temporär für die Speicherung der Update-Dateien während der Aufgabenausführung zur Verfügung. Standardmäßig ist ein Arbeitsspeichervolumen von 640 MB eingestellt. Das minimale Arbeitsspeichervolumen beträgt 400 MB.

Wenn die *Update*-Aufgabe mit aktivierter Optimierung für Datenträgersubsysteme ausgeführt wird, kann eines der folgenden Ereignisse auftreten:

- Wenn der Wert zu klein ist, reicht die zugewiesene RAM-Größe möglicherweise nicht aus, um die Aufgabe zum Update der Programm-Datenbanken abzuschließen (z. B. während der ersten Aktualisierung), wodurch die Aufgabe mit einem Fehler abgeschlossen wird.

  In diesem Fall wird empfohlen, mehr RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

- Wenn der Wert zu Beginn der Aufgabe zur Aktualisierung der Datenbank zu groß ist, kann es vorkommen, dass es unmöglich ist, ein virtuelles Laufwerk mit der ausgewählten Größe im RAM zu erstellen. Die Funktion zur Optimierung des Festplattensubsystems wird daher automatisch deaktiviert und die Aufgabe zur Aktualisierung der Datenbank wird ohne die Funktion zur Optimierung ausgeführt.

  In diesem Fall wird empfohlen, weniger RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

5. Konfigurieren Sie die Updates für Programm-Module:

a. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen**.

Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Embedded Systems Security den Benutzer über verfügbare Updates für Programm-Module und aktualisiert im Verlauf von *Update*-Vorgängen die Programm-Module. Die Art der Updates für Programm-Module, die angewendet werden, wird separat konfiguriert. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

b. Wählen Sie aus, welche Updates für Programm-Module Sie installieren möchten.

- **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Embedded Systems 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 Embedded Systems Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.

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.

6. Konfigurieren Sie das Kopieren von Updates in einen lokalen Ordner:

   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Updates in einen lokalen Ordner kopieren**.

   b. Wählen Sie aus, welche Update-Inhalte das Programm in den lokalen Ordner kopieren soll:

   - **Datenbanken-Updates verteilen**. Das Programm lädt nur Datenbanken-Updates herunter.

   - **Kritische Updates für Programm-Module verteilen**. Das Programm lädt nur wichtige Updates für Programm-Module herunter.

   - **Datenbanken-Updates und kritische Updates für Programm-Module verteilen**. Das Programm lädt Datenbanken-Updates und wichtige Updates für Programm-Module herunter.

   c. Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Kaspersky Embedded Systems Security die erhaltenen Updates kopieren soll.

7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Aufgabe Update (in der Kaspersky Security Center Web Console)

1. Gehen Sie in der Web Console zu der lokalen *Update*-Aufgabe oder Update-Gruppenaufgabe, die Sie konfigurieren möchten.

2. Öffnen Sie den Abschnitt **Einstellungen**.

3. Wählen Sie die Registerkarte **Lokaler Modus** aus, um die *Update*-Aufgabe für Kaspersky Embedded Systems Security zu konfigurieren, das mit dem Kaspersky Security Center Administrationsserver verbunden ist.

4. Konfigurieren Sie die Update-Quellen:

   a. Aktivieren Sie unter **Update-Quellen** das Kontrollkästchen neben den Update-Quellen, die Sie verwenden möchten:

   - **Kaspersky Security Center Administrationsserver**

   - **Kaspersky-Update-Server**

   Klicken Sie bei Bedarf auf die Schaltfläche **Hinzufügen**, um eine benutzerdefinierte Update-Quelle hinzuzufügen.

b. Wenn Sie mehrere Update-Quellen auswählen, können Sie die Update-Quellen mit den Schaltflächen **Nach oben** und **Nach unten** nach Priorität sortieren. Kaspersky Embedded Systems Security greift genau in der festgelegten Reihenfolge auf die Update-Quellen zu und führt die Update-Aufgabe mit dem Update-Paket aus der ersten verfügbaren Update-Quelle aus.

   Standardmäßig verwendet Kaspersky Embedded Systems 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*-Aufgabe die Kaspersky-Server als primäre Update-Quelle ausgewählt, da das Programm möglicherweise keinen Zugriff auf Kaspersky Security Center hat.

5. Update der Programm-Datenbanken konfigurieren:

   a. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Updates für Programm-Datenbanken herunterladen**.

   b. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern**. Dieses Kontrollkästchen aktiviert oder deaktiviert den Prozess zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher. Das Kontrollkästchen ist standardmäßig deaktiviert.

   c. Wenn das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern** ausgewählt haben, geben Sie im Feld **Für die Optimierung genutzter Arbeitsspeicher (MB)** die Größe des Arbeitsspeichers in Megabyte an. Das Betriebssystem stellt dieses Arbeitsspeichervolumen temporär für die Speicherung der Update-Dateien während der Aufgabenausführung zur Verfügung. Standardmäßig ist ein Arbeitsspeichervolumen von 640 MB eingestellt. Das minimale Arbeitsspeichervolumen beträgt 400 MB.

      Wenn die *Update*-Aufgabe mit aktivierter Optimierung für Datenträgersubsysteme ausgeführt wird, kann eines der folgenden Ereignisse auftreten:

      - Wenn der Wert zu klein ist, reicht die zugewiesene RAM-Größe möglicherweise nicht aus, um die Aufgabe abzuschließen (z. B. während der ersten Aktualisierung), wodurch die Aufgabe mit einem Fehler abgeschlossen wird.

        In diesem Fall wird empfohlen, mehr RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

      - Wenn der Wert zu Beginn der Aufgabe zu groß ist, kann es vorkommen, dass es unmöglich ist, ein virtuelles Laufwerk mit der ausgewählten Größe im RAM zu erstellen. Die Funktion zur Optimierung des Festplattensubsystems wird daher automatisch deaktiviert und die Aufgabe zur Aktualisierung der Datenbank wird ohne die Funktion zur Optimierung ausgeführt.

        In diesem Fall wird empfohlen, weniger RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

6. Konfigurieren Sie die Updates für Programm-Module:

   a. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Updates für Programm-Module herunterladen**.

      Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Embedded Systems Security den Benutzer über verfügbare Updates für Programm-Module und aktualisiert im Verlauf von *Update*-Vorgängen die Programm-Module. Die Art der Updates für Programm-Module, die angewendet werden, wird separat konfiguriert. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

b. Wählen Sie aus, welche Updates für Programm-Module Sie installieren möchten.

- **Kritische und bestätigte Updates installieren**. Wenn diese Variante ausgewählt ist, installiert Kaspersky Embedded Systems 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 Embedded Systems Security vorhandene Programm-Modul-Updates, nachdem deren Installation lokal über die Programmoberfläche oder in Kaspersky Security Center genehmigt wurde. Dieser Status gilt als Standard.

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.

7. Konfigurieren Sie das Kopieren von Updates in einen lokalen Ordner:

a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Updates in folgenden Ordner kopieren**.

b. Wählen Sie aus, welche Update-Inhalte das Programm in den lokalen Ordner kopieren soll:

- **Datenbanken-Updates verteilen**. Das Programm lädt nur Datenbanken-Updates herunter.

- **Kritische Updates für Programm-Module verteilen**. Das Programm lädt nur wichtige Updates für Programm-Module herunter.

- **Datenbanken-Updates und kritische Updates für Programm-Module verteilen**. Das Programm lädt Datenbanken-Updates und wichtige Updates für Programm-Module herunter.

c. Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Kaspersky Embedded Systems Security die erhaltenen Updates kopieren soll.

8. Speichern Sie die vorgenommenen Änderungen.

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 Embedded Systems Security lädt die neue Programmversion zusammen mit den Antiviren-Datenbanken aus derselben Quelle herunter.

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* verwalten. Damit die neue Programmversion in das Paket mit den Antiviren-Datenbanken aufgenommen wird, müssen Sie das Update der *Programm-Module* in den Einstellungen der Aufgabe Update zulassen.

Schritte eines SMU-Programm-Updates

1. **Nachdem eine neue Programmversion veröffentlicht oder ein Modul aktualisiert wurde, verteilt Kaspersky ein Update.**
2. **Der Benutzer stimmt dem Programm-Update zu.**

   Wenn der Computer mit Kaspersky Security Center verbunden ist, steht das Update in Kaspersky Security Center im Abschnitt **Updates für Kaspersky-Datenbanken und -Softwaremodule** zur Verfügung. 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 in der Programmkonsole zur Verfügung. Um das Update zu genehmigen, gehen Sie zum Abschnitt **Update** → **Programm-Update**, wählen Sie eine Programmversion aus und akzeptieren Sie gegebenenfalls die Bedingungen der Vereinbarungen.
3. **Kaspersky Embedded Systems Security führt die Aufgabe Update nach einem Zeitplan aus.**

Dabei aktualisiert Kaspersky Embedded Systems Security das Programm im unbeaufsichtigten Modus.

Sicheres Kopieren der Programm-Datenbanken

Die Aufgabe kann nur in der Anwendungskonsole konfiguriert werden. Diese Aufgabe kann nicht in der Kaspersky Security Center-Management-Konsole oder Kaspersky Security Center Web Console konfiguriert werden.

So konfigurieren und starten Sie die Aufgabe „Sicheres Kopieren der App-Datenbanken“:

1. Wählen in der Anwendungskonsolenstruktur im Kontextmenü des Knotens **Update** den Punkt **Sicheres Kopieren der Datenbanken wird gestartet** aus.

   Das Willkommensfenster des Assistenten zum Kopieren sicherer App-Datenbanken wird geöffnet.
2. Klicken Sie auf **Weiter >**.
3. Wählen Sie unter **Update-Quelle** eine Update-Quelle aus:

   - **Kaspersky Security Center Administrationsserver**.

     Sie können diese Variante auswählen, wenn die Programme von Kaspersky in Ihrem Netzwerk mithilfe des Remote-Verwaltungssystems von Kaspersky Security Center verwaltet werden und auf dem geschützten Gerät der Administrationsagent installiert ist – eine Komponente von Kaspersky Security Center, die eine Kommunikation zwischen den geschützten Geräten und dem Administrationsserver gewährleistet.

     Dieser Status gilt als Standard.

- **Kaspersky-Update-Server**.

  HTTP- und HTTPS-Server von Kaspersky, von denen die Anwendungen Datenbanken-Updates und Updates von Modulen der Anwendung erhalten.

- **Benutzerdefinierte HTTP- oder FTP-Server oder Netzwerkordner**.

4. Wenn Sie im vorherigen Schritt **Kaspersky Security Center Administrationsserver** ausgewählt haben, konfigurieren Sie die Funktion **Kaspersky-Update-Server verwenden, wenn die angegebenen Server nicht verfügbar sind**. Wenn diese Option aktiviert ist, verwendet Kaspersky Embedded Systems Security die Kaspersky-Update-Server als Update-Quelle, wenn der Kaspersky Security Center Administrationsserver nicht verfügbar ist.

5. Konfigurieren Sie unter **Einstellungen für die Verbindung zur Update-Quelle** die Verwendung eines Proxyservers für die Verbindung mit Update-Quellen.

6. Klicken Sie auf **Weiter >**.

7. Wählen Sie aus der Dropdown-Liste den angeschlossenen sicheren Rutoken-Wechseldatenträger aus, auf dem Sie die Antiviren-Datenbanken des Programms speichern möchten.

   Als sicherer Wechseldatenträger kann nur ein Rutoken-Wechseldatenträger verwendet werden, der durch eine Regel der Komponente Gerätekontrolle ausdrücklich autorisiert wurde.

8. Geben Sie unter **Sicherheitseinstellungen** im Feld **Aktuellen Administrator-PIN-Code eingeben** die Administrator-PIN ein, die für den Rutoken-Wechseldatenträger festgelegt wurde, um dessen Inhalte vor dem Lesen, Kopieren oder Schreiben durch potenzielle Angreifer zu schützen.

9. So ändern Sie die aktuelle Administrator-PIN:

   a. Aktivieren Sie das Kontrollkästchen **Aktuellen Administrator-PIN-Code ändern (nur Ziffern und lateinische Buchstaben sind zulässig)**.

   b. Geben Sie die neue PIN ein.

   c. Bestätigen Sie die neue PIN.

10. Legen Sie eine Benutzer-PIN fest. Diese PIN wird von dem Mitarbeiter benötigt, der die Programm-Datenbanken mithilfe der Aufgabe *Sicheres Update der Programm-Datenbanken* und des ausgewählten Rutoken-Wechseldatenträgers aktualisiert:

    a. Geben Sie die Benutzer-PIN ein.

    b. Bestätigen Sie die Benutzer-PIN.

11. Klicken Sie auf **Weiter >**.

Das sichere Kopieren der Programm-Datenbanken auf den Rutoken-Wechseldatenträger wird gestartet. Die Einstellungen werden gespeichert und angewendet, während die Aufgabe ausgeführt wird.

Sicheres Update der Programm-Datenbanken

Die Aufgabe *Sicheres Update der Programm-Datenbanken* ist erforderlich, um die Programm-Datenbanken mithilfe eines sicheren Wechseldatenträgers, der vor dem Lesen, Kopieren und Schreiben durch potenzielle Angreifer geschützt ist, in einem geschlossenen Unternehmensnetzwerk und auf Geräten ohne Zugriff auf die Programm-Datenbanken zu aktualisieren.

Diese Aufgabe kann nur über die Programmkonsole gestartet werden, die auf demselben Gerät wie Kaspersky Embedded Systems Security installiert ist. Eine Konfiguration der Aufgabe über die Verwaltungskonsole oder die Web Console ist nicht möglich.

So starten Sie die Aufgabe Sicheres Update der Programm-Datenbanken:

1. Wählen in der Anwendungskonsolenstruktur im Kontextmenü des Knotens **Update** den Punkt **Sicheres Datenbanken-Update wird gestartet** aus.

   Das Willkommensfenster des Assistenten für das sichere Update der Programm-Datenbanken wird geöffnet. Klicken Sie auf die Schaltfläche **Weiter >**.

2. Wählen Sie aus der Dropdown-Liste den angeschlossenen sicheren Wechseldatenträger aus, der die Antiviren-Datenbanken des Programms enthält.

   Als sicherer Wechseldatenträger kann nur ein Rutoken-Wechseldatenträger verwendet werden, der durch eine Regel der Komponente Gerätekontrolle ausdrücklich autorisiert wurde.

3. Geben Sie die PIN für den Rutoken-Wechseldatenträger ein, die beim Schritt Kopieren der Programm-Datenbanken festgelegt wurde.

4. Klicken Sie auf **Fertig**.

Die Aufgabe zum sicheren Update der Programm-Datenbanken wird gestartet. Die Programm-Datenbanken werden von dem Rutoken-Wechseldatenträger kopiert.

Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security

Vor dem Update der Datenbanken legt Kaspersky Embedded Systems Security Backup-Kopien der bis dahin verwendeten Datenbanken an. Wenn eine Aktualisierung unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zum zuletzt installierten Datenbank-Update zurück.

Wenn nach einem Datenbanken-Update Probleme auftreten, können Sie die Datenbanken mit den zuvor installierten Updates wiederherstellen. Starten Sie dazu die Aufgabe *Rollback des letzten Updates*.

So starten Sie die Aufgabe Rollback des letzten Updates:

1. Öffnen Sie in der Struktur der Anwendungskonsole den Abschnitt **Update → Rollback des letzten Updates**.

2. Klicken Sie im Ergebnisbereich auf den Link **Starten**.

Statistik zu Update-Aufgaben

Während die Update-Aufgabe ausgeführt wird, können Sie in Echtzeit Informationen über das seit dem Aufgabenstart heruntergeladene Volumen der Daten, sowie eine Statistik über die Aufgabenausführung anzeigen.

Wenn die Aufgabe abgeschlossen ist oder abgebrochen wurde, ist die Information im Protokoll der Aufgabenausführung verfügbar.

So zeigen Sie Update-Statistik an:

Öffnen Sie in der Struktur der Anwendungskonsole den Abschnitt **Update → Update der Datenbanken und Programm-Module**.

Im Ergebnisbereich unter **Statistik** finden Sie Informationen über die Gesamtmenge der abgerufenen Daten.

Backup-Kopien von Objekten erstellen

Hier erfahren Sie, wie Sie für erkannte schädliche Objekte vor der Desinfektion oder dem Löschen eine Backup-Kopie anlegen.

Backup-Kopien von Objekten erstellen. Datenverwaltung

Kaspersky Embedded Systems Security speichert verschlüsselte Kopien desinfizierter oder gelöschter Objekte im Ordner Backup.

Wenn ein Objekt Bestandteil eines zusammengesetzten Objekts ist (z. B. zu einem Archiv gehört), wird das gesamte zusammengesetzte Objekt von Kaspersky Embedded Systems Security ins Backup kopiert. Wenn Kaspersky Embedded Systems Security z. B. ein Objekt aus einer Mail-Datenbank als infiziert einstuft, wird die komplette Mail-Datenbank gesichert.

Wenn ein Objekt, das von Kaspersky Embedded Systems Security ins Backup kopiert wird, umfangreich ist, kann sich das System verlangsamen und der verfügbare Festplattenplatz kann sich verringern.

Sie können Dateien aus dem Backup entweder im ursprünglichen Ordner oder in einem anderen Ordner auf dem geschützten Gerät wiederherstellen. Eine Datei kann aus dem Backup wiederhergestellt werden, z. B. wenn eine infizierte Datei wichtige Informationen enthält, aber Kaspersky Embedded Systems Security nicht in der Lage ist, die Datei zu desinfizieren ohne die Integrität zu beschädigen und Daten zu verlieren.

Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des geschützten Geräts führen.

Objekte im Backup anzeigen

Dieser Abschnitt enthält Informationen darüber, wie Sie die Liste der Dateien im Backup anzeigen können.

So zeigen Sie Backup-Objekte an (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Speicher** aus.
3. Gehen Sie zum Ordner **Backup**.
4. Die Informationen über die im Backup befindlichen Objekte werden auf der rechten Seite der Konsole angezeigt.

So zeigen Sie Backup-Objekte an (in der Kaspersky Security Center Web Console)

1. Öffnen Sie die Web Console.
2. Wählen Sie in der Konsolenstruktur den Punkt **Vorgänge** → **Speicher** aus.

3. Gehen Sie zum Ordner **Backup**.

4. Die Informationen über die im Backup befindlichen Objekte werden auf der rechten Seite der Konsole angezeigt.

So zeigen Sie Backup-Objekte an (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Speicher → Backup** aus.

2. Die Informationen über die im Backup befindlichen Objekte werden auf der rechten Seite der Konsole angezeigt.

Um ein bestimmtes Objekt in der Liste der Backup-Objekte zu finden,

sortieren Sie die Objekte oder verwenden Sie einen Filter.

Dateien aus Backup wiederherstellen

Kaspersky Embedded Systems Security speichert Dateien im Backup im verschlüsselten Format, damit das geschützte Gerät vor schädlichen Wirkungen bewahrt wird.

Sie können Dateien aus dem Backup wiederherstellen.

In den folgenden Fällen müssen Sie möglicherweise eine Datei wiederherstellen:

- Die Ursprungsdatei, die sich als infiziert herausgestellt hat, enthielt wichtige Informationen und Kaspersky Embedded Systems Security konnte bei der Reparatur dieser Datei deren Integrität nicht retten, sodass auf die Informationen deshalb nicht mehr zugegriffen werden kann.

- Sie schätzen die Datei als nicht gefährlich für das geschützte Gerät ein und wollen sie benutzen. Damit Kaspersky Embedded Systems Security diese Datei bei künftigen Untersuchungen nicht als infiziert einstuft, können Sie sie von der Untersuchung in der Aufgabe zum Echtzeitschutz für Dateien und in den Aufgaben zur Echtzeitschutz für Dateien ausschließen.

Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des geschützten Geräts führen.

Wenn Sie eine Datei wiederherstellen, können Sie auswählen, wo sie gespeichert werden soll: am ursprünglichen Speicherort (Standard), in einem speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Gerät oder in einem benutzerdefinierten Ordner auf dem geschützten Gerät, auf dem die Anwendungskonsole installiert ist.

Wenn Kaspersky Embedded Systems Security eine Datei wiederherstellt, wird standardmäßig eine Kopie im Backup angelegt. Nach der Wiederherstellung können Sie die Backup-Kopie aus dem Backup entfernen.

Backup-Dateien wiederherstellen (in der Kaspersky Security Center-Verwaltungskonsole)

1. Wählen Sie in der Struktur der Kaspersky Security Center-Verwaltungskonsole den Ordner **Erweitert → Speicher** aus.

2. Gehen Sie zum Ordner **Backup**.

3. Führen Sie einen der folgenden Schritte aus:

   - Um ein Objekt wiederherzustellen, wählen Sie im Kontextmenü des Objekts den Punkt **Wiederherstellen** aus.
   - Um mehrere Objekte wiederherzustellen, wählen Sie die zu löschenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der ausgewählten Objekte und wählen Sie **Wiederherstellen** aus.

4. Das Objekt wird im ursprünglichen Ordner wiederhergestellt.

Dateien aus dem Backup wiederherstellen (in der Kaspersky Security Center Web Console)

1. Öffnen Sie die Web Console.
2. Wählen Sie in der Konsolenstruktur den Punkt **Vorgänge → Speicher** aus.
3. Gehen Sie zum Ordner **Backup**.
4. Wählen Sie die Objekte aus der Liste aus und klicken Sie auf die Schaltfläche **Wiederherstellen**.
5. Das Objekt wird im ursprünglichen Ordner wiederhergestellt.

Dateien aus dem Backup wiederherstellen (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Speicher → Backup** aus.
2. Führen Sie im Ergebnisfenster des Knotens **Backup** eine der folgenden Aktionen aus:

   - Wählen Sie zur Wiederherstellung eines Objekts im Kontextmenü des Objekts, das Sie wiederherstellen wollen, den Punkt **Wiederherstellen** aus.
   - Um mehrere Objekte wiederherzustellen, wählen Sie die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der ausgewählten Objekte und wählen Sie **Wiederherstellen** aus.

3. Geben Sie im Fenster **Objekt wiederherstellen** für jedes ausgewählte Objekt den Ordner an, in dem das wiederhergestellte Objekt gespeichert werden soll.

   Der Name des Objekts wird im Feld **Objekt** im oberen Bereich des Fensters angezeigt. Wenn Sie mehrere Objekte ausgewählt haben, wird der Name des ersten Objekts in der Liste der ausgewählten Objekte angezeigt.

4. Führen Sie einen der folgenden Schritte aus:

   - Um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im ursprünglichen Ordner wiederherstellen**.
   - Um ein Objekt in dem Ordner wiederherzustellen, den Sie bei der Programm-Installation als Speicherort für wiederhergestellte Objekte angegeben haben, wählen Sie **Im Standard-Wiederherstellungsordner wiederherstellen** aus.
   - Um ein Objekt in einem anderen Ordner auf dem geschützten Gerät zu speichern, auf dem die Anwendungskonsole installiert ist, wählen Sie **In einem Ordner auf Ihrem lokalen Computer wiederherstellen** und wählen dann den gewünschten Ordner oder geben den Pfad dazu an.

5. Wenn Sie nach der Wiederherstellung keine Kopie der Datei im Backup-Ordner speichern möchten, aktivieren Sie das Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Speicher entfernen** (standardmäßig deaktiviert).

6. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

7. Klicken Sie auf **OK**.

8. Kaspersky Embedded Systems Security beginnt damit, das erste ausgewählte Objekt wiederherzustellen.

9. Wenn am angegebenen Ort bereits ein Objekt mit diesem Namen vorhanden ist, wird das Fenster **Ein Objekt mit diesem Namen ist bereits vorhanden** geöffnet.

   a. Wählen Sie eine der folgenden Aktionen für Kaspersky Embedded Systems Security aus:

      - **Ersetzen**, um das vorhandene Objekt mit dem wiederhergestellten Objekt zu ersetzen.
      - **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie den Dateinamen und den vollständigen Pfad für das neue wiederhergestellte Objekt ein.
      - **Umbenennen mit Suffix**, um das wiederhergestellte Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie im Eingabefeld das Suffix ein.

   b. Wenn Sie mehrere Objekte zur Wiederherstellung ausgewählt haben, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**, um die ausgewählte Aktion (**Ersetzen** oder **Umbenennen**) auf die übrigen ausgewählten Objekte anzuwenden. Wenn Sie **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, steht das Kontrollkästchen **Umbenennen** nicht zur Verfügung.

   c. Klicken Sie auf **OK**.

      Das Objekt wird wiederhergestellt. Informationen über den Wiederherstellungsvorgang werden im Systemaudit-Protokoll aufgezeichnet.

Wenn Sie im Fenster **Objekt wiederherstellen** nicht **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, öffnet sich das Fenster **Objekt wiederherstellen** noch einmal. Verwenden Sie dieses Fenster, um den Speicherort anzugeben, an dem das nächste ausgewählte Objekt gespeichert werden soll.

Dateien aus Backup löschen

Backup-Dateien löschen (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.

2. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert → Speicher** aus.

3. Gehen Sie zum Ordner **Backup**. Im rechten Bereich wird eine Liste der Objekte im Backup angezeigt.

4. Führen Sie einen der folgenden Schritte aus:

    - Um ein Objekt zu löschen, klicken Sie im Kontextmenü des Objekts auf **Löschen**.
    - Um mehrere Objekte zu löschen, wählen Sie die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der ausgewählten Objekte und wählen Sie **Löschen** aus.

5. Die ausgewählten Objekte werden aus dem Backup gelöscht.

Dateien aus dem Backup löschen (in der Kaspersky Security Center Web Console)

1. Öffnen Sie die Web Console.
2. Wählen Sie in der Konsolenstruktur den Punkt **Vorgänge → Speicher** aus.
3. Gehen Sie zum Ordner **Backup**.
4. Wählen Sie die Objekte aus der Liste aus und klicken Sie auf die Schaltfläche **Löschen**.
5. Die ausgewählten Objekte werden aus dem Backup gelöscht.

Dateien aus dem Backup löschen (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Speicher → Backup** aus.
2. Im rechten Bereich wird eine Liste der Objekte im Backup angezeigt.
3. Führen Sie einen der folgenden Schritte aus:

    - Um ein Objekt zu löschen, klicken Sie im Kontextmenü des Objekts auf **Löschen**.
    - Um mehrere Objekte zu löschen, wählen Sie die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der ausgewählten Objekte und wählen Sie **Löschen** aus.

4. Die ausgewählten Objekte werden aus dem Backup gelöscht.

Möglicherweise infizierte Quarantäneobjekte zur Analyse an Kaspersky einschicken

Wenn das Verhalten eines bestimmten Objekts darauf hinweist, dass es eine Bedrohung enthält, Kaspersky Embedded Systems Security das Objekt jedoch als virenfrei einstuft, handelt es sich möglicherweise um eine unbekannte Bedrohung, deren Beschreibung noch nicht in den Datenbanken verzeichnet ist. Sie können dieses Objekt zur Analyse an Kaspersky schicken. Die Viren-Analytiker von Kaspersky untersuchen die Datei. Wenn sie eine neue Bedrohung finden, wird den Datenbanken ein entsprechender Eintrag und ein Desinfektionsalgorithmus hinzugefügt. Wenn Sie das Objekt nach einem Datenbanken-Update erneut untersuchen, ist es wahrscheinlich, dass Kaspersky Embedded Systems Security die Datei als infiziert einstuft und sie desinfizieren kann. Dadurch können Sie nicht nur das Objekt retten, sondern auch dabei helfen, eine Virenepidemie zu verhindern.

So senden Sie ein Objekt zur Analyse an die Kaspersky-Experten (in der Kaspersky Security Center-Verwaltungskonsole)

1. Öffnen Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur den Punkt **Erweitert** → **Speicher** aus.
3. Gehen Sie zum Ordner **Backup**.
4. Führen Sie einen der folgenden Schritte aus:
   - Um ein Objekt zu senden, wählen Sie im Kontextmenü des Objekts den Punkt **An Kaspersky senden** aus.
   - Um mehrere Objekte zu senden, wählen Sie die entsprechenden Objekte mithilfe der Taste STRG oder UMSCHALT aus. Öffnen Sie anschließend das Kontextmenü eines der markierten Objekte und klicken Sie dort auf **An Kaspersky senden**.
5. Wählen Sie den Ordner aus, in dem das Objekt auf Ihrem Computer gespeichert werden soll.
6. Danach werden Sie aufgefordert, zur Plattform des Kaspersky Threat Intelligence Portal zu wechseln und das gespeicherte Objekt hochzuladen, um vollständige Informationen darüber zu erhalten.

So senden Sie ein Objekt zur Analyse an die Kaspersky-Experten (in der Kaspersky Security Center Web Console)

1. Öffnen Sie die Web Console.
2. Wählen Sie in der Konsolenstruktur den Punkt **Vorgänge** → **Speicher** aus.
3. Gehen Sie zum Ordner **Datei-Backups**.
4. Wählen Sie die Objekte aus der Liste aus und klicken Sie auf die Schaltfläche **An Kaspersky senden**.
5. Wählen Sie den Ordner aus, in dem das Objekt auf Ihrem Computer gespeichert werden soll.
6. Danach werden Sie aufgefordert, zur Plattform des Kaspersky Threat Intelligence Portal zu wechseln und das gespeicherte Objekt hochzuladen, um vollständige Informationen darüber zu erhalten.

Kaspersky Security Center Web Console oder die Administrationskonsole können nicht verwendet werden, um Backup-Objekte zur Analyse an Kaspersky zu senden, falls sie nach einem Upgrade von Programmversion 3.4 oder früher auf Version 4.0 oder höher migriert wurden.

Backup-Einstellungen anpassen

So konfigurieren Sie die Backup-Einstellungen (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Zusätzlich** → **Speicher** aus und klicken Sie auf **Einstellungen**.

4. Gehen Sie auf die Registerkarte **Backup**.
5. Geben Sie die Backup-Einstellungen an (siehe folgende Tabelle).
6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Backup-Einstellungen (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 Embedded Systems Security.
   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie **Zusätzlich → Speicher** aus und klicken Sie auf die Schaltfläche **Anpassen**.
5. Gehen Sie auf die Registerkarte **Backup**.
6. Geben Sie die Backup-Einstellungen an (siehe folgende Tabelle).
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Backup-Einstellungen (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Speicher → Backup** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Backup** auf **Eigenschaften**.
3. Geben Sie im Fenster **Eigenschaften: Backup** die Backup-Einstellungen an (siehe folgende Tabelle).
4. Speichern Sie die vorgenommenen Änderungen.

Backup-Einstellungen

Einstellung	Beschreibung
Objekte speichern für maximal	Wenn diese Funktionalität aktiviert ist, wird die maximale Speicherdauer für Dateien durch den festgelegten Wert beschränkt. Die maximale Speicherdauer für Dateien beträgt standardmäßig 30 Tage. Nach Ablauf der maximalen Speicherdauer löscht Kaspersky Embedded Systems Security die ältesten Dateien aus dem Backup.
Maximale Größe des Backups	Wenn diese Funktionalität aktiviert ist, überwacht Kaspersky Embedded Systems Security die Gesamtgröße der Objekte, die im Backup abgelegt werden können. Bei einer Überschreitung des vorgegebenen Wertes (als Standard gelten 400 MB) protokolliert Kaspersky Embedded Systems Security das Ereignis *Maximale Größe des Backups wurde überschritten* und benachrichtigt gemäß den Einstellungen für Benachrichtigungen über Ereignisse dieses Typs. Wenn diese Funktionalität aktiviert ist, überwacht Kaspersky Embedded Systems Security die Gesamtgröße der Objekte im Backup nicht. Die Funktionalität ist standardmäßig deaktiviert.

Einstellung	Beschreibung
Grenzwert für verfügbaren Speicherplatz beschränken auf	Wenn diese Funktionalität aktiviert ist, überwacht Kaspersky Embedded Systems Security, wie viel freien Speicherplatz es im Backup gibt (Standardwert 100 MB). Ist der Umfang des freien Speicherplatzes kleiner als der vorgegebene Grenzwert, protokolliert Kaspersky Embedded Systems Security das Ereignis *Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* und benachrichtigt gemäß den Benachrichtigungseinstellungen über Ereignisse dieses Typs. Das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz beschränken auf** ist aktiv, wenn das Kontrollkästchen **Maximale Größe des Backups** aktiviert ist. Diese Option ist standardmäßig aktiviert.

Überschreitet der Umfang der im Backup befindlichen Objekte die maximale Größe des Backups oder den Grenzwert für den verfügbaren Speicherplatz, so werden Sie von Kaspersky Embedded Systems Security hierüber benachrichtigt, wobei die Objekte jedoch trotzdem ins Backup verschoben werden.

Backup-Statistik

In der so genannten Backup-Statistik können Sie Informationen über den aktuellen Status des Backups erhalten.

Um eine Statistik für das Backup anzuzeigen:

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Speicher → Backup** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Backup** auf **Statistik**.

   Dadurch wird das Fenster **Backup. Statistik** geöffnet. Im Fenster **Backup-Statistik** werden Informationen über den aktuellen Status des Backups angezeigt (s. Tabelle unten).

Informationen über den aktuellen Backup-Status

Feld	Beschreibung
Aktuelle Größe des Backups	Gesamtgröße der Daten im Backup-Ordner. Die Größe bezieht sich auf die verschlüsselten Dateien.
Objekte insgesamt	Aktuelle Anzahl der Objekte im Backup.

Zugriff auf Netzwerkressourcen blockieren. Blockierte Netzwerksitzungen

In diesem Abschnitt wird beschrieben, wie Sie Remote-Geräte blockieren und die Einstellungen für die Liste der blockierten Netzwerksitzungen anpassen.

Liste der blockierten Netzwerksitzungen

Standardmäßig ist die Liste der blockierten Netzwerksitzungen verfügbar, wenn eine der folgenden Komponenten installiert ist: Schutz vor Netzwerkbedrohungen oder Verhaltensanalyse. Diese Komponenten erkennen per Fernzugriff ausgeführte Versuche, Objekte auf dem geschützten Gerät oder über ein NAS freigegebene Ordner zu verschlüsseln, zu öffnen oder auszuführen, gemäß der Liste der blockierten Netzwerksitzungen. Informationen über blockierte Netzwerksitzungen auf allen geschützten Geräten werden an Kaspersky Security Center gesendet. Kaspersky Embedded Systems Security blockiert die aktuelle Sitzung und macht freigegebene Ordner oder an das Netzwerk angeschlossene Speicherordner nicht mehr verfügbar.

Die Liste der blockierten Netzwerksitzungen wird befüllt, wenn mindestens eine der folgenden Aufgaben im aktiven Modus gestartet wird (unter festgelegten Bedingungen):

- Für die Aufgabe zum *Schutz vor Netzwerkbedrohungen*: Es werden Aktivitäten erkannt, die typisch für Netzwerkangriffe sind.

  Kaspersky Embedded Systems Security löscht die Sperrliste, wenn das Programm neu gestartet wird und wenn die Einstellungen für den „Schutz vor Netzwerkbedrohungen“ geändert werden.

- Für die Aufgabe „*Verhaltensanalyse*“: Es wurde eine bösartige Verschlüsselung durch ein Gerät erkannt, das auf Dateiressourcen im Netzwerk zugreift.

Wenn eine bösartige Aktivität oder ein Verschlüsselungsversuch erkannt wird, sendet die Aufgabe Informationen über die angreifende Netzwerksitzung an die Liste der blockierten Netzwerksitzungen, und das Programm erstellt ein Ereignis der Stufe *Warnung* für die aktuelle Sitzung des angreifenden Hosts. Alle Versuche, über diese Sitzung auf geschützte freigegebene Netzwerkordner zuzugreifen, werden blockiert.

Wenn der lokal eindeutige Identifikator (LUID) des Hosts, der die angreifende Netzwerksitzung initiiert hat, zur Liste der blockierten Netzwerksitzungen hinzugefügt wird, ermittelt Kaspersky Embedded Systems Security die IP-Adresse des Hosts und fügt sie anstelle der LUID des angreifenden Hosts zur Liste der blockierten Netzwerksitzungen hinzu.

Standardmäßig entfernt Kaspersky Embedded Systems Security blockierte Hosts 30 Minuten, nachdem sie zur Liste hinzugefügt wurden, aus der Liste. Der Zugriff auf freigegebene Netzwerkordner wird automatisch wiederhergestellt, nachdem die Netzwerksitzungen aus der Liste der blockierten Netzwerksitzungen gelöscht wurden. Sie können einen Zeitraum angeben, nach dem die blockierten Netzwerksitzungen automatisch entsperrt werden.

Beachten Sie, dass die Liste der blockierten Netzwerksitzungen weiterhin verfügbar ist, wenn Sie für ein beliebiges Benutzerkonto den Zugriff auf die Speicherverwaltung beschränken. Die Einstellungen für blockierte Hosts kann nicht geändert werden, es sei denn, das ausgewählte Benutzerkonto verfügt über **Berechtigungen bearbeiten** für die Verwaltung von Kaspersky Embedded Systems Security.

Liste der blockierten Netzwerksitzungen verwalten

Damit Sie Netzwerksitzungen, die eine schädliche Aktivität oder Verschlüsselungsaktivität aufweisen, zur Liste der blockierten Netzwerksitzungen hinzufügen und den Zugriff auf freigegebene Netzwerkordner für diese Sitzungen blockieren können, muss mindestens eine der folgenden Komponenten aktiviert sein:

- Schutz vor Netzwerkbedrohungen
- Verhaltensanalyse.

Sperrung von nicht vertrauenswürdigen Hosts aktivieren (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Punkt **Kontrolle der Netzwerkaktivität → Einstellungen für den Schutz vor Netzwerkbedrohungen** aus und klicken Sie auf **Einstellungen**.
4. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Schutz vor Netzwerkbedrohungen**.
5. Aktivieren Sie auf der Registerkarte **Allgemein** den Modus **Verbieten**.
6. Aktivieren Sie das Kontrollkästchen **Angreifende Geräte sperren für** und geben Sie die Sperrdauer an.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Sperrung von nicht vertrauenswürdigen Netzwerksitzungen für die Komponente Verhaltensanalyse in den Richtlinieneigenschaften:

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 den Punkt **Echtzeit-Computerschutz → Verhaltensanalyse** aus und klicken Sie auf **Einstellungen**.
4. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Verhaltensanalyse**.
5. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner** und aktivieren Sie das Kontrollkästchen **Freigegebene Ordner schützen**.
6. Wählen Sie **Verbindung blockieren für** aus und geben Sie die Sperrdauer an.
7. Geben Sie bei Bedarf die Schutzbereiche und Ausnahmen nach IP-Adresse und Maske an.
8. Speichern Sie die vorgenommenen Änderungen.

Sperrung von nicht vertrauenswürdigen Hosts aktivieren (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Kontrolle der Netzwerkaktivität → Schutz vor Netzwerkbedrohungen** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Schutz vor Netzwerkbedrohungen aktivieren**.
6. Aktivieren Sie den Modus **Blockieren**.
7. Aktivieren Sie das Kontrollkästchen **Angreifende Geräte sperren für** und geben Sie die Sperrdauer an.
8. Geben Sie bei Bedarf Ausnahmen nach der IP-Adresse an.
9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Sperrung von nicht vertrauenswürdigen Netzwerksitzungen für die Komponente Verhaltensanalyse:

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung → Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Echtzeit-Computerschutz → Verhaltensanalyse** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Verhaltensanalyse aktivieren**.
6. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner** und aktivieren Sie das Kontrollkästchen **Schutz vor der externen Verschlüsselung freigegebener Ordner aktivieren**.
7. Wählen Sie **Verbindung blockieren** aus und geben Sie im Abschnitt **Wenn eine externe Verschlüsselung freigegebener Ordner erkannt wird** die Sperrdauer an.
8. Geben Sie bei Bedarf die Schutzbereiche und Ausnahmen nach IP-Adresse und Maske an.
9. Speichern Sie die vorgenommenen Änderungen.

Sperrung von nicht vertrauenswürdigen Hosts aktivieren (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Schutz vor Netzwerkbedrohungen** aus.
2. Klicken Sie im Ergebnisbereich des Knotens **Schutz vor Netzwerkbedrohungen** auf **Eigenschaften**.

   Das Fenster **Eigenschaften: Schutz vor Netzwerkbedrohungen** wird geöffnet.
3. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Schutz vor Netzwerkbedrohungen**.

4. Aktivieren Sie auf der Registerkarte **Allgemein** den Modus **Verbieten**.

5. Aktivieren Sie das Kontrollkästchen **Angreifende Geräte sperren für** und geben Sie die Sperrdauer an.

6. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Sperrung von nicht vertrauenswürdigen Netzwerksitzungen für die Komponente Verhaltensanalyse:

1. Wählen Sie in der Struktur der Konsole für Kaspersky Embedded Systems Security den Punkt **Echtzeit-Computerschutz → Schutz vor Verschlüsselung** aus.

2. Klicken Sie im Ergebnisbereich des Knotens **Verhaltensanalyse** auf **Eigenschaften**.

3. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Verhaltensanalyse**.

4. Gehen Sie auf die Registerkarte **Schutz für freigegebene Ordner** und aktivieren Sie das Kontrollkästchen **Freigegebene Ordner schützen**.

5. Wählen Sie **Verbindung blockieren für** aus und geben Sie die Sperrdauer an.

6. Geben Sie bei Bedarf die Schutzbereiche und Ausnahmen nach IP-Adresse und Maske an.

7. Speichern Sie die vorgenommenen Änderungen.

Liste der blockierten Sitzungen konfigurieren (in der Anwendungskonsole)

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Speicher**.

2. Wählen Sie den untergeordneten Knoten **Blockierte Netzwerksitzungen** aus.

3. Klicken Sie im Ergebnisbereich auf die Schaltfläche **Eigenschaften**.

4. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Angreifende Geräte sperren für** und geben Sie die Sperrdauer an.

5. Um den Zugriff auf alle blockierten Netzwerksitzungen wiederherzustellen, klicken Sie im oberen Fensterbereich auf **Alle entsperren**.

   Alle Netzwerksitzungen werden aus der Liste entfernt und entsperrt.

6. Um Netzwerksitzungen aus der Liste der blockierten Netzwerksitzungen zu entfernen, wählen Sie in der Liste im Ergebnisbereich eine oder mehrere Sitzungen aus und klicken Sie im oberen Fensterbereich auf **Ausgewählte entsperren**.

   Die Sperre der ausgewählten Netzwerksitzungen wird aufgehoben.

Registrierung von Ereignissen. Berichte in Kaspersky Embedded Systems Security

In diesem Abschnitt finden Sie Informationen zur Arbeit mit den Protokollen von Kaspersky Embedded Systems Security.

Möglichkeiten zur Registrierung der Dienste von Kaspersky Embedded Systems Security

Ereignisse werden in Kaspersky Embedded Systems Security in zwei Gruppen aufgeteilt:

- Ereignisse im Zusammenhang mit dem Betrieb der Programmkomponenten, die Objekte in den Aufgaben von Kaspersky Embedded Systems Security verarbeiten.
- Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security, beispielsweise Programmstart, Erstellen oder Löschen von Aufgaben, Bearbeiten der Aufgabeneinstellungen.

Kaspersky Embedded Systems Security verwendet die folgenden Methoden zum Protokollieren von Ereignissen:

- **Protokolle der Programmkomponenten**. Protokolle enthalten Informationen über Ereignisse, die während des Betriebs von Programmkomponenten aufgetreten sind.
- **Systemaudit-Protokoll**. Das Systemaudit-Protokoll enthält Informationen über Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security. Es enthält auch Informationen über Ereignisse, die mit Sicherheitsverstößen oder versuchten Sicherheitsverstößen auf dem geschützten Gerät zusammenhängen.
- **Ereignisprotokoll**. Das Ereignisprotokoll enthält Informationen über Ereignisse, die für die Crash-Diagnose von Kaspersky Embedded Systems Security erforderlich sind. Der Ereignisbericht ist in der Konsole "Event Viewer" von Microsoft Windows verfügbar.

Die unter den folgenden Links zum Download verfügbaren Dateien enthalten Tabellen mit allen Ereignissen von Kaspersky Embedded Systems Security für folgende Kategorien:

- Ereignisse, die von Kaspersky Embedded Systems Security in das Ereignisprotokoll geschrieben werden.

   WEL-EVENTS.ZIP HERUNTERLADEN

- Ereignisse, die von Kaspersky Embedded Systems Security an den Administrationsserver gesendet werden.

   KSC-EVENTS.ZIP HERUNTERLADEN

Einstellungen für Protokolle konfigurieren

Sie können folgenden Einstellungen der Protokolle von Kaspersky Embedded Systems Security anpassen:

- Aufbewahrungsdauer der Ereignisse in den Protokollen der Aufgabenausführung und im Systemaudit-Protokoll.
- Pfad des Ordners, in dem Kaspersky Embedded Systems Security die Log-Dateien der Protokolle der Aufgabenausführung und die Systemaudit-Protokolldatei speichert.
- Schwellenwerte für die Ereignisgenerierung für *Datenbanken sind veraltet*, *Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche wurde lange nicht ausgeführt*.
- Ereignisse, die Kaspersky Embedded Systems Security in den Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisbericht von Kaspersky Embedded Systems Security in der Ereignisanzeige speichert.
- Ereignisse, die von Kaspersky Embedded Systems Security an den SIEM-Server gesendet werden.

So konfigurieren Sie die Protokollierungseinstellungen (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Protokolle und Meldungen** aus.
4. Klicken Sie im Abschnitt **Aufgabenprotokolle** auf **Einstellungen**.

   Das Fenster **Benachrichtigungen** wird geöffnet.
5. Wählen Sie in diesem Fenster das Protokoll aus, das Sie konfigurieren möchten, und passen Sie die Einstellungen für die einzelnen Ereignisse an:
   - Speicherort für Ereignisse: lokaler Bericht oder Windows-Ereignisprotokoll.
   - Ereignisbenachrichtigungen: Per E-Mail informieren, Benachrichtigung per Terminal-Dienst und/oder Benachrichtigung durch den Start einer ausführbaren Datei.
   - Ob Sie das Ereignis an einen SIEM-Server und/oder an Kaspersky Security Center senden möchten.
6. Konfigurieren Sie die Schwellenwerte für die Ereignisgenerierung. Klicken Sie dazu auf **Grenzwerteinstellungen für Ereigniserstellung**.
7. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster an, nach wie vielen Tagen die folgenden Ereignisse registriert werden sollen: *Datenbanken sind veraltet*, *Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche wurde lange nicht ausgeführt*.
8. Konfigurieren Sie die E-Mail-Benachrichtigungen. Klicken Sie dazu auf **E-Mail-Benachrichtigungseinstellungen**.
9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Protokollierungseinstellungen (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Gehen Sie zu **Protokolle und Meldungen** → **Aufgabenprotokolle** und klicken Sie auf die Schaltfläche **Anpassen**.
5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster auf der Registerkarte **Benachrichtigungen** das Protokoll aus, das Sie konfigurieren möchten, und geben Sie die Einstellungen für die einzelnen Ereignisse an:

   - Speicherort für Ereignisse: lokaler Bericht oder Windows-Ereignisprotokoll.
   - Ereignisbenachrichtigungen: Per E-Mail informieren, Benachrichtigung per Terminal-Dienst und/oder Benachrichtigung durch den Start einer ausführbaren Datei.
   - Ob Sie das Ereignis an einen SIEM-Server und/oder an Kaspersky Security Center senden möchten.
6. Konfigurieren Sie die E-Mail-Benachrichtigungen auf der Registerkarte **Einstellungen für E-Mail-Benachrichtigungen**.
7. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie die Protokollierungseinstellungen (in der Anwendungskonsole):

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Meldungen**.
2. Wählen Sie den Punkt **Eigenschaften**.

   Das Fenster **Meldungen** wird geöffnet.
3. Wählen Sie in diesem Fenster das Protokoll aus, das Sie konfigurieren möchten, und passen Sie die Einstellungen für die einzelnen Ereignisse an:

   - Speicherort für Ereignisse: lokaler Bericht oder Windows-Ereignisprotokoll.
   - Ereignisbenachrichtigungen: Per E-Mail informieren, Benachrichtigung per Terminal-Dienst und/oder Benachrichtigung durch den Start einer ausführbaren Datei.
   - Ob Sie das Ereignis an einen SIEM-Server und/oder an Kaspersky Security Center senden möchten.
4. Konfigurieren Sie die Schwellenwerte für die Ereignisgenerierung. Klicken Sie dazu auf **Grenzwerteinstellungen für Ereigniserstellung**.
5. Dadurch wird ein Fenster geöffnet. Geben Sie in diesem Fenster an, nach wie vielen Tagen die folgenden Ereignisse registriert werden sollen: *Datenbanken sind veraltet (Tage)*, *Datenbanken sind stark veraltet (Tage)* und *Untersuchung wichtiger Bereiche wurde lange nicht durchgeführt (Tage)*.
6. Konfigurieren Sie die E-Mail-Benachrichtigungen. Klicken Sie dazu auf **E-Mail-Benachrichtigungseinstellungen**.
7. Speichern Sie die vorgenommenen Änderungen.

Ereignisse im Protokoll sortieren

Standardmäßig werden die Ereignisse im Protokoll in umgekehrter chronologischer Reihenfolge dargestellt.

So sortieren Sie die Ereignisse im Protokoll:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Meldungen**.
2. Wählen Sie das gewünschte Protokoll aus.
3. Klicken Sie im Ergebnisbereich auf den Titel der Spalte, nach deren Inhalt die Ereignisse in der Ereignisliste sortiert werden sollen.

Die sortierten Ergebnisse bleiben gespeichert, bis Sie das Protokoll zum nächsten Mal anzeigen.

Ereignisse im Protokoll filtern

Sie können das Protokoll so konfigurieren, dass nur die Ereigniseinträge angezeigt werden, die den festgelegten Filterkriterien (Filtern) entsprechen.

So filtern Sie Ereignisse im Protokoll:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Meldungen**.
2. Wählen Sie das Protokoll aus, für das Sie einen Filter konfigurieren möchten, und klicken Sie im Ergebnisbereich auf **Filter**.

   Das Fenster **Filtereinstellungen** wird geöffnet.
3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie in der Liste **Feldname** die Spalte aus, nach der Sie die Ereignisse filtern möchten.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen aus. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.
   c. Wählen Sie unter **Feldwert** den Filterwert.
   d. Klicken Sie auf **Hinzufügen**.

Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.

4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:

   - Um mehrere Filter mithilfe des logischen Operators „UND“ zu kombinieren, wählen Sie **Wenn alle Bedingungen erfüllt sind** aus.
   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.

5. Klicken Sie auf **OK**, um die Filterkriterien für Protokollereignisse zu speichern.

   In der Ereignisliste des Protokolls werden nur Ereignisse angezeigt, die den Filterkriterien entsprechen. Die gefilterten Ergebnisse bleiben gespeichert, bis Sie das Protokoll zum nächsten Mal anzeigen.

Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Meldungen**.
2. Wählen Sie das Protokoll aus, für das Sie einen Filter entfernen möchten, und klicken Sie auf **Filter entfernen**.

   Dann werden alle Ereignisse im Protokoll angezeigt.

Ereignisse aus dem Protokoll löschen

Kaspersky Embedded Systems Security bewahrt Protokolleinträge standardmäßig für 30 Tage auf. Sie können die Aufbewahrungsdauer für Einträge in einem Protokoll ändern.

So löschen Sie Ereignisse aus dem Protokoll:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Meldungen**.
2. Wählen Sie das Protokoll aus, aus dem Sie Ereignisse löschen möchten, und klicken Sie im Ergebnisbereich auf **Leeren**.
3. Bestätigen Sie den Löschvorgang.

   Das Protokoll wird gelöscht.

Informationen aus dem Protokoll exportieren

Sie können Daten aus Protokollen in eine csv-Datei oder txt-Datei exportieren.

So exportieren Sie Ereignisse aus Protokollen:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Meldungen**.
2. Wählen Sie ein Protokoll aus und klicken Sie im Ergebnisbereich auf **Protokoll exportieren**.

   Das Fenster **Speichern unter** wird geöffnet.

3. Geben Sie den Namen, den Speicherort und den Typ der Datei an, in die Sie Daten aus dem Protokoll exportieren möchten.

4. Klicken Sie auf **Speichern**.

Die Informationen aus den Protokollen werden in der angegebenen Datei gespeichert.

Systemaudit-Protokoll

Kaspersky Embedded Systems Security führt für Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security ein Systemaudit durch. Das Programm protokolliert Informationen zum Start des Programms, zum Starten und Stoppen von Kaspersky Embedded Systems Security-Aufgaben, zu Änderungen der Aufgabeneinstellungen sowie zum Erstellen und Löschen von Aufgaben der Direktsuche. Das Programm protokolliert auch Informationen über Ereignisse, die mit Sicherheitsverstößen oder versuchten Sicherheitsverstößen auf dem geschützten Gerät zusammenhängen. Einträge zu diesen Ereignissen werden im Ergebnisbereich angezeigt, wenn Sie in der Programmkonsole den Knoten **Systemaudit** auswählen.

Kaspersky Embedded Systems Security bewahrt Ereignisse standardmäßig für 30 Tage im Systemaudit-Protokoll auf. Sie können die Aufbewahrungsdauer für Einträge in einem Protokoll ändern.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Embedded Systems Security die Log-Dateien des Systemaudit-Protokolls speichert.

Komponenten- und Aufgabenprotokolle

Informationen über den Betrieb der Komponenten und Aufgaben von Kaspersky Embedded Systems Security werden im Ergebnisbereich der Anwendungskonsole angezeigt, wenn Sie einen Knoten mit dem Komponenten- oder Aufgabennamen im Abschnitt **Protokolle und Meldungen** auswählen.

Kaspersky Embedded Systems Security bewahrt die Einträge in den Komponenten- und Aufgabenprotokollen standardmäßig für 30 Tage auf. Für Aufgaben: ab dem Zeitpunkt, zu dem die Aufgabe abgeschlossen wurde. Sie können die Aufbewahrungsdauer für Einträge in Komponenten- und Aufgabenprotokollen ändern.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Embedded Systems Security die Dateien der Komponenten- und Aufgabenprotokollen speichern soll. Ferner können Sie die Ereignisse auswählen, über die Kaspersky Embedded Systems Security Einträge in Komponenten- und Aufgabenprotokollen speichern soll.

In den Protokollen der Aufgabenausführung können Sie detaillierte Informationen über alle Ereignisse, die in den Aufgaben seit ihrem Start aufgetreten sind, sowie eine Statistik über die Aufgabenausführung und die Aufgabeneinstellungen anzeigen.

Um Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in den Berichten über Aufgabenausführung anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Meldungen**.

2. Wählen Sie im Ergebnisbereich die Registerkarte **Statistik** aus.

Ereignisbericht von Kaspersky Embedded Systems Security in der Ereignisanzeige anzeigen

Mithilfe des Snap-Ins „Microsoft Windows-Ereignisanzeige“ für Microsoft Management Console können Sie das Ereignisprotokoll von Kaspersky Embedded Systems Security anzeigen. Darin protokolliert Kaspersky Embedded Systems Security Ereignisse, die für die Crash-Diagnose erforderlich sind.

Sie können auf Grundlage folgender Kriterien Ereignisse auswählen, die im Ereignisprotokoll eingetragen werden sollen:

- **nach Ereignistypen**.
- **nach der Genauigkeitsstufe**. Die Genauigkeitsstufe entspricht der Prioritätsstufe von Ereignissen, die im Bericht registriert werden (informative, wichtige oder kritische Ereignisse). Die Stufe "Informative Ereignisse" bietet die meisten Informationen, da hier die Ereignisse aller Kategorien aufgezeichnet werden. Die Stufe "Kritische Ereignisse" bietet weniger ausführliche Informationen, da hier ausschließlich kritische Ereignisse aufgezeichnet werden.

Um den Ereignisbericht für Kaspersky Embedded Systems Security anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie auf die **Start**-Schaltfläche, geben Sie in der Suchzeile den Befehl `mmc` ein und drücken Sie die **EINGABE**-Taste.

   Die Microsoft Management Console wird geöffnet.

2. Wählen Sie **Datei** > **Snap-in hinzufügen/entfernen** aus.

   Das Fenster **Snap-in hinzufügen/entfernen** wird geöffnet.

3. Wählen Sie in der Liste der verfügbaren Snap-ins das **Snap-in „Ereignisanzeige“** aus und klicken Sie auf **Hinzufügen**.

   Das Fenster **Computer auswählen** wird geöffnet.

4. Geben Sie im Fenster **Computer auswählen** das geschützte Gerät an, auf dem Kaspersky Embedded Systems Security installiert ist, und klicken Sie auf **OK**.

5. Klicken Sie im Fenster **Snap-ins hinzufügen/entfernen** auf **OK**.

   In der Struktur der Microsoft Management Console erscheint der Knoten **Ereignisanzeige**.

6. Öffnen Sie den Knoten **Ereignisanzeige** und wählen Sie den untergeordneten Knoten **Anwendungs- und Dienstprotokolle** > **Kaspersky Embedded Systems Security** aus.

Der Ereignisbericht für Kaspersky Embedded Systems Security wird geöffnet.

Über die SIEM-Integration

Um die Belastung für leistungsschwache Geräte zu reduzieren und Systemleistungsrisiken infolge umfangreicher Programmprotokolle zu verringern, können Sie die Veröffentlichung von Audit-Ereignissen und Aufgabenausführungsereignissen über das syslog-Protokoll auf dem *syslog-Server* einrichten.

Ein syslog-Server ist ein externer Server für Ereignis-Management (SIEM), der eingehende Ereignisse speichert und analysiert sowie andere Protokollverwaltungsaktionen ausführt.

Sie können die SIEM-Integration in zwei Modi verwenden:

- Ereignisse auf dem syslog-Server duplizieren: In diesem Modus werden alle Ereignisse der Aufgabenausführung, deren Veröffentlichung in den Protokolleinstellungen konfiguriert wurde, sowie alle Ereignisse des Systemaudits nach dem Versand an SIEM auch weiterhin auf dem geschützten Gerät gespeichert.

  Wir empfehlen, dass Sie diesen Modus verwenden, um die Last für das geschützte Gerät so gering wie möglich zu halten.

- Lokale Kopien der Ereignisse löschen: In diesem Modus werden alle Ereignisse, die während der Programmausführung registriert und in SIEM veröffentlicht wurden, vom geschützten Gerät gelöscht.

  > Das Programm löscht niemals lokale Versionen des Sicherheitsprotokolls.

Kaspersky Embedded Systems Security kann die Ereignisse in den Programmprotokollen in die vom syslog-Server unterstützten Formate konvertieren, damit sie von SIEM-Server empfangen und erfolgreich identifiziert werden können. Das Programm unterstützt die Konvertierung von Ereignissen in ein Format für strukturierte Daten und in das JSON-Format.

Es wird empfohlen, sich bei der Auswahl des Ereignisformats an der Konfiguration des verwendeten SIEM-Servers zu orientieren.

Anpassen der Einstellungen der SIEM-Integration

Standardmäßig wird die SIEM-Integration nicht verwendet. Sie können die SIEM-Integration aktivieren und deaktivieren und die entsprechenden Einstellungen konfigurieren.

Sie können das Risiko verringern, dass Ereignisse nicht an den SIEM-Server gesendet werden, indem Sie Verbindungen zu mehreren SIEM-Servern konfigurieren.

Kaspersky Embedded Systems Security verbindet sich mit dem ersten SIEM-Server in der Liste. Schlägt ein Verbindungsversuch fehl, versucht Kaspersky Embedded Systems Security eine Verbindung zu anderen Servern aus der Liste herzustellen.

Kaspersky Embedded Systems Security verwendet Systemaudit-Ereignisse, um Sie über erfolglose Verbindungsversuche zum SIEM-Server und Fehler beim Senden von Ereignissen an den SIEM-Server zu benachrichtigen.

So konfigurieren Sie die SIEM-Integration (in der Kaspersky Security Center-Verwaltungskonsole)

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 den Abschnitt **Protokolle und Meldungen** aus.
4. Klicken Sie im Block **SIEM-Integration** auf **Einstellungen**.

   Das Fenster **SIEM-Integration** wird geöffnet.

5. Aktivieren Sie im Block **Integrationseinstellungen** das Kontrollkästchen **Übertragung von Sicherheitsereignissen an einen SIEM-Server aktivieren**.

6. Konfigurieren Sie die Verbindung zum SIEM-Server im Block **Einstellungen der Verbindung zu SIEM-Servern**:

   a. Klicken Sie auf **Hinzufügen**.

   b. Dadurch wird das Fenster **Server hinzufügen** geöffnet. Geben Sie in diesem Fenster die SIEM-Serveradresse (IPv4, DNS), den Port und das Verbindungsprotokoll an.

   c. Klicken Sie auf **Sicherheitseinstellungen für TCP-Verbindungen**.

   d. Dadurch wird das Fenster **Sicherheitseinstellungen für TCP-Verbindungen** geöffnet. Passen Sie in diesem Fenster die Verbindungseinstellungen für den SIEM-Server an (siehe folgende Tabelle).

7. Aktivieren Sie, sofern erforderlich, das Kontrollkästchen **Lokale Kopien für Ereignisse entfernen, die an einen syslog-Remote-Server gesendet wurden** im Block **Einstellungen für die Ereignisübertragung an einen SIEM-Server**. Wenn das Kontrollkästchen aktiviert ist, löscht das Programm die lokalen Kopien der Ereignisse, sobald sie erfolgreich auf dem SIEM-Server veröffentlicht wurden. Es wird empfohlen, diesen Modus auf leistungsschwachen Geräten zu verwenden. Wenn das Kontrollkästchen deaktiviert ist, sendet das Programm lediglich die Ereignisse an den SIEM-Server. Die Kopien der Berichte werden weiterhin lokal gespeichert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   Das Programm löscht niemals lokale Versionen des Sicherheitsprotokolls.

8. Geben Sie im Block **Ereignisformat** das Format an, in das die Programmereignisse konvertiert werden sollen, damit sie an den SIEM-Server gesendet werden können. Die Option **Ereignisse in STRUCTURED-DATA konvertieren** ist standardmäßig ausgewählt. Es wird empfohlen, sich bei der Auswahl des Ereignisformats an der Konfiguration des verwendeten SIEM-Servers zu orientieren.

9. Verriegeln Sie das Vorhängeschloss , um die Richtlinie auf die Computer anzuwenden.

10. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So konfigurieren Sie die SIEM-Integration (in der Kaspersky Security Center Web Console)

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

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

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wählen Sie den Abschnitt **Protokolle und Meldungen** aus.

5. Klicken Sie im Block **SIEM-Integration** auf **Anpassen**.

   Das Fenster **SIEM-Integration** wird geöffnet.

6. Aktivieren Sie das Kontrollkästchen **Übertragung von Sicherheitsereignissen an einen SIEM-Server aktivieren**.

7. Konfigurieren Sie die Verbindung zum SIEM-Server im Block **Einstellungen der Verbindung zu SIEM-Servern**:

    a. Klicken Sie auf **Hinzufügen**.

    b. Dadurch wird das Fenster **SIEM-Server** geöffnet. Geben Sie in diesem Fenster die SIEM-Serveradresse (IPv4, DNS), den Port und das Verbindungsprotokoll an.

    c. Klicken Sie im Block **Verbindungsschutz** auf den Link **Einstellungen der Verbindung zu SIEM-Servern**.

    d. Dadurch wird das Fenster **Einstellungen der Verbindung zu SIEM-Servern** geöffnet. Passen Sie in diesem Fenster die Verbindungseinstellungen für den SIEM-Server an (siehe folgende Tabelle).

    e. Geben Sie im Block **Ereignisformat** das Format an, in das die Programmereignisse konvertiert werden sollen, damit sie an den SIEM-Server gesendet werden können. Die Option **Ereignisse in STRUCTURED-DATA konvertieren** ist standardmäßig ausgewählt. Es wird empfohlen, sich bei der Auswahl des Ereignisformats an der Konfiguration des verwendeten SIEM-Servers zu orientieren.

    f. Aktivieren Sie, sofern erforderlich, das Kontrollkästchen **Lokale Kopien für Ereignisse entfernen, die an einen syslog-Remote-Server gesendet wurden** im Block **Verbindungseinstellungen**. Wenn das Kontrollkästchen aktiviert ist, löscht das Programm die lokalen Kopien der Ereignisse, sobald sie erfolgreich auf dem SIEM-Server veröffentlicht wurden. Es wird empfohlen, diesen Modus auf leistungsschwachen Geräten zu verwenden. Wenn das Kontrollkästchen deaktiviert ist, sendet das Programm lediglich die Ereignisse an den SIEM-Server. Die Kopien der Berichte werden weiterhin lokal gespeichert. Das Kontrollkästchen ist standardmäßig deaktiviert.

    > Das Programm löscht niemals lokale Versionen des Sicherheitsprotokolls.

8. Verriegeln Sie das Vorhängeschloss, um die Richtlinie auf die Computer anzuwenden.

9. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So konfigurieren Sie die SIEM-Integration (in der Anwendungskonsole)

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Meldungen**.

2. Wählen Sie den Punkt **SIEM-Integration**.

   Das Fenster **SIEM-Integration** wird geöffnet.

3. Aktivieren Sie im Block **Integrationseinstellungen** das Kontrollkästchen **Übertragung von Sicherheitsereignissen an einen SIEM-Server aktivieren**.

4. Konfigurieren Sie die Verbindung zum SIEM-Server im Block **Einstellungen der Verbindung zu SIEM-Servern**:

    a. Klicken Sie auf **Hinzufügen**.

    b. Dadurch wird das Fenster **Server hinzufügen** geöffnet. Geben Sie in diesem Fenster die SIEM-Serveradresse (IPv4, DNS), den Port und das Verbindungsprotokoll an.

    c. Klicken Sie auf **Sicherheitseinstellungen für TCP-Verbindungen**.

    d. Dadurch wird das Fenster **Sicherheitseinstellungen für TCP-Verbindungen** geöffnet. Passen Sie in diesem Fenster die Verbindungseinstellungen für den SIEM-Server an (siehe folgende Tabelle).

5. Aktivieren Sie, sofern erforderlich, das Kontrollkästchen **Lokale Kopien für Ereignisse entfernen, die an einen syslog-Remote-Server gesendet wurden** im Block **Einstellungen für die Ereignisübertragung an einen SIEM-Server**. Wenn das Kontrollkästchen aktiviert ist, löscht das Programm die lokalen Kopien der Ereignisse, sobald sie erfolgreich auf dem SIEM-Server veröffentlicht wurden. Es wird empfohlen, diesen Modus auf leistungsschwachen Geräten zu verwenden. Wenn das Kontrollkästchen deaktiviert ist, sendet das Programm lediglich die Ereignisse an den SIEM-Server. Die Kopien der Berichte werden weiterhin lokal gespeichert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   Das Programm löscht niemals lokale Versionen des Sicherheitsprotokolls.

6. Geben Sie im Block **Ereignisformat** das Format an, in das die Programmereignisse konvertiert werden sollen, damit sie an den SIEM-Server gesendet werden können. Die Option **Ereignisse in STRUCTURED-DATA konvertieren** ist standardmäßig ausgewählt. Es wird empfohlen, sich bei der Auswahl des Ereignisformats an der Konfiguration des verwendeten SIEM-Servers zu orientieren.

7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Verbindungseinstellungen für den SIEM-Server

Einstellung	Beschreibung
Timeout (Sek)	Maximales Timeout für die Antwort des SIEM-Servers. Nach Ablauf des Timeouts versucht Kaspersky Embedded Systems Security, sich mit einem anderen SIEM-Server zu verbinden.
TLS-Serverzertifikat	TLS-Zertifikat zum Herstellen einer vertrauenswürdigen Verbindung mit dem SIEM-Server. Sie können ein TLS-Zertifikat über die SIEM-Verwaltungsoberfläche abrufen.
Zwei-Wege-Authentifizierung verwenden	Zwei-Wege-Authentifizierung beim Aufbau einer sicheren Verbindung zwischen Kaspersky Embedded Systems Security und SIEM. Um die Zwei-Wege-Authentifizierung zu verwenden, müssen Sie die Zwei-Wege-Authentifizierung in den SIEM-Einstellungen 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. Nachdem Sie die SIEM-Einstellungen konfiguriert haben, müssen Sie die Zwei-Wege-Authentifizierung mithilfe des entsprechenden Kontrollkästchens in den Einstellungen von Kaspersky Embedded Systems 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.

Methoden zur Benachrichtigung von Administrator und Benutzer

Sie können das Programm so konfigurieren, dass es den Administrator und die Benutzer, die auf das Gerät zugreifen, über folgende Ereignisse im Betrieb von Kaspersky Embedded Systems Security und den Status des Virenschutzes auf dem Gerät informiert.

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerks, die auf das geschützte Gerät zugreifen, sowie die Terminalbenutzer des Servers können Informationen über Ereignisse des Typs *Objekt gefunden* erhalten, die in der Aufgabe zum Echtzeitschutz für Dateien auftreten.

Benachrichtigungen an den Administrator oder an die Benutzer können auf unterschiedliche Weise aktiviert werden:

- Werkzeuge für Terminaldienst.

  Sie können diese Methode für die Benachrichtigung von Terminalserverbenutzer anwenden, wenn das geschützte Gerät ein Terminalserver ist.

- Starten einer ausführbaren Datei.

  Mit dieser Methode wird eine ausführbare Datei ausgeführt, die auf einem lokalen Laufwerk auf einem geschützten Gerät gespeichert ist, wenn ein Ereignis auftritt.

- Per E-Mail senden.

  Diese Methode dient der Zustellung von Nachrichten per E-Mail-Nachricht.

Sie können den Text einer Nachricht verfassen, um individuelle Ereignistypen zu erstellen. In den Text können Sie Felder mit Informationen zum Ereignis aufnehmen. Standardmäßig wird für die Benachrichtigung von Benutzern ein Standard-Nachrichtentext verwendet.

Benachrichtigungen an Administrator und Benutzer anpassen

Sollen Benachrichtigungen über Ereignisse eingestellt werden, müssen zunächst die Art der Benachrichtigung und der Inhalt der Textnachricht festgelegt sein.

So konfigurieren Sie Ereignisbenachrichtigungen (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Protokolle und Meldungen** aus.
4. Klicken Sie im Abschnitt **Aufgabenprotokolle** auf **Einstellungen**.

   Das Fenster **Benachrichtigungen** wird geöffnet.
5. Wählen Sie das Ereignis aus, für das Sie eine Benachrichtigungsmethode festlegen möchten, und klicken Sie auf **Benachrichtigungseinstellungen**.

   Das Fenster **Benachrichtigungseinstellungen** wird geöffnet.
6. Für eine E-Mail-Benachrichtigung können Sie auf der Registerkarte **E-Mail** den Text der Ereignisbenachrichtigung hinzufügen.

   Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Variable** und wählen Sie die entsprechenden Punkte in der Dropdown-Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**.

7. Für eine Benachrichtigung, bei denen eine ausführbare Datei gestartet wird: Wählen Sie auf der Registerkarte **Ausführbare Datei** die Datei auf dem lokalen Laufwerk des geschützten Geräts aus oder geben Sie den vollständigen Dateipfad ein. Diese Datei wird auf dem geschützten Gerät ausgeführt, wenn das Ereignis auftritt. Tragen Sie Name und Kennwort des Benutzers ein, unter dessen Benutzerkonto die Datei ausgeführt werden soll.

   Wenn Sie den Pfad einer ausführbaren Datei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable können hingegen nicht verwendet werden.

8. Für eine Benachrichtigung über den Terminaldienst können Sie auf der Registerkarte **Terminaldienst** den Text der Ereignisbenachrichtigung hinzufügen.

   Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Variable** und wählen Sie die entsprechenden Punkte in der Dropdown-Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**.

9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Ereignisbenachrichtigungen (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Protokolle und Meldungen** → **Aufgabenprotokolle** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Dadurch wird ein Fenster geöffnet. Klicken Sie in diesem Fenster auf das Ereignis, für das Sie eine Benachrichtigungsmethode auswählen möchten.

   Das Fenster **Benachrichtigungseinstellungen** wird geöffnet.

6. Für eine E-Mail-Benachrichtigung: Aktivieren Sie im Abschnitt **Benutzer benachrichtigen** das Kontrollkästchen **Per E-Mail** und fügen Sie den Text der Ereignisbenachrichtigung hinzu.

   Um weitere Felder mit Ereignisinformationen hinzuzufügen, klicken Sie auf **Variable hinzufügen** und wählen Sie die entsprechenden Elemente in der Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Zurücksetzen**.

7. Für eine Benachrichtigung, bei der eine ausführbare Datei gestartet wird: Aktivieren Sie im Abschnitt **Administratoren benachrichtigen** das Kontrollkästchen **Ausführbare Datei starten** und geben Sie den vollständigen Pfad einer Datei auf der lokalen Festplatte des geschützten Geräts ein. Diese Datei wird auf dem geschützten Gerät ausgeführt, wenn das Ereignis auftritt. Tragen Sie Name und Kennwort des Benutzers ein, unter dessen Benutzerkonto die Datei ausgeführt werden soll.

   Wenn Sie den Pfad einer ausführbaren Datei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable können hingegen nicht verwendet werden.

8. Für eine Benachrichtigung über den Terminaldienst: Aktivieren Sie im Abschnitt **Administratoren benachrichtigen** das Kontrollkästchen **Mit dem Terminaldienst** und fügen Sie den Text der Ereignisbenachrichtigung hinzu.

Um weitere Felder mit Ereignisinformationen hinzuzufügen, klicken Sie auf **Variable hinzufügen** und wählen Sie die entsprechenden Elemente in der Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Zurücksetzen**.

9. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie Ereignisbenachrichtigungen (in der Anwendungskonsole)

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Meldungen**.
2. Wählen Sie den Punkt **Eigenschaften**.

   Das Fenster **Meldungen** wird geöffnet.
3. Wählen Sie das Ereignis aus, für das Sie eine Benachrichtigungsmethode festlegen möchten, und klicken Sie auf **Benachrichtigungseinstellungen**.

   Das Fenster **Benachrichtigungseinstellungen** wird geöffnet.
4. Für eine E-Mail-Benachrichtigung können Sie auf der Registerkarte **E-Mail** den Text der Ereignisbenachrichtigung hinzufügen.

   Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Variable** und wählen Sie die entsprechenden Punkte in der Dropdown-Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**.
5. Für eine Benachrichtigung, bei denen eine ausführbare Datei gestartet wird: Wählen Sie auf der Registerkarte **Ausführbare Datei** die Datei auf dem lokalen Laufwerk des geschützten Geräts aus oder geben Sie den vollständigen Dateipfad ein. Diese Datei wird auf dem geschützten Gerät ausgeführt, wenn das Ereignis auftritt. Tragen Sie Name und Kennwort des Benutzers ein, unter dessen Benutzerkonto die Datei ausgeführt werden soll.

   Wenn Sie den Pfad einer ausführbaren Datei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable können hingegen nicht verwendet werden.
6. Für eine Benachrichtigung über den Terminaldienst können Sie auf der Registerkarte **Terminaldienst** den Text der Ereignisbenachrichtigung hinzufügen.

   Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Variable** und wählen Sie die entsprechenden Punkte in der Dropdown-Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**.
7. Speichern Sie die vorgenommenen Änderungen.

Felder mit Informationen über Ereignisse

Variable	Beschreibung
%EVENT_TYPE%	Ereignistyp.
%EVENT_TIME%	Zeitpunkt, zu dem ein Ereignis eingetreten ist.
%EVENT_SEVERITY%	Prioritätsstufe.
%OBJECT%	Name des Objekts (in den Aufgaben zum Echtzeit-Computerschutz und zur Untersuchung auf Befehl). In der Aufgabe Update der Programm-Module steht der Name des Updates und die Adresse der Internetseite mit näheren Angaben zum Update.

Variable	Beschreibung
%VIRUS_NAME%	Name des Objekts gemäß der Klassifizierung der Viren-Enzyklopädie. Dieser Name wird in den vollständigen Namen des erkannten Objekts aufgenommen, den Kaspersky Embedded Systems Security bei der Erkennung eines Objekts zurück gibt. Den vollständigen Namen eines gefundenen Objekts können Sie im Aufgabenprotokoll einsehen.
%VIRUS_TYPE%	Typ des gefundenen Objekts gemäß der Klassifizierung von Kaspersky, beispielsweise "Virus" oder "Trojaner". Dieser ist im vollständigen Namen des erkannten Objekts enthalten, der von Kaspersky Embedded Systems Security zurückgegeben wird, wenn ein infiziertes oder wahrscheinlich infiziertes Objekt gefunden wird. Sie können den vollständigen Namen eines gefundenen Objekts im Protokoll der Aufgabenausführung einsehen.
%USER_COMPUTER%	In der Aufgabe *Echtzeitschutz für Dateien*, der Name des geschützten Geräts jenes Benutzers, der auf dem Gerät auf das Objekt zugegriffen hat.
%USER_NAME%	In der Aufgabe *Echtzeitschutz für Dateien*, der Name des Benutzers, der auf dem Gerät auf das Objekt zugegriffen hat.
%FROM_COMPUTER%	Name des geschützten Geräts, von dem die Benachrichtigung geschickt wurde.
%EVENT_REASON%	Grund für Eintreten eines Ereignisses (Dieses Feld ist für bestimmte Ereignisse nicht verfügbar).
%ERROR_CODE%	Fehlercode (nur das Ereignis "Interner Aufgabenfehler").
%TASK_NAME%	Aufgabenname (nur für Ereignisse, die mit der Aufgabenausführung verbunden sind).
%PROTOCOL%	Das verwendete Protokoll.
%MESSAGE%	Text der Nachricht.
%DEVICE_INSTANCEPATH%	Pfad zur Instanz des Geräts.
%DEVICE_VID%	Gerätehersteller
%DEVICE_PID%	Typ des Controllers.
%DEVICE_SERIALNUMBER%	Seriennummer des Geräts.

E-Mail-Benachrichtigungen konfigurieren

So konfigurieren Sie E-Mail-Benachrichtigungen (in der Kaspersky Security Center-Verwaltungskonsole)

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 Fenster mit den Richtlinieneigenschaften den Punkt **Protokolle und Meldungen** aus.
4. Klicken Sie im Abschnitt **Aufgabenprotokolle** auf **Einstellungen**.

   Das Fenster **Benachrichtigungen** wird geöffnet.
5. Klicken Sie auf **Einstellungen für E-Mail-Benachrichtigungen**.
6. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Ereignisbenachrichtigungen senden**.
7. Geben Sie unter **Benachrichtigungsabsender** die Absenderinformationen an: Adresse des Absenders, SMTP-Server, Port des SMTP-Servers, Benutzername und Kennwort.
8. Geben Sie unter **Benachrichtigungsempfänger** die E-Mail-Adresse des Empfängers an.

9. Klicken Sie zum Testen der Einstellungen auf die Schaltfläche **Testnachricht senden**.

   Die Testnachrichtenfunktion ist nur in der Kaspersky Security Center Verwaltungskonsole und in der Programmkonsole verfügbar.

10. Geben Sie den Sendemodus an: **Bei Ereigniseintritt** oder **Nach Zeitplan (kein Zeitplan festgelegt)**. Um den Zeitplan zu konfigurieren, klicken Sie auf **Ändern**.

11. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie E-Mail-Benachrichtigungen (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Gehen Sie zu **Protokolle und Meldungen** → **Aufgabenprotokolle** und klicken Sie auf die Schaltfläche **Anpassen**.

5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Registerkarte **Einstellungen für E-Mail-Benachrichtigungen** aus.

6. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen senden**.

7. Geben Sie die Absenderinformationen an: Adresse des Absenders, SMTP-Server, Port des SMTP-Servers, Benutzername und Kennwort.

8. Geben Sie die E-Mail-Adresse des Empfängers an.

9. Geben Sie den Sendemodus an: **Beim Eintritt von Ereignissen** oder **Nach Zeitplan**. Konfigurieren Sie gegebenenfalls den Zeitplan.

10. Speichern Sie die vorgenommenen Änderungen.

So konfigurieren Sie E-Mail-Benachrichtigungen (in der Anwendungskonsole)

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Meldungen**.

2. Wählen Sie den Punkt **Eigenschaften**.

   Das Fenster **Meldungen** wird geöffnet.

3. Klicken Sie auf **E-Mail-Benachrichtigungseinstellungen**.

4. Aktivieren Sie im angezeigten Fenster das Kontrollkästchen **Ereignisbenachrichtigungen senden**.

5. Geben Sie unter **Benachrichtigungsabsender** die Absenderinformationen an: Adresse des Absenders, SMTP-Server, Port des SMTP-Servers, Benutzername und Kennwort.

6. Geben Sie unter **Benachrichtigungsempfänger** die E-Mail-Adresse des Empfängers an.

7. Klicken Sie zum Testen der Einstellungen auf die Schaltfläche **Testnachricht senden**.

   Die Testnachrichtenfunktion ist nur in der Kaspersky Security Center Verwaltungskonsole und in der Programmkonsole verfügbar.

8. Geben Sie den Sendemodus an: **Bei Ereigniseintritt** oder **Nach Zeitplan (kein Zeitplan festgelegt)**. Um den Zeitplan zu konfigurieren, klicken Sie auf **Ändern**.

9. Speichern Sie die vorgenommenen Änderungen.

Konfigurieren der Interaktion mit dem Administrationsserver

Sie müssen die Typen der Objekte auswählen, über die Kaspersky Embedded Systems Security Informationen an den Kaspersky Security Center Administrationsserver senden soll.

So konfigurieren Sie die Integration in den Administrationsserver (in der Kaspersky Security Center-Verwaltungskonsole)

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. Klicken Sie im Abschnitt **Protokolle und Meldungen** im Unterabschnitt **Interaktion mit dem Administrationsserver** auf die Schaltfläche **Einstellungen**.

4. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Objekttypen aus, über die Kaspersky Embedded Systems Security Informationen an den Kaspersky Security Center Administrationsserver senden soll:

   - **Über Backup-Dateien**
   - **Über nicht verarbeitete Dateien**
   - **Über installierte Geräte**
   - **Über eine Bedrohungsentwicklungskette**

5. Speichern Sie die vorgenommenen Änderungen.

   Kaspersky Embedded Systems Security wird Informationen über die ausgewählten Objekttypen an den Administrationsserver übertragen.

So konfigurieren Sie Interaktion mit dem Administrationsserver (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Klicken Sie im Abschnitt **Protokolle und Meldungen** im Unterabschnitt **Interaktion mit dem Administrationsserver** auf die Schaltfläche **Anpassen**.

5. Dadurch wird ein Fenster geöffnet. Wählen Sie in diesem Fenster die Objekttypen aus, über die Kaspersky Embedded Systems Security Informationen an den Kaspersky Security Center Administrationsserver senden soll:

   - **Backup-Dateien**
   - **Über nicht verarbeitete Dateien**
   - **Blockierte Netzwerkverbindungen**
   - **Installierte Geräte**

6. Speichern Sie die vorgenommenen Änderungen.

Verwaltung der vollständigen BitLocker-Laufwerkverschlüsselung

BitLocker ist eine integrierte Verschlüsselungstechnologie des Windows-Betriebssystems. In Kaspersky Embedded Systems Security können Sie BitLocker mithilfe von Kaspersky Security Center überwachen und verwalten. BitLocker verschlüsselt ein logisches Volume. Details über BitLocker finden Sie in der Microsoft-Dokumentation.

Die Verwaltung von BitLocker auf Computern mit Windows Vista und Windows Server 2008 wird von Kaspersky Embedded Systems Security nicht unterstützt.

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 BitLocker-Verschlüsselung von Wechseldatenträgern wird von Kaspersky Embedded Systems Security nicht unterstützt.

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.

Vor der Laufwerkverschlüsselung erstellt BitLocker einen Wiederherstellungsschlüssel. Kaspersky Embedded Systems Security liest den Wiederherstellungsschlüssel und sendet ihn an Kaspersky Security Center, damit Sie den Zugriff auf das Laufwerk wiederherstellen können, beispielsweise wenn ein Benutzer sein Kennwort vergessen hat.

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.

Wenn ein Benutzer ein Laufwerk mithilfe von BitLocker verschlüsselt, sendet Kaspersky Embedded Systems Security Informationen über die Laufwerkverschlüsselung und den Wiederherstellungsschlüssel 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 Embedded Systems 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 aus (in der Kaspersky Security Center Verwaltungskonsole)

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 den Abschnitt **Datenverschlüsselung** aus.
4. 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.

5. Passen Sie die erweiterten Einstellungen der „BitLocker-Laufwerkverschlüsselung" an (s. folgende Tabelle).
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So führen Sie die BitLocker-Laufwerkverschlüsselung aus (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

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

4. Wechseln Sie zum Abschnitt **Datenverschlüsselung**.

5. Klicken Sie im Unterabschnitt **Vollständige Festplattenverschlüsselung** auf die Schaltfläche **Anpassen**.

6. 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.

7. Passen Sie die erweiterten Einstellungen der „BitLocker-Laufwerkverschlüsselung“ an (s. folgende Tabelle).

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Sie können die Festplattenverschlüsselung und -entschlüsselung auf einem Benutzercomputer über die Programmkonsole steuern.

Nachdem eine Richtlinie angewendet wurde, zeigt das Programm im Fenster „Kompakte Diagnose-Benutzeroberfläche“ oder in der Programmkonsole die folgenden Anfragen an (die Auswahl der Anfragen ist von den Authentifizierungseinstellungen abhängig):

- 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 ein Kennwort oder ein PIN-Code festgelegt wurde, fordert BitLocker zum Neustart des Benutzercomputers auf, um die Kompatibilität des Computers mit BitLocker zu überprüfen. Kaspersky Embedded Systems Security zeigt im Fenster „Kompakte Diagnose-Benutzeroberfläche“ oder in der Programmkonsole eine entsprechende Benachrichtigung an. Anschließend muss der Benutzer den BitLocker-Authentifizierungsvorgang durchlaufen. Nach erfolgreichem BitLocker-Authentifizierungsvorgang ist die Anmeldung am System erforderlich. Nachdem das Betriebssystem geladen wurde, startet BitLocker die Laufwerkverschlüsselung.

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.
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 (Windows 8 und höher)** 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. Wenn neue Daten hinzugefügt werden, werden sie von Kaspersky Embedded Systems 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	**Trusted Platform Module (TPM)** Bei Auswahl dieser Variante verwendet BitLocker das Trusted Platform Module (TPM). Trusted Platform Module (TPM) 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. **Nur Kennwort (Windows 8 und höher)** Bei Auswahl dieser Variante fragt Kaspersky Embedded Systems 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. Die ausgewählte Authentifizierungsmethode muss durch Angabe von Kennwort- oder PIN-Anforderungen konfiguriert werden: • **Mindestlänge der PIN (Zeichen)**. • **Erweiterte PIN verwenden (Buchstaben und Ziffern)**. In einer erweiterten PIN sind nicht nur numerische Zeichen zulässig, sondern auch lateinische Groß- und Kleinbuchstaben, Sonderzeichen und Leerzeichen. • **Mindestlänge des Kennworts (Zeichen)**. • **Kennwort/PIN-Gültigkeitsdauer für TPM beschränken (Tage)**.
Wiederherstellungsschlüssel automatisch neu erstellen (Tage)	Kennwort automatisch aktualisieren, um den Zugriff auf ein BitLocker-geschütztes Laufwerk wiederherzustellen. Wenn das Kontrollkästchen aktiviert ist, geben Sie die Gültigkeitsdauer des Kennworts für den Wiederherstellungsschlüssel an.

Entschlüsselung einer Festplatte, die mit BitLocker geschützt ist

Der Benutzer kann das Laufwerk selbstständig mithilfe von Betriebssystem-Tools entschlüsseln (Funktion *BitLocker deaktivieren*). Danach fordert Kaspersky Embedded Systems Security auf, die Festplatte erneut zu verschlüsseln. Kaspersky Embedded Systems Security schlägt so lange vor, das Laufwerk zu verschlüsseln, bis Sie die Entschlüsselung von Laufwerken in der Richtlinie aktivieren.

So entschlüsseln Sie eine mit BitLocker geschützte Festplatte (in der Kaspersky Security Center Verwaltungskonsole)

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 den Abschnitt **Datenverschlüsselung** aus.
4. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Alle Festplatten entschlüsseln**.
5. Klicken Sie auf **OK**, um die Änderungen zu speichern.

So entschlüsseln Sie eine mit BitLocker geschützte Festplatte (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wechseln Sie zum Abschnitt **Datenverschlüsselung**.
5. Klicken Sie im Unterabschnitt **Vollständige Festplattenverschlüsselung** auf die Schaltfläche **Anpassen**.
6. Wählen Sie in der Dropdown-Liste **Verschlüsselungsmodus** die Option **Alle Festplatten entschlüsseln**.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Sie können die Festplattenverschlüsselung und -entschlüsselung über die Programmkonsole steuern.

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.

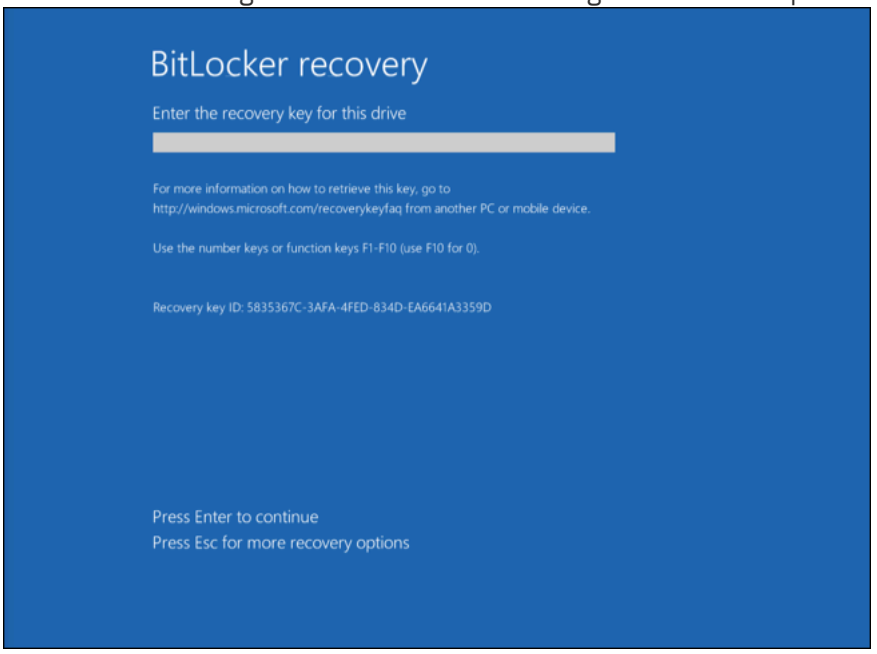
Um den Zugriff auf eine Festplatte wiederherzustellen, die mit BitLocker verschlüsselt ist, sind die folgenden Schritte erforderlich:

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.

   Wenn die IDs der Wiederherstellungsschlüssel übereinstimmen, übergibt der Administrator den Wiederherstellungsschlüssel an den Benutzer.

3. 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.

So zeigen Sie den Wiederherstellungsschlüssel für ein Systemlaufwerk an, das mit BitLocker verschlüsselt wurde (in der Kaspersky Security Center Verwaltungskonsole)

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

2. Gehen Sie auf die Registerkarte **Geräte**.

3. Öffnen Sie das Kontextmenü des Benutzercomputers, für den Wiederherstellung des Zugriffs auf verschlüsselte Daten angefordert wurde.

4. Wählen Sie im Kontextmenü den Punkt **Freigabe im Offline-Modus**.

5. Fragen Sie den Benutzer nach der Wiederherstellungsschlüssel-ID an, die im Eingabefenster für das BitLocker-Kennwort angegeben ist, und vergleichen Sie diese ID mit der ID im Feld **ID des Wiederherstellungsschlüssels** auf der Registerkarte **Zugriff auf ein Systemlaufwerk mit BitLocker-Schutz**.

   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. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.

So zeigen Sie den Wiederherstellungsschlüssel für ein Systemlaufwerk an, das mit BitLocker verschlüsselt wurde (in der Kaspersky Security Center Web Console)

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. 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.

5. Klicken Sie auf **Schlüssel anfordern**.
6. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.

Nachdem das Betriebssystem geladen wurde, fordert Kaspersky Embedded Systems 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 ein neues Wiederherstellungskennwort und das Programm sendet dieses Kennwort an Kaspersky Security Center.

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.

So zeigen Sie den Wiederherstellungsschlüssel für ein Nicht-Systemlaufwerk an, das mit BitLocker verschlüsselt wurde (in der Kaspersky Security Center Verwaltungskonsole)

1. Wählen Sie in der Struktur der Kaspersky Security Center Verwaltungskonsole den Ordner **Erweitert → Verschlüsselung und Datenschutz → Verschlüsselte Laufwerke** aus.

2. 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 Embedded Systems Security**.

3. 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.

4. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, an den Benutzer.

So zeigen Sie den Wiederherstellungsschlüssel für ein Nicht-Systemlaufwerk an, das mit BitLocker verschlüsselt wurde (in der Kaspersky Security Center Web Console)

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 für Kaspersky Embedded Systems Security 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**.

5. Übermitteln Sie den Schlüssel, der im Feld **Wiederherstellungsschlüssel** angegeben ist, 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 an (in der Kaspersky Security Center Verwaltungskonsole)

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 Embedded Systems Security für Windows (4.1)** → **Verwaltung des BitLocker-Schutzes**.

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** die Option **Kaspersky Embedded Systems Security** 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 Embedded Systems Security generiert nach jedem Neustart des Computers ohne BitLocker-Authentifizierung ein entsprechendes Ereignis und merkt sich die Anzahl der verbleibenden Neustarts.

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 Embedded Systems Security gezählt. Um die BitLocker-Authentifizierung nach jedem Neustart automatisch zu aktivieren, muss deshalb Kaspersky Embedded Systems 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**.

Integration mit Drittherstellersystemen

Dieser Abschnitt beschreibt die Integration von Kaspersky Embedded Systems Security mit Funktionen und Technologien von Drittherstellern.

Leistungsindikatoren für das Programm Systemmonitor

„Leistungsindikatoren“ ist eine Komponente von Kaspersky Embedded Systems Security. Mit ihr können Sie die Programmleistung überwachen, während Schutzkomponenten ausgeführt werden. Leistungsindikatoren werden während der Installation durch Kaspersky Embedded Systems Security registriert.

Die Programm-Leistungsindikatoren können mithilfe des Programms „Systemmonitor“ überprüft werden, das in der Windows-Systemsteuerung verfügbar ist. Ausführliche Informationen zur Verwendung von Leistungsindikatoren finden Sie auf der Website des technischen Supports von Microsoft.

Mithilfe von Leistungsindikatoren können Sie beispielsweise Ressourcenengpässe erkennen (wenn Kaspersky Embedded Systems Security zusammen mit anderen Programmen ausgeführt wird), Abstürze analysieren und ungeeignete Einstellungen von Kaspersky Embedded Systems Security identifizieren.

Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden

Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden

Beschreibung	Gesamtzahl der Anfragen des File-Interception-Treibers, die aufgrund ungenügender Systemressourcen (beispielsweise des Arbeitsspeichers) nicht verarbeitet wurden. Es wird ab dem letzten Start von Kaspersky Embedded Systems Security gezählt. Kaspersky Embedded Systems Security überspringt Anfragen zur Verarbeitung von Objekten, die nicht vom File-Interceptor-Treiber verarbeitet werden.
Ziel	Der Indikator kann mögliche Qualitätsverluste des Echtzeit-Computerschutzes erkennen und beseitigen, die aufgrund eines Mangels an Systemressourcen eintreten.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert ungleich null ist, benötigt der Prozess von Kaspersky Embedded Systems Security mehr Arbeitsspeicher, um die Anfragen zu bearbeiten. Es ist möglich, dass es andere aktive Prozesse gibt, die den ganzen Arbeitsspeicher in Anspruch nehmen.

Anzahl der zur Bearbeitung eingereichten Anfragen

Anzahl der zur Bearbeitung eingereichten Anfragen

Beschreibung	Anzahl der Objekte, die auf Verarbeitung durch aktive Prozesse warten.
Ziel	Dieser Indikator kann verwendet werden, um die Belastung der Arbeitsprozesse von Kaspersky Embedded Systems Security und Gesamtstufe der Dateiaktivität auf dem geschützten Gerät zu überwachen.
Normalwert / Grenzwert	Der Indikator kann je nach Stufe der Dateiaktivität auf dem geschützten Gerät schwanken.

Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	N/V

Anzahl der pro Sekunde verarbeiteten Objekte

Anzahl der pro Sekunde verarbeiteten Objekte

Beschreibung	Anzahl der verarbeiteten Objekte geteilt durch die Zeit, in der diese Objekte verarbeitet wurden. Wird in gleichmäßigen Zeitabständen berechnet.
Ziel	Dieser Indikator informiert über die Geschwindigkeit der Objektverarbeitung. Damit lassen sich Leistungsprobleme auf dem geschützten Gerät erkennen und beseitigen. Mögliche Gründe für Leistungsengpässe: mangelnde Zuweisung von Prozessorzeit an die Prozesse von Kaspersky Embedded Systems Security oder Fehler bei der Ausführung von Kaspersky Embedded Systems Security.
Normalwert / Grenzwert	Variiert / Nein.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Die Indikatorwerte hängen von den aktivierten Werten der Einstellungen für Kaspersky Embedded Systems Security und von der Belastung des geschützten Geräts durch Prozesse anderer Programme ab. Beobachten Sie längere Zeit das mittlere Anzeige-Niveau des Indikators. Wenn der durchschnittliche Zählerwert sinkt, ist eine der folgenden Situationen möglich: • Der Prozess von Kaspersky Embedded Systems Security verfügt über zu wenig Prozessorzeit für die Objektverarbeitung. Räumen Sie Kaspersky Embedded Systems Security zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Belastung am geschützten Gerät durch andere Anwendungen senken). • Kaspersky Embedded Systems Security ist abgestürzt (mehrere Datenströme stehen still). Kaspersky Embedded Systems Security neu starten

Anzahl der Elemente in der Warteschlange für infizierte Objekte

Anzahl der Elemente in der Warteschlange für infizierte Objekte

Beschreibung	Anzahl der infizierten Objekte, die momentan auf die Verarbeitung (Desinfektion oder Löschen) warten.
Ziel	Ein Indikator kann überwachen: • Unterbrechung des Echtzeit-Computerschutzes aufgrund von möglichen Fehlern in den File-Interception-Dispatchern. • Überlastung der Prozesse wegen ungleichmäßiger Verteilung der Prozessorzeit zwischen den anderen laufenden Programmen und Kaspersky Embedded Systems Security. • Virenepidemien.
Normalwert / Grenzwert	Der Indikatorwert kann von Null abweichen, wenn Kaspersky Embedded Systems Security gefundene infizierte oder möglicherweise infizierte Objekte verarbeitet, aber nicht sofort nach Bearbeitungsschluss zur Null zurückkehrt. / Der Indikatorwert bleibt längere Zeit nicht auf Null.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert längere Zeit nicht auf Null bleibt: • Kaspersky Embedded Systems Security verarbeitet keine Objekte (möglicherweise aufgrund eines Absturzes des File-Interception-Dispatchers) Kaspersky Embedded Systems Security neu starten • Möglicherweise steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Belastung am geschützten Gerät durch andere Anwendungen senken). • Es ist eine Virenepidemie eingetreten. Ein weiteres Anzeichen für den Ausbruch einer Virenepidemie ist eine hohe Anzahl von infizierten oder möglicherweise infizierten Objekten in der Komponente Echtzeitschutz für Dateien. Informationen über die Anzahl der gefundenen Objekte finden Sie in den Komponentenstatistiken oder im Komponentenprotokoll.

Gesamtzahl der abgelehnten Anfragen

Gesamtzahl der abgelehnten Anfragen

Beschreibung	**Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die nicht von den Programmprozessen angenommen wurden. Es wird ab dem letzten Start von Kaspersky Embedded Systems Security gezählt.** **Das Programm überspringt Objekte, für die Verarbeitungsanfragen von Prozessen durch Kaspersky Embedded Systems Security zurückgewiesen werden.**
Ziel	Ein Indikator kann überwachen: • Senkung des Echtzeit-Computerschutzes, weil die Prozesse von Kaspersky Embedded Systems Security überlastet sind. • Unterbrechung des Echtzeit-Computerschutzes aufgrund von Fehlern in den File-Interception-Dispatchern.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Summe der abgelehnten Verarbeitungsanfragen entspricht der Summe der übersprungenen Objekte. Folgende Situationen sind abhängig vom "Verhalten" des Indikators möglich: • Der Indikator zeigt einige Anfragen an, die über einen längeren Zeitraum abgelehnt wurden: Der Prozess von Kaspersky Embedded Systems Security war komplett ausgelastet. Das Programm konnte die Objekte nicht untersuchen. Um zu verhindern, dass Objekte übersprungen werden, weisen Sie dem Programm mehr Systemressourcen zu. • Die Summe der abgelehnten Anfragen übersteigt den kritischen Schwellenwert erheblich und steigt schnell an: Der File-Interception-Dispatcher ist ausgefallen. Kaspersky Embedded Systems Security untersucht Objekte nicht, wenn darauf zugegriffen wird. Kaspersky Embedded Systems Security neu starten

Gesamtzahl der übersprungenen Anfragen

Gesamtzahl der übersprungenen Anfragen

Beschreibung	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die von Kaspersky Embedded Systems Security angenommen wurden, über die aber kein Ereignis über den Verarbeitungsabschluss gesendet wurde. Es wird ab dem letzten Programmstart gezählt. Wenn eine Anfrage zur Verarbeitung eines Objekts, das von einem aktiven Prozess angenommen wurde, kein Ereignis über den Verarbeitungsabschluss gesendet hat, übergibt der Treiber diese Anfrage an einen anderen Prozess und der Wert des Indikators **Anzahl der übersprungenen Anfragen** wird um 1 erhöht. Wenn der Treiber alle aktiven Prozesse aufgerufen hat und die Verarbeitungsanfrage von keinem der Prozesse angenommen wurde (wegen Überlastung) oder keine Ereignisse über den Verarbeitungsabschluss gesendet wurden, überspringt Kaspersky Embedded Systems Security das Objekt und erhöht den Wert des Indikators **Gesamtzahl der übersprungenen Anfragen** um 1.
Ziel	Der Indikator kann einen Produktivitätsverlust wegen ausbleibender Datenströme von File-Interception-Dispatchern überwachen.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Ein Indikator, der ungleich null ist, bedeutet, dass ein oder mehrere Datenströme des File-Interception-Dispatchers hängen geblieben sind und stillstehen. Der Indikatorwert entspricht der Anzahl der Datenströme, die zurzeit stillstehen. Wenn das Untersuchungstempo nicht befriedigt, starten Sie Kaspersky Embedded Systems Security neu, um die angehaltenen Datenströme wiederherzustellen.

Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Ab Version 4.1 von Kaspersky Embedded Systems Security wird der Leistungsindikator „Maximale Anzahl der Streams des Dispatchers zum Abfangen von Dateien“ nicht mehr unterstützt.

Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

Ab Version 4.1 von Kaspersky Embedded Systems Security wird der Leistungsindikator „Durchschnittliche Anzahl der Streams des Dispatchers zum Abfangen von Dateien“ nicht mehr unterstützt.

SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security

Wenn Sie die Komponente SNMP-Protokoll-Unterstützung in die Auswahl der zu installierenden Antiviren-Komponenten aufgenommen haben, können Sie die Indikatoren und Traps von Kaspersky Embedded Systems Security mithilfe von Simple Network Management Protocol (SNMP) anzeigen.

Um die Indikatoren und Traps für Kaspersky Embedded Systems Security am Administrator-Arbeitsplatz anzuzeigen, starten Sie auf dem geschützten Gerät den SNMP-Dienst und am Administrator-Arbeitsplatz den SNMP-Dienst und den Dienst SNMP-Traps.

SNMP-Indikatoren in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Tabellen mit einer Beschreibung der Einstellungen für die SNMP-Indikatoren von Kaspersky Embedded Systems Security.

Leistungsindikatoren

Leistungsindikatoren

Indikatoren	Definition
currentRequestsAmount	Anzahl der zur Bearbeitung eingereichten Anfragen
currentInfectedQueueLength	Anzahl der Elemente in der Warteschlange für infizierte Objekte

Indikatoren	Definition
currentObjectProcessingRate	Anzahl der pro Sekunde verarbeiteten Objekte
currentWorkProcessesNumber	Aktuelle Anzahl von Arbeitsprozessen, die von Kaspersky Embedded Systems Security genutzt werden

Indikator für Backup

Indikator für Backup

Indikatoren	Definition
currentBackupStorageSize	Gesamtmenge der Daten im Backup-Ordner (MB)

Allgemeine Indikatoren

Allgemeine Indikatoren

Indikatoren	Definition
lastCriticalAreasScanAge	Das Zeitintervall in Sekunden seit dem Abschluss der Aufgabe *Untersuchung wichtiger Bereiche*.
licenseExpirationDate	Lizenzablaufdatum. Wenn ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt wurden, wird das Ablaufdatum der Lizenz des Reserveschlüssels angezeigt.
currentApplicationUptime	Ausführungszeit von Kaspersky Embedded Systems Security seit dem letzten Start, in Hundertstelsekunden

Update-Indikatoren

Update-Indikatoren

Indikatoren	Definition
avBasesAge	Seit dem Erstellungsdatum der zuletzt installierten Datenbanken-Updates verstrichene Zeit in Hundertstelsekunden.

Indikatoren für den Echtzeitschutz für Dateien

Indikatoren für den Echtzeitschutz für Dateien

Indikatoren	Definition
totalObjectsProcessed	Gesamtzahl der seit dem letzten Start der Komponente Echtzeitschutz für Dateien untersuchten Objekte
totalInfectedObjectsFound	Gesamtzahl der seit dem letzten Start der Komponente Echtzeitschutz für Dateien erkannten infizierten und anderen Objekte
totalSuspiciousObjectsFound	Gesamtzahl der seit dem letzten Start der Komponente Echtzeitschutz für Dateien erkannten möglicherweise infizierten Objekte
totalVirusesFound	Gesamtzahl der seit dem letzten Start der Komponente Echtzeitschutz für Dateien erkannten Objekte
totalObjectsQuarantined	Gesamtzahl der infizierten, möglicherweise infizierten und anderen Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
totalObjectsNotQuarantined	Gesamtzahl der infizierten oder möglicherweise infizierten Objekte, die Kaspersky Embedded Systems Security erfolglos in die Quarantäne zu verschieben versuchte; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
totalObjectsDisinfected	Gesamtzahl der von Kaspersky Embedded Systems Security desinfizierten infizierten Objekte; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien

Indikatoren	Definition
totalObjectsNotDisinfected	Gesamtzahl der infizierten und anderen Objekte, deren Desinfektion durch Kaspersky Embedded Systems Security fehlgeschlagen ist; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
totalObjectsDeleted	Gesamtzahl der infizierten, möglicherweise infizierten und anderen Objekte, die von Kaspersky Embedded Systems Security gelöscht wurden; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
totalObjectsNotDeleted	Gesamtzahl der infizierten, möglicherweise infizierten und anderen Objekte, die Kaspersky Embedded Systems Security erfolglos zu löschen versuchte; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
totalObjectsBackedUp	Gesamtzahl der infizierten und anderen Objekte, die von Kaspersky Embedded Systems Security ins Backup verschoben wurden; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
totalObjectsNotBackedUp	Gesamtzahl der infizierten und anderen Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu verschieben versuchte; gezählt seit dem letzten Start der Komponente Echtzeitschutz für Dateien
currentFileMonitorTaskStatus	Status der Komponente Echtzeitschutz für Dateien: • `1` bedeutet, dass die Komponente aktiviert ist und Schutz bietet. • `0` bedeutet, dass die Komponente keinen Schutz bietet. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.

Leistungsindikatoren des AMSI-Scanners

Leistungsindikatoren des AMSI-Scanners

Indikatoren	Definition
currentScriptCheckerTaskStatus	Status der Komponente AMSI-Scanner: • `1` bedeutet, dass die Komponente aktiviert ist und Schutz bietet. • `0` bedeutet, dass die Komponente keinen Schutz bietet. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
totalScriptsProcessed	Anzahl der seit dem letzten Start der Komponente AMSI-Scanner verarbeiteten Skripte.
totalInfectedIDangerousScriptsFound	Anzahl der seit dem letzten Start der Komponente AMSI-Scanner erkannten gefährlichen Skripte.
totalSuspiciousScriptsFound	Gesamtzahl der seit dem letzten Start der Komponente AMSI-Scanner erkannten verdächtigen Skripte.
totalScriptsBlocked	Gesamtzahl der seit dem letzten Start der Komponente AMSI-Scanner blockierten Skripte. Der Wert des Leistungsindikators ändert sich, wenn die Komponente in **Blockieren** aktiviert ist, und entspricht dem Wert des Leistungsindikators totalInfectedIDangerousScriptsFound.

SNMP-Traps und ihre Optionen in Kaspersky Embedded Systems Security

Die Optionen von SNMP-Traps in Kaspersky Embedded Systems Security sind wie folgt zusammengefasst:

- eventThreatDetected: Objekt gefunden.
  Der Trap verfügt über die folgenden Optionen:
  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName

- threatName
- detectType
- detectCertainty

- eventBackupStorageSizeExceeds: Maximale Größe des Backups wurde überschritten. Die Gesamtdatenmenge im Backup überschreitet den durch **Maximale Größe des Backups** angegebenen Wert. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

  Der Trap verfügt über die folgenden Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten. Der freie Speicherplatz im Backup beträgt weniger als oder ist gleich dem Wert **Grenzwert für verfügbaren Speicherplatz (MB)**. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

  Der Trap verfügt über die folgenden Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotBackuped: Objekt wurde nicht ins Backup verschoben.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason

- eventBackupInternalError: Backup-Fehler.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime

- eventSource
- eventReason

- eventAVBasesOutdated: Datenbanken sind veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum *Update* der Programm-Datenbanken zum letzten Mal ausgeführt wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von geschützten Geräten).

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated: Datenbanken sind stark veraltet. Anzahl der Tage seit der letzten Ausführung der Aufgabe *Update* (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von geschützten Geräten).

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: Programm wurde gestartet.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown: Programm wurde beendet.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Untersuchung wichtiger Bereiche wurde lange nicht ausgeführt. Anzahl der Tage seit dem letzten Abschluss der Aufgabe *Untersuchung wichtiger Bereiche*.

Der Trap verfügt über die folgenden Optionen:

- eventSeverity
- eventDateAndTime
- eventSource
- days

- eventLicenseHasExpired: Lizenz abgelaufen.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: Die Lizenz läuft bald ab. Es werden die Tage gezählt, die bis zum Ablauf der Lizenz verbleiben.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError: Fehler beim Abschluss der Aufgabe.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError: Fehler beim Ausführen der Aufgabe *Update*.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - taskName

- updaterErrorEventReason
- eventSource

Beschreibungen und mögliche Werte der Optionen von SNMP-Traps in Kaspersky Embedded Systems Security

Beschreibungen der Trap-Optionen und ihrer möglichen Werte werden nachfolgend aufgeführt:

- eventDateAndTime: Datum und Uhrzeit des Ereignisses
- eventSeverity: Prioritätsstufe

  Diese Option kann folgende Werte annehmen:

  - critical (1) – kritisch
  - warning (2) – Warnung
  - info (3) – informativ
- userName: Benutzername (beispielsweise der Name eines Benutzers, der versucht hat, auf eine infizierte Datei zuzugreifen).
- computerName: Name des geschützten Geräts (beispielsweise der Name eines geschützten Geräts, von dem aus ein Benutzer versucht hat, auf eine infizierte Datei zuzugreifen).
- eventSource: funktionale Komponente, die das Ereignis generiert hat.

  Diese Option kann folgende Werte annehmen:

  - unknown (0) – Funktionale Komponente unbekannt
  - quarantine (1) – Quarantäne
  - backup (2) – Backup
  - reporting (3) – Protokolle der Aufgabenausführung
  - updates (4) – Update
  - realTimeProtection (5) – Echtzeitschutz für Dateien
  - onDemandScanning (6) – Untersuchung auf Befehl
  - product (7) – Ereignis, das sich auf den Betrieb von Kaspersky Embedded Systems Security als Ganzes und nicht auf den Betrieb einzelner Komponenten bezieht
  - systemAudit (8) – Systemaudit-Protokoll
- eventReason: Ereignisauslöser: Grund für den Ereigniseintritt.

Diese Option kann folgende Werte annehmen:

- reasonUnknown (0) – der Grund ist unbekannt.
- reasonInvalidSettings (1) – nur für Backup- und Quarantäne-Ereignisse. Wird angezeigt, wenn der Quarantäne- oder Backup-Ordner nicht verfügbar ist (unzureichende Zugriffsberechtigungen oder ein ungültiger Ordner in den Quarantäne-Einstellungen angegeben, z. B. ein Netzwerkpfad). In diesem Fall verwendet Kaspersky Embedded Systems Security den Standardordner für Backup oder Quarantäne.

- objectName: Objektname (beispielsweise der Name der Datei, in der ein Virus gefunden wurde).
- threatName: Name des Objekts gemäß der Klassifizierung der Viren-Enzyklopädie. Dieser Name gehört zur vollständigen Bezeichnung, die Kaspersky Embedded Systems Security beim Fund eines Objekts zurückgibt. Sie können den vollständigen Namen eines gefundenen Objekts im Protokoll der Aufgabenausführung einsehen.
- detectType: Typ des gefundenen Objekts.

  Diese Option kann folgende Werte annehmen:

  - undefined (0) – Nicht definiert
  - virware – klassische Viren und Netzwerkwürmer
  - trojware – Trojanische Programme
  - malware – sonstige schädliche Programme
  - adware – Werbesoftware
  - pornware – pornografische Software
  - riskware – legale Programme, die von Angreifern genutzt werden können, um das Gerät oder persönliche Daten des Benutzers zu schädigen

- detectCertainty: Gewissheitsgrad bei der Erkennung einer Bedrohung.

  Diese Option kann folgende Werte annehmen:

  - Suspicion (möglicherweise infiziert) – Kaspersky Embedded Systems Security hat erkannt, dass ein Codeabschnitt des Objekts teilweise mit einem bekannten Schadcode übereinstimmt.
  - Sure (infiziert) – Kaspersky Embedded Systems Security hat erkannt, dass ein Codeabschnitt des Objekts vollständig mit einem bekannten Schadcode übereinstimmt.

- days: Anzahl der Tage (z. B. Anzahl der Tage bis zum Ablauf einer Lizenz).
- errorCode: ein Fehlercode.
- taskName: Aufgabenname.
- updaterErrorEventReason: der Grund für den Update-Fehler.

  Diese Option kann folgende Werte annehmen:

  - reasonUnknown(0) – der Grund ist unbekannt.
  - reasonAccessDenied – Zugriff verweigert.

- reasonUrlsExhausted – das Ende der Liste mit Update-Quellen wurde erreicht.
- reasonInvalidConfig – ungültige Konfigurationsdatei.
- reasonInvalidSignature – ungültige Signatur.
- reasonCantCreateFolder – der Ordner kann nicht angelegt werden.
- reasonFileOperError – Dateifehler.
- reasonDataCorrupted – Objekt beschädigt.
- reasonConnectionReset – Verbindung zurückgesetzt.
- reasonTimeOut – Zeitüberschreitung bei der Verbindung.
- reasonProxyAuthError – Fehler bei der Authentifizierung auf dem Proxyserver.
- reasonServerAuthError – Fehler bei der Authentifizierung auf dem Server.
- reasonHostNotFound – Gerät nicht gefunden.
- reasonServerBusy – Server nicht verfügbar.
- reasonConnectionError – Verbindungsfehler.
- reasonModuleNotFound – Objekt nicht gefunden.
- reasonBlstCheckFailed (16) – Fehler bei der Untersuchung der Deny-Liste für Schlüssel. Möglicherweise wurden während des Updatevorgangs Datenbanken-Updates veröffentlicht. Wiederholen Sie bitte das Update in einigen Minuten.

- storageObjectNotAthreatddedEventReason: der Grund, warum das Objekt nicht im Backup oder in der Quarantäne abgelegt wurde.

  Diese Option kann folgende Werte annehmen:

  - reasonUnknown (0) – der Grund ist unbekannt.
  - reasonStorageInternalError – Datenbankfehler; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
  - reasonStorageReadOnly – Datenbank ist schreibgeschützt; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
  - reasonStorageIOError – Eingabe-Ausgabe-Fehler: a) Kaspersky Embedded Systems Security ist beschädigt und muss wiederhergestellt werden; b) der Datenträger, auf dem die Dateien von Kaspersky Embedded Systems Security gespeichert sind, ist beschädigt.
  - reasonStorageCorrupted – Speicher ist beschädigt; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
  - reasonStorageFull – Datenbank ist voll; freier Speicherplatz ist erforderlich.
  - reasonStorageOpenError – Datenbankdatei konnte nicht geöffnet werden; Kaspersky Embedded Systems Security muss wiederhergestellt werden.

- reasonStorageOSFeatureError – einige Funktionen des Betriebssystems entsprechen nicht den Anforderungen von Kaspersky Embedded Systems Security.
- reasonObjectNotFound – das in die Quarantäne zu verschiebende Objekt ist auf dem Datenträger nicht vorhanden.
- reasonObjectAccessError – unzureichende Rechte für die Verwendung der Backup-API: Das Benutzerkonto, mit dessen Rechten der Vorgang ausgeführt wird, hat nicht die Berechtigung „Backup Operator“.
- reasonDiskOutOfSpace – zu wenig Speicherplatz auf dem Datenträger.

WMI-Integration

Kaspersky Embedded Systems Security unterstützt die Integration mit Windows Management Instrumentation (WMI): Sie können Client-Systeme verwenden, die WMI zum Empfangen von Daten über den Web-Based Enterprise Management-Standard (WBEM) nutzen, um Informationen über den Status von Kaspersky Embedded Systems Security und seiner Komponenten zu erhalten.

Wenn Kaspersky Embedded Systems Security installiert ist, werden eigene Module im System registriert, um einen Namensraum von Kaspersky Embedded Systems Security auf dem geschützten Gerät zu erstellen. Ein Namensraum von Kaspersky Embedded Systems Security ermöglicht die Nutzung von Klassen und Exemplarklassen für Kaspersky Embedded Systems Security sowie deren Eigenschaften.

Die Werte einiger Eigenschaften von Exemplarklassen hängen von Aufgabentypen ab.

Eine *nicht-periodische Aufgabe* ist eine Programmaufgabe, die zeitlich nicht beschränkt ist und entweder dauerhaft ausgeführt oder beendet werden kann. Bei diesen Aufgaben wird kein Ausführungsfortschritt angezeigt. Die Ergebnisse der Aufgabe werden während der Ausführung der Aufgabe fortlaufend als einzelne Ereignisse protokolliert (beispielsweise Fund eines infizierten Objekts durch Aufgaben zum Echtzeit-Computerschutz). Dieser Aufgabentyp wird über Richtlinien von Kaspersky Security Center verwaltet.

Eine *periodische Aufgabe* ist eine Programmaufgabe, die zeitlich beschränkt ist und deren Ausführungsfortschritt als Prozentsatz angezeigt wird. Die Aufgabenergebnisse werden generiert, wenn die Aufgabe abgeschlossen ist, und werden als einzelnes Element oder als geänderter Anwendungsstatus dargestellt (z. B. abgeschlossene Aktualisierung der Anwendungsdatenbank, generierte Konfigurationsdateien für Regelgenerierungsaufgaben). Mehrere periodische Aufgaben desselben Typs können auf einem einzelnen geschützten Gerät gleichzeitig ausgeführt werden (drei Aufgaben zur Untersuchung auf Befehl mit unterschiedlichen Untersuchungsbereichen). Periodische Aufgaben können über Kaspersky Security Center als Gruppenaufgaben verwaltet werden.

Wenn Sie Werkzeuge für die Erstellung von WMI-Namensraumabfragen verwenden und dynamische Daten aus WMI-Namensräume in Ihrem Unternehmensnetzwerk empfangen, haben Sie die Möglichkeit, Informationen über den aktuellen Zustand des Programms zu empfangen (siehe Tabelle unten).

Informationen über den Zustand des Programms

Eigenschaft der Exemplarklasse	Beschreibung	Werte
`ProductName`	Name des installierten Programms.	Vollständiger Name des Programms ohne Versionsnummer.
`ProductVersion`	Vollständige Versionsnummer des installierten Programms.	Vollständige Versionsnummer des Programms einschließlich Nummer des Builds
`InstalledPatches`	Übersicht der Anzeigenamen der installierten Patches.	Liste von kritischen Fehlerbehebungen, die für das Programm installiert wurden.

Eigenschaft der Exemplarklasse	Beschreibung	Werte
`IsLicenseInstalled`	Status der Aktivierung des Programms.	Status des Schlüssels, der zur Aktivierung des Programms verwendet wurde. Mögliche Werte: • `False` Es wurde kein Lizenzschlüssel hinzugefügt. • `True` Es wurde ein Lizenzschlüssel hinzugefügt.
`LicenseDaysLeft`	Zeigt an, wie viele Tage bis zum Ablauf einer aktuellen Lizenz übrig sind.	Anzahl der Tage, die bis zum Ablauf der aktuellen Lizenz verbleiben. Mögliche nicht-positive Werte: • `0` Die Lizenz ist abgelaufen. • `-1` Es können keine Informationen über den aktuellen Schlüssel abgerufen werden oder der angegebene Schlüssel kann nicht zur Aktivierung des Programms verwendet werden (beispielsweise, wenn er aufgrund einer Deny-Liste für Schlüssel gesperrt ist).
`AVBasesDatetime`	Zeitstempel für die aktuelle Version der Antiviren-Datenbanken.	Datum und Uhrzeit der Erstellung der derzeit verwendeten Antiviren-Datenbanken. Wenn das installierte Programm keine Antiviren-Datenbanken verwendet, weist das Feld den Wert `{Not installed}` auf.
`IsExploitPreventionEnabled`	Status der Komponente Exploit-Prävention.	Status der Komponente Exploit-Prävention. Mögliche Werte: • `True` Die Komponente Exploit-Prävention ist aktiviert und bietet Schutz. • `False` Die Komponente Exploit-Prävention bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
`ProtectionTasksRunning`	Zusammenstellung von Schutzaufgaben, die derzeit ausgeführt werden.	Liste der Aufgaben zum Schutz, zur Kontrolle und Überwachung, die derzeit ausgeführt werden. In diesem Feld sollten alle ausgeführten nicht periodischen Aufgaben angeführt sein. Wenn keine nicht-periodische Aufgabe ausgeführt wird, weist das Feld den Wert `{No}` auf.
`IsAppControlRunning`	Status der Komponente Kontrolle des Programmstarts.	Mögliche Werte • `True` Die Komponente Kontrolle des Programmstarts ist aktiviert und bietet Schutz. • `False` Die Komponente Kontrolle des Programmstarts bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
`AppControlMode`	Funktionsmodus der Komponente Kontrolle des Programmstarts.	Mögliche Werte: • `Active` Der Modus **Blockieren** ist in den Komponenteneinstellungen festgelegt. • `Statistics Only` Der Modus **Informieren** ist in den Komponenteneinstellungen festgelegt. • `Not installed` Die Komponente Kontrolle des Programmstarts ist nicht installiert. • `Unknown` Die Komponente ist deaktiviert.
`AppControlRulesNumber`	Gesamtanzahl der Regeln für die Kontrolle des Programmstarts.	Die Anzahl der Regeln, die derzeit in den Einstellungen der Komponente Kontrolle des Programmstarts festgelegt sind.
`AppControlLastBlocking`	Zeitstempel für den letzten von der Komponente Kontrolle des Programmstarts in einem beliebigen Modus blockierten Programmstart.	Datum und Uhrzeit des letzten von der Komponente Kontrolle des Programmstarts blockierten Programmstarts. Dieses Feld beinhaltet alle blockierten Programme unabhängig vom Funktionsmodus der Komponente. Wenn zum Zeitpunkt der Verarbeitung der WMI-Abfrage keine blockierten Programmstarts registriert sind, wird dem Feld der Wert `{No}` zugewiesen.
`PeriodicTasksRunning`	Zusammenstellung von periodischen Aufgaben, die derzeit ausgeführt werden.	Liste von Aufgaben zur Untersuchung auf Befehl, zum Update und zur Inventarisierung, die derzeit ausgeführt werden. Dieses Feld sollte alle ausgeführten periodischen Aufgaben beinhalten. Wenn derzeit keine periodischen Aufgaben ausgeführt werden, weist das Feld den Wert `{No}` auf.

Eigenschaft der Exemplarklasse	Beschreibung	Werte
`ConnectionState`	Status der Verbindung zwischen der WMI-Anbieterkomponente und dem Kaspersky Embedded Systems Security Service.	Informationen über den Status der Verbindung zwischen der WMI-Anbieterkomponente und dem Kaspersky Embedded Systems Security Service. Mögliche Werte: • `Success` Die Verbindung wurde erfolgreich hergestellt: Der WMI-Client kann Informationen über den Programmstatus empfangen. • `Failed. Error Code: <code>` Die Verbindung konnte aufgrund eines Fehlers mit dem angegebenen Code nicht hergestellt werden.
`IsDumpingEnabled`	Status der Speicher-Dump-Aufzeichnung.	Mögliche Werte • `True` Die Speicher-Dump-Aufzeichnung ist aktiviert. • `False` Die Speicher-Dump-Aufzeichnung ist deaktiviert.
`DumpsFolder`	Ordner zum Speichern von Dump-Dateien.	Vollständiger Ordnerpfad. Wenn die Dump-Aufzeichnung deaktiviert ist, ist dieses Feld leer.
`IsTracingEnabled`	Status der Programmablaufverfolgung.	Mögliche Werte • `True` Die Programmablaufverfolgung ist aktiviert. • `False` Die Programmablaufverfolgung ist deaktiviert.
`TraceFolder`	Ordner zum Speichern von Protokolldateien.	Vollständiger Ordnerpfad. Wenn die Programmablaufverfolgung deaktiviert ist, ist dieses Feld leer.
`AllTasksState`	Status aller Aufgaben.	Informationen über den Status von Aufgaben im Format `{<profile-name_1>, <profile-type_1>, <profile-state_1>,...<profile-name_N>, <profile-type_N>, <profile-state_N>}`, wobei `profile-name` der Name der Aufgabe, `profile-type` der Aufgabentyp und `profile-state` der aktuelle Status der Aufgabe ist. Mögliche Statuswerte: • `not started` Die Aufgabe wurde noch nicht gestartet. • `running` Die Aufgabe wird ausgeführt. • `running ma` Die Aufgabe wird ausgeführt; bei der Ausführung ist ein Fehler aufgetreten. • `paused` Die Aufgabe ist angehalten. • `stopped` Die Aufgabe ist beendet. • `completed` Die Aufgabe wurde erfolgreich abgeschlossen. • `failed` Die Aufgabe wurde mit einem Fehler beendet. • `disabled` Die Aufgabe ist deaktiviert und kann nicht ausgeführt werden. • `starting` Die Aufgabe wird gerade gestartet. • `pausing` Die Aufgabe wird gerade angehalten. • `stopping` Die Aufgabe wird gerade beendet. • `<unknown>` Der Status kann nicht ermittelt werden.
`IsDevControlRunning`	Status der Komponente Gerätekontrolle.	Mögliche Werte: • `True` Die Komponente Gerätekontrolle ist aktiviert und bietet Schutz. • `False` Die Komponente Gerätekontrolle bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
`IsKSNRunning`	Status der Komponente Kaspersky Security Network.	Mögliche Werte: • `True` Die Komponente Kaspersky Security Network ist aktiviert und bietet Schutz. • `False` Die Komponente Kaspersky Security Network bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
`IsOASRunning`	Status der Komponente Echtzeitschutz für Dateien.	Mögliche Werte: • `True` Die Komponente Echtzeitschutz für Dateien ist aktiviert und bietet Schutz. • `False` Die Komponente Echtzeitschutz für Dateien bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.

Diese Daten stellen die Instanzeigenschaften `KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security` dar. Dabei gilt:

- `KasperskySecurity_ProductInfo` ist der Name der Klasse von Kaspersky Embedded Systems Security.
- `.ProductName=Kaspersky Embedded Systems Security` sind Schlüsseleigenschaften von Kaspersky Embedded Systems Security.

Die Klasse wird im Namespace `ROOT\Kaspersky\Security` instanziiert.

Managed Detection and Response

Kaspersky Embedded Systems Security unterstützt die Integration in die Managed Detection and Response-Lösung.

Kaspersky Managed Detection and Response (auch MDR genannt) bietet rund um die Uhr Schutz vor der steigenden Zahl von Bedrohungen, die automatisierte Sicherheitsbarrieren umgehen. Es eignet sich für Unternehmen, die über begrenzte externe und interne Sicherheitsressourcen verfügen. Im Gegensatz zu ähnlichen Angeboten auf dem Markt weist dieser Dienst eine echte Erfolgsbilanz in der effektiven Untersuchung gezielter Angriffe auf und bietet selbst gegen die komplexesten Bedrohungen einen kontinuierlichen Schutz. Der Dienst verbessert die Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyberbedrohungen und entlastet gleichzeitig Ihre vorhandenen Ressourcen, die sich dann auf andere Aufgaben konzentrieren können.

MDR verwendet Telemetrie-Daten, die von Endpunkten bereitgestellt werden, 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“.

Konfiguration der MDR-Integration

Zur Integration von Kaspersky Managed Detection and Response sind folgende Schritte erforderlich:

1. **Installation der Komponente Managed Detection and Response**

   Für die Integration von Kaspersky Embedded Systems Security in die Lösung Managed Detection and Response wird die Komponente Managed Detection and Response verwendet. Um diese Komponente über die Einstellungen des Installationspakets oder den Setup-Assistenten oder durch Ändern der Auswahl der Programmkomponenten in der Windows-Systemsteuerung zu installieren, wählen Sie **Managed Detection and Response** aus. Sie können die Komponente auch mithilfe der Aufgabe *Komponenten für Kaspersky Embedded Systems Security ändern* installieren.

   > Um die Komponente Managed Detection and Response ohne Neustart des Computers mithilfe der Aufgabe *Komponenten für Kaspersky Embedded Systems Security ändern* zu installieren, müssen Sie in den Aufgabeneinstellungen die Option **Auf inkompatible Dritthersteller-Programme überprüfen** deaktivieren.

2. **Kaspersky Private Security Network konfigurieren**

   Ab dem Update vom Juli 2025 kann die Lösung „Managed Detection and Response“ ohne die KPSN-Konfigurationsdatei verwendet werden. Ausführliche Informationen darüber, wie die MDR-Lösung das Kaspersky Security Network verwendet, finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

   Wenn Ihre Konfiguration eine Ausführung ohne KPSN-Konfigurationsdateien nicht unterstützt, laden Sie in den Eigenschaften des Administrationsservers die KPSN-Konfigurationsdatei hoch. Die KPSN-Konfigurationsdatei befindet sich im zip-Archiv der MDR-Konfigurationsdatei. Sie können die KPSN-Konfigurationsdatei auch über die Befehlszeile hochladen.

   Ausführliche Informationen über die Konfiguration von Kaspersky Private Security Network finden Sie in der Hilfe zu Kaspersky Security Center.

3 Aktivieren von Kaspersky Managed Detection and Response

Um die Lösung Managed Detection and Response in Kaspersky Embedded Systems Security zu aktivieren, benötigen Sie eine separate Lizenz für das Add-on von Kaspersky Managed Detection and Response für Embedded Systems Security. Ausführliche Informationen darüber, wie die Lösung aktiviert wird, finden Sie in der Hilfe zu Kaspersky Managed Detection and Response.

Kaspersky Embedded Systems Security unterstützt keine MDR-Konfigurationsdateien (BLOB-Dateien). Alle Assets werden im Stammmandanten abgelegt.

4 Aktivieren der Komponente Managed Detection and Response

So aktivieren Sie die Komponente Managed Detection and Response in der Kaspersky Security Center Verwaltungskonsole

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 den Abschnitt **Telemetrie-Erfassungsserver** aus.
4. Klicken Sie im Block **Managed Detection and Response** auf **Einstellungen**.

   Das Fenster **Managed Detection and Response** wird geöffnet.
5. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response**.
6. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Komponente Managed Detection and Response 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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Telemetrie-Erfassungsserver** aus.
5. Klicken Sie im Block **Managed Detection and Response** auf **Einstellungen**.

   Das Fenster **Managed Detection and Response** wird geöffnet.
6. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response DEAKTIVIERT**.
7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie die Komponente Managed Detection and Response in der Programmkonsole

1. Wählen Sie in der Struktur der Anwendungskonsole den Abschnitt **Telemetrie-Erfassungsserver** → **Managed Detection and Response** aus.
2. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Managed Detection and Response** wird auf der Registerkarte **Allgemein** des Dateiintegritätsmonitors geöffnet.
3. Aktivieren Sie das Kontrollkästchen **Managed Detection and Response**.
4. Speichern Sie die vorgenommenen Änderungen.

Sie können die Komponente Managed Detection and Response auch über die Befehlszeile aktivieren.

5 **Andere Programmkomponenten für den Empfang von Telemetriedaten konfigurieren**

Sie müssen die folgenden Komponenten aktivieren, damit „Kaspersky Managed Detection and Response“ funktioniert:

- Kaspersky Security Network (erweiterter Modus).
- Echtzeitschutz für Dateien.
- AMSI-Scanner.
- Verhaltensanalyse.
- Exploit-Prävention.
- Schutz vor Netzwerkbedrohungen.
- Firewall.
- Untersuchung auf Befehl.

Damit „Kaspersky Managed Detection and Response“ gemeinsam mit dem Administrationsserver über „Kaspersky Security Center Web Console“ funktioniert, müssen Sie auch eine neue sichere Verbindung herstellen, und zwar eine *Hintergrundverbindung*. Kaspersky Managed Detection and Response fordert Sie auf, eine Hintergrundverbindung herzustellen, wenn Sie die Lösung bereitstellen. Stellen Sie sicher, dass die Hintergrundverbindung hergestellt wurde.

Herstellen einer Hintergrundverbindung in Kaspersky Security Center 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.

Kaspersky Embedded Systems Security über die Befehlszeile verwalten

Sie können Kaspersky Embedded Systems Security über die Befehlszeile steuern und verwalten.

Um Kaspersky Embedded Systems Security über die Befehlszeile zu verwalten, gehen Sie wie folgt vor:

1. Führen Sie auf dem Gerät einen Befehlszeileninterpreter (z. B. cmd.exe) mit den Berechtigungen des lokalen Administrators aus.

2. Navigieren Sie mit dem Befehl `cd` zu dem Ordner, in dem sich die Datei kavshell.exe befindet.

   Beispiel

   ```
   cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0
   ```

   Sie können den Pfad der ausführbaren Datei auch während der Programm-Installation zur Systemvariablen %PATH% hinzufügen und den Befehl ausführen, ohne den Programmordner besuchen.

3. Verwenden Sie die folgende Vorlage, um den Befehl auszuführen:

   ```
   KAVSHELL <command> [options]
   ```

   Eine Liste der Befehle für die Programmverwaltung erhalten Sie mithilfe des Befehls `KAVSHELL HELP`. Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, geben Sie den Befehl `KAVSHELL HELP <command>` ein.

Daraufhin führt Kaspersky Embedded Systems Security die angegebene Aktion aus.

APPCONTROL. Regeln für die Kontrolle des Programmstarts importieren

Mit dem Befehl `KAVSHELL APPCONTROL` können Regeln der Komponente Kontrolle des Programmstarts aus einer XML-Datei importiert und alle Regeln aus der Regelliste der Komponente entfernt werden. Zum Erstellen einer XML-Datei mit Regeln können Sie eine lokale Aufgabe oder eine Gruppenaufgabe vom Typ *Erstellen von Regeln für die Kontrolle des Programmstarts* verwenden.

Syntax des Befehls

```
KAVSHELL APPCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Obligatorisches Argument. Regeln für die Kontrolle des Programmstarts aus der angegebenen XML-Datei importieren: • `/APPEND` fügt alle Regeln aus der Datei zur Regelliste der Komponente hinzu. Wenn eine Regel bereits in der Liste enthalten ist, wird sie dupliziert. • `/REPLACE` ersetzt die gesamte vorhandene Regelliste der Komponente durch die Regeln aus der Datei. • `/MERGE` führt die Regeln aus der Datei mit der vorhandenen Regelliste zusammen. Wenn eine Regel bereits in der Liste enthalten ist, wird sie nicht dupliziert. Um alle Regeln der Komponente Kontrolle des Programmstarts zu entfernen, verwenden Sie `/CLEAR`.
`<path to XML file>`	Erforderlich, wenn `/APPEND`, `/REPLACE` und `/MERGE` übergeben werden. Vollständiger Pfad zur XML-Datei mit den Regeln.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL APPCONTROL /APPEND c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

APPCONTROL /CONFIG. Komponente Kontrolle des Programmstarts konfigurieren

Mit dem Befehl `KAVSHELL APPCONTROL /CONFIG` können Sie die Einstellungen der Komponente Kontrolle des Programmstarts verwalten.

Syntax des Befehls

```
KAVSHELLKAVSHELL APPCONTROL /CONFIG [/MODE:<applyrules|statistics>] [/DLL:<no|yes>] [/SAVETOFILE:<path to XML
file>] [/SDC] [/CLEARSDC] /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/MODE: <applyrules|statistics>`	Optionales Argument. Funktionsmodus der Komponente Kontrolle des Programmstarts: • `applyrules`: Kaspersky Embedded Systems Security kontrolliert den Start von Programmen anhand der Regeln zur Kontrolle des Programmstarts. • `statistics` (Standardwert): Kaspersky Embedded Systems Security erlaubt den Start aller Programme. In diesem Modus zeichnet das Programm lediglich Informationen über alle Programmstarts, die für die gestarteten Programme geltenden Regeln und die Aktionen auf, die ausgeführt worden wären, wenn die Komponente im Modus `applyrules` ausgeführt worden wäre.
`/DLL:<no|yes>`	Optionales Argument. Überwachung des Ladens von DDL-Modulen: • `no` (Standardwert): Kaspersky Embedded Systems Security kontrolliert das Laden von DLL-Modulen nicht anhand von Regeln zur Kontrolle des Programmstarts. Laden von DLL-Modulen ist erlaubt. • `yes`: Ist diese Funktionalität aktiviert, erlaubt oder verweigert Kaspersky Embedded Systems Security das Laden von DLL-Modulen anhand von Regeln zur Kontrolle des Programmstarts.

`/SAVETOFILE:<path to XML file>`	Optionales Argument. Speichern der Liste der Regeln für die Kontrolle des Programmstarts in der angegebenen XML-Datei.
`/SDC`	Optionales Argument. Exportieren Sie den Cache für die Programmverteilung in eine XML-Konfigurationsdatei, die mit der Option `/SAVETOFILE` angegeben wird.
`/CLEARSDC`	Optionales Argument. Löschen des Software-Verteilungscaches.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml /PWD:p@ssw0rd
```

APPCONTROL /GENERATE. Erstellen von Regeln für die Kontrolle des Programmstarts

Mit dem Befehl `KAVSHELL APPCONTROL /GENERATE` können Sie die Aufgabe *Erstellen von Regeln für die Kontrolle des Programmstarts* verwalten.

Syntax des Befehls

```
KAVSHELL APPCONTROL /GENERATE <path to folder> | /SOURCE:<path to file with folders list> [/MASKS:<edms>]
[/RUNAPP] [/RULES:<ch|cp|h>] [/STRONG] [/USER:<user or group of users>] [/EXPORT:<path to XML file>] [/IMPORT:
<a|r|m>] [/PREFIX:<prefix for rules names>] [/UNIQUE] [/ADDPATH] /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`<path to folder>`	Erforderlich, wenn `/SOURCE` nicht angegeben wird. Pfad zu einem Ordner mit ausführbaren Dateien, MSI-Paketen und Skripten. Die Aufgabe erstellt Erlaubnisregeln, wenn Dateien der angegebenen Typen in den angegebenen Ordnern gestartet werden.
`/SOURCE:<path to file with folders list>`	Erforderlich, wenn `<path to folder>` nicht angegeben wird. Pfad zu einer TXT-Datei mit einer Liste der Ordner, die ausführbare Dateien enthalten, für die automatisch Erlaubnisregeln generiert werden.
`/MASKS:<edms>`	Optionales Argument. Dateierweiterungen der ausführbaren Dateien, für die automatisch Erlaubnisregeln generiert werden. Sie können Dateien mit den folgenden Erweiterungen in den Aufgabenbereich aufnehmen: • `e` für EXE-Dateien • `d` für DLL-Dateien • `m` für MSI-Dateien • `s` für Skripte
`/RUNAPP`	Optionales Argument. Erlaubnisregeln auf Grundlage laufender Programme erstellen.

`/RULES:<ch|cp|h>`	Optionales Argument. Das Kriterium, das die Aufgabe beim Erstellen von Erlaubnisregeln für die Kontrolle des Programmstarts anwendet: • `ch` zum Verwenden des digitalen Zertifikats. Wenn das Zertifikat fehlt, SHA256-Hash verwenden. • `cp` zum Verwenden des digitalen Zertifikats. Wenn das Zertifikat fehlt, den Wert des Pfades der ausführbaren Datei verwenden. • `h` zum Verwenden des SHA256-Hashs.
`/STRONG`	Optionales Argument. Verwendung des Eigentümers und des Fingerabdrucks des digitalen Zertifikats der Datei als Auslösekriterium für die Erlaubnisregeln der Kontrolle des Programmstarts. Wird zusammen mit dem Parameter `/RULES:<ch|cp>` verwendet.
`/USER:<user or group of users>`	Optionales Argument. Name des Benutzers oder der Benutzergruppe, für den bzw. die die Regeln angewendet werden.
`/EXPORT:<path to XML file>`	Optionales Argument. Pfad und Name der XML-Datei, in der die angegebenen Regeln gespeichert werden sollen.
`/IMPORT:<a|r|m>`	Optionales Argument. Generierte Regeln in die Liste der Regeln für die Kontrolle des Programmstarts importieren: • `a` fügt alle Regeln aus der Datei zur Regelliste der Komponente hinzu. Wenn eine Regel bereits in der Liste enthalten ist, wird sie dupliziert. • `r` ersetzt die gesamte vorhandene Regelliste der Komponente durch die Regeln aus der Datei. • `m` führt die Regeln aus der Datei mit der vorhandenen Regelliste zusammen. Wenn eine Regel bereits in der Liste enthalten ist, wird sie nicht dupliziert.
`/PREFIX:<prefix for rules names>`	Angabe eines Präfixes für die Namen von Erlaubnisregeln der Kontrolle des Programmstarts.
`/UNIQUE`	Hinzufügen von Informationen über das geschützte Gerät zu den Regeln, auf deren Grundlage die Erlaubnisregeln für die Kontrolle des Programmstarts generiert werden.
`/ADDPATH`	Fügen Sie den auf Grundlage von Hashes generierten Regeln einen Pfad zu einer ausführbaren Datei hinzu.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml /PWD:p@ssw0rd
```

CONFIG. Unterstützung der AM-PPL-Technologie

Mit dem Befehl `KAVSHELL CONFIG` können Sie den Schutz von Programmprozessen mithilfe der AM-PPL-Technologie verwalten.

Damit der Befehl ordnungsgemäß funktioniert, müssen Sie den Selbstschutzmechanismus deaktivieren.

Syntax des Befehls

```
KAVSHELL CONFIG /PPL:<ON|OFF> /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/PPL:<ON|OFF>`	Obligatorisches Argument. Aktiviert oder deaktiviert die Unterstützung der AM-PPL-Technologie: • `ON` – Unterstützung der AM-PPL-Technologie aktivieren. • `OFF` – Unterstützung der AM-PPL-Technologie deaktivieren.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL CONFIG /PPL:ON
KAVSHELL CONFIG /PPL:OFF
```

DEVCONTROL. Regeln für die Gerätekontrolle importieren

Mit dem Befehl `KAVSHELL DEVCONTROL` können Sie Regeln der Komponente Gerätekontrolle aus einer XML-Datei importieren, die mit dem Befehl *Erstellen von Regeln für die Gerätekontrolle* erstellt wurde, oder alle Regeln aus der Regelliste der Komponente entfernen.

Syntax des Befehls

```
KAVSHELL DEVCONTROL /APPEND <path to XML file> | /REPLACE <path to XML file> | /MERGE <path to XML file> | /CLEAR
/PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/APPEND | /REPLACE | /MERGE | /CLEAR`	Obligatorisches Argument. Regeln für die Gerätekontrolle aus der angegebenen XML-Datei importieren: • `/APPEND` fügt alle Regeln aus der Datei zur Regelliste der Komponente hinzu. Wenn eine Regel bereits in der Liste enthalten ist, wird sie dupliziert. • `/REPLACE` ersetzt die gesamte vorhandene Regelliste der Komponente durch die Regeln aus der Datei. • `/MERGE` führt die Regeln aus der Datei mit der vorhandenen Regelliste zusammen. Wenn eine Regel bereits in der Liste enthalten ist, wird sie nicht dupliziert. Um alle Regeln der Komponente Gerätekontrolle zu entfernen, verwenden Sie `/CLEAR`.
`<path to XML file>`	Erforderlich, wenn `/APPEND`, `/REPLACE` und `/MERGE` übergeben werden. Vollständiger Pfad zur XML-Datei mit den Regeln.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.

Einstellung	Beschreibung
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL DEVCONTROL /MERGE c:\rules\appctrlrules.xml /PWD:p@ssw0rd
```

DUMP. Speicherabbilder aufzeichnen

Mit dem Befehl `KAVSHELL DUMP` können Sie die Erstellung von Speicherauszügen aktivieren oder deaktivieren.

Syntax des Befehls

```
KAVSHELL DUMP </ON /F:<dump_file_folder> | /SNAPSHOT /F:<dump_file_folder> /P:<process_ID> | /OFF > [/PWD:
<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/ON`	Erstellung von Dump-Dateien aktivieren.
`/F:<dump_file_folder>`	Obligatorisches Argument. Legt den Ordner fest, in dem die Dump-Dateien gespeichert werden.
`/SNAPSHOT`	Erstellt einen Speicherauszug eines laufenden Prozesses mit der angegebenen ID. Die Dump-Datei wird in dem mit der Option `/F` angegebenen Ordner gespeichert.
`/P:<process_ID>`	Erforderlich, wenn `/SNAPSHOT` angegeben wird. Legt eine Prozess-ID fest. Sie können die Prozess-ID mithilfe des Befehls `tasklist` ermitteln.
`/OFF`	Erstellung von Dump-Dateien deaktivieren.
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL DUMP /ON /F:"C:\Dumps and others"
KAVSHELL DUMP /SNAPSHOT /F:"C:\Dumps and others" /P:1234 /PWD:p@ssw0rd
KAVSHELL DUMP /OFF
```

EXITPOLICY. Deaktivieren der Richtlinie auf dem Gerät

Der Befehl `KAVSHELL EXITPOLICY` deaktiviert die Kaspersky Security Center-Richtlinie auf dem Gerät. Nach dem Deaktivieren der Richtlinie können alle Einstellungen von Kaspersky Embedded Systems Security konfiguriert werden, einschließlich der Einstellungen, die in der Richtlinie mit einem geschlossenen Vorhängeschloss (🔒) gekennzeichnet sind.

Syntax des Befehls

```
KAVSHELL EXITPOLICY [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL EXITPOLICY /PWD:p@ssw0rd
```

EXPORT. Programmeinstellungen exportieren

Mit dem Befehl `KAVSHELL EXPORT` können Sie aus einer Konfigurationsdatei im XML-Format Einstellungen von Kaspersky Embedded Systems Security exportieren. In einer Konfigurationsdatei können entweder alle Einstellungen des Programms oder nur die Einstellungen bestimmter Programmkomponenten gespeichert werden.

Syntax des Befehls

```
KAVSHELL EXPORT <profile> <file name> [/LOGIN:<user name>] [/PWD:<password>]
```

Befehlsoptionen

Einstellung	Beschreibung
`<profile>`	Obligatorisches Argument. Geben Sie den Namen des Profils für den Export der Einstellungen ein. Ein Profil ist eine Komponente, Aufgabe oder Funktion von Kaspersky Embedded Systems Security. Eine Liste der verfügbaren Profile erhalten Sie mit dem Befehl `KAVSHELL EXPORT /?`. Um alle Programmeinstellungen zu exportieren, geben Sie das Profil `product` an.

`<file name>`	Obligatorisches Argument. Geben Sie den Namen der Datei im XML-Format an, in die die Profileinstellungen exportiert werden sollen. Sie können auch den Dateipfad angeben. Beispiel: `C:\Test\settings.xml` • Wenn im Befehl nur ein Dateiname angegeben ist, versucht das Programm, die Datei im Installationsordner des Programms abzulegen. Wenn die Selbstschutzmechanismen des Programms aktiviert sind, schlägt der Export fehl, da der Selbstschutz des Programms das Erstellen einer neuen Datei im Programmordner blockiert. Geben Sie den Dateipfad an, um die Programmeinstellungen zu exportieren.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.

Beispiel

```
KAVSHELL EXPORT product C:\Test\settings.xml /LOGIN:Admin /PWD:p@ssw0rd
```

FBRESET. iSwift-Datenbank leeren

Kaspersky Embedded Systems Security kann die iSwift-Technologie verwenden. Dadurch kann die Anwendung vermeiden, Dateien erneut zu untersuchen, die seit der letzten Untersuchung nicht verändert wurden. Der Befehl `KAVSHELL FBRESET` leert die Datenbank, in der Informationen über untersuchte, nicht infizierte Dateien gespeichert werden. Nach dem Leeren der Datenbank untersucht Kaspersky Embedded Systems Security alle Dateien, auf die die Anwendung erstmals zugreift.

Syntax des Befehls

```
KAVSHELL FBRESET
```

FIM /BASELINE. Baseline-Überwachung der Systemintegrität

Mit dem Befehl `KAVSHELL FIM /BASELINE` können Sie die Aufgabe *Baseline-Überwachung der Systemintegrität* verwalten.

```
KAVSHELL FIM /BASELINE [[/CREATE {<monitoring scope>|/L:<path to TXT file containing the list of monitoring areas>}] [/MD5 | /SHA256] [/SF] [/W:<file name>] [/ANSI]] [/SCAN {[/BL:<id baseline>] | [/ALIAS:<existing task id>]} [/W:<file name>] [/ANSI]] [/CLEAR [/BL:<id baseline>] | [/ALIAS:<existing task id>]] [/SHOW [[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/EXPORT:<path to folder>[[/BL:<id baseline>] | [/ALIAS:<existing task id>]]] [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/CREATE`	Starten einer neuen *Baseline-Überwachung der Systemintegrität*-Aufgabe, die einen Snapshot des Systemstatus erstellt.

`/SCAN`	Führen Sie *Baseline-Überwachung der Systemintegrität*-Aufgaben mit der ID des System-Snapshots oder dem alternativen Namen einer vorhandenen Aufgabe aus.
`/CLEAR`	Baseline löschen. Geben Sie die ID eines System-Snapshots oder den alternativen Namen der Aufgabe an, die den Snapshot erstellt hat. Wenn weder ein alternativer Aufgabenname noch eine Snapshot-ID angegeben ist, löscht die Anwendung alle Snapshots.
`/EXPORT`	Exportiert die Daten aller Snapshots oder des mit der Option `/BL` angegebenen Snapshots in eine TXT-Datei im angegebenen Ordner.
`/SHOW`	Zeigt Daten aus allen Snapshots des Systemstatus oder aus dem mit der Option `/BL` angegebenen Snapshot an.
`<monitoring scope>`	Erforderlich, wenn /L nicht angegeben ist. Legt den Überwachungsbereich der Aufgabe fest. Mithilfe der Zeichen `*` und `?` können Sie eine Pfadmaske eingeben.
`/L`	Erforderlich, wenn `<monitoring scope>` nicht angegeben ist. Ermöglicht die Angabe des Pfads zur TXT-Datei, welche die Liste der Überwachungsbereiche enthält.
`/MD5`	Optionales Argument. Kann nicht zusammen mit dem Parameter `/SHA256` verwendet werden. Legt den MD5-Algorithmus zur Berechnung der Prüfsumme fest. Der MD5-Algorithmus wird standardmäßig verwendet.
`/SHA256`	Optionales Argument. Kann nicht zusammen mit dem Parameter `/MD5` verwendet werden. Legt den SHA256-Algorithmus zur Berechnung der Prüfsumme fest. Der MD5-Algorithmus wird standardmäßig verwendet.
`/SF`	Optionales Argument. Bezieht alle Unterordner in den Überwachungsbereich der Aufgabe ein. Standardmäßig werden Unterordner nicht in den Überwachungsbereich einbezogen.
`/ALIAS:<existing task id>`	Erforderlich, wenn `/BL` nicht angegeben ist. Aufgabenalias. Sie können den Aufgabenalias mithilfe des Befehls `KAVSHELL FIM /BASELINE /SHOW` ermitteln.
`/BL:<id baseline>`	Erforderlich, wenn `/ALIAS` nicht angegeben ist. Legt die ID des System-Snapshots fest. Sie können die Baseline-ID mithilfe des Befehls `KAVSHELL FIM /BASELINE /SHOW` ermitteln.
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL FIM /BASELINE /CREATE "c:\program files\*" /MD5 /SF
KAVSHELL FIM /BASELINE /CREATE /L:c:\programdata\mytask\list.txt /ALIAS:SystemIntegrityMonitorOnDemandTask$001
/MD5 /SF
KAVSHELL FIM /BASELINE /SCAN /ALIAS:SystemIntegrityMonitorOnDemandTask$001
KAVSHELL FIM /BASELINE /EXPORT:c:\programdata\mytask\baselines\
```

HELP. Anzeigen der Hilfe zu Befehlen

Um eine Liste aller verfügbaren Befehle für Kaspersky Embedded Systems Security anzuzeigen, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Um die Beschreibung und Syntax eines Befehls anzuzeigen, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL HELP <command>
KAVSHELL <command> /?
```

Beispiel

```
KAVSHELL HELP SCAN
```

IMPORT. Programmeinstellungen importieren

Mit dem Befehl `KAVSHELL IMPORT` können Sie aus einer Konfigurationsdatei im XML-Format Einstellungen von Kaspersky Embedded Systems Security importieren. Eine Konfigurationsdatei kann mit dem Befehl `KAVSHELL EXPORT` erstellt werden.

Syntax des Befehls

```
KAVSHELL IMPORT <file_name> /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`<file name>`	Obligatorisches Argument. Geben Sie den vollständigen Pfad zur XML-Datei einschließlich ihres Namens und ihrer Erweiterung an, aus der Sie die Einstellungen importieren möchten.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL IMPORT C:\Test\settings.xml /PWD:p@ssw0rd
```

Rückgabewerte des Befehls:

- 0: Der Vorgang wurde erfolgreich abgeschlossen.
- -2: Der Dienst wird nicht ausgeführt.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.
- -4: Objekt nicht gefunden.
- -9: Der Versuch, das verwaltete Gerät unter einem anderen Benutzerkonto auszuführen, ist fehlgeschlagen.
- -99: Unbekannter Fehler.
- -501: Der Vorgang wurde erfolgreich abgeschlossen, bei der Ausführung ist jedoch ein Fehler oder eine Warnung aufgetreten (beispielsweise hat das Programm die Einstellungen einiger Komponenten nicht importiert).
- -502: Die Importdatei ist nicht vorhanden oder hat ein unbekanntes Format.
- -503: Inkompatible Einstellungen (die Konfigurationsdatei wurde aus einem anderen Programm oder einer neueren, inkompatiblen Version von Kaspersky Embedded Systems Security exportiert).

KSN. Verwenden von KSN/KPSN

Mit dem Befehl `KAVSHELL KSN` können Sie eine Kaspersky-Lösung auswählen, um die Reputation von Dateien oder Websites zu ermitteln. Kaspersky Embedded Systems 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 Embedded Systems 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.

Syntax des Befehls

```
KAVSHELL KSN /GLOBAL|/PRIVATE <settings-file> /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/GLOBAL`	Wechsel zur Verwendung von Kaspersky Security Network.

`/PRIVATE <settings-file>`	Wechsel zur Verwendung von Kaspersky Private Security Network. Geben Sie den Namen der Konfigurationsdatei an, die die Einstellungen von Kaspersky Private Security Network enthält. Diese Datei hat die Erweiterung .PKCS7 oder .PEM.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL KSN /GLOBAL /PWD:p@ssw0rd
KAVSHELL KSN /PRIVATE c:\settings.pkcs7 /PWD:p@ssw0rd
```

LICENSE. Aktivierung des Programms

Die Schlüssel und Aktivierungscodes von Kaspersky Embedded Systems Security können mit dem Befehl `KAVSHELL LICENSE` verwaltet werden.

Syntax des Befehls

```
KAVSHELL LICENSE [/ADD:<key_file | activation code> [/R]|/DEL:<license key serial number>|/REFRESH:<license id>]
/PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
Keine Optionen angegeben.	Der Befehl gibt folgende Informationen über die hinzugefügten Schlüssel zurück: • Schlüssel. • Lizenztyp (kommerziell). • Gültigkeitsdauer der Lizenz, die zum Schlüssel gehört. • Status des Schlüssels (aktiv oder Reserve). Wenn der Status * ist, wurde der Schlüssel als Reserveschlüssel hinzugefügt.
`/ADD:<key_file | activation code>`	Aktivieren von Kaspersky Embedded Systems Security mit einer Schlüsseldatei. Wenn das Programm bereits aktiviert ist, wird der Schlüssel als Reserveschlüssel hinzugefügt.
`/R`	Wenn die Option `/R` angegeben wird, wird der Aktivierungscode oder Schlüssel als Reservecode bzw. Reserveschlüssel hinzugefügt.
`/DEL:<license key serial number>`	Löschen Sie den angegebenen Schlüssel oder Aktivierungscode.
`/REFRESH:<license id>`	Aktualisieren Sie den Status der angegebenen Lizenz.
`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Rückgabewerte des Befehls:

- 0: Der Vorgang wurde erfolgreich abgeschlossen.
- -2: Der Dienst wird nicht ausgeführt.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.
- -4: Schlüssel mit der angegebenen Nummer nicht gefunden.
- -5: Syntaxfehler.
- -6: Ungültiger Vorgang (Schlüssel bereits hinzugefügt).
- -99: Unbekannter Fehler.
- -301: Die Lizenz ist ungültig.
- -303: Die Lizenz gilt für ein anderes Programm.

MDR. Konfiguration der Integration von Managed Detection and Response

Mit dem Befehl `KAVSHELL MDR` können Sie die Integration von Kaspersky Embedded Systems Security in die Lösung Managed Detection and Response konfigurieren.

Syntax des Befehls

```
KAVSHELL MDR /ENABLE [/PWD:<password>] [/LOGIN:<user name>] | /DISABLE [/PWD:<password>] [/LOGIN:<user name>] |
/SHOW
```

Befehlsoptionen

Einstellung	Beschreibung
`MDR /<enable|disable|show>`	Obligatorisches Argument. Ermöglicht das Aktivieren, Deaktivieren oder Anzeigen der aktuellen Einstellungen der Komponente Managed Detection and Response.
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL MDR /ENABLE /PWD:p@ssw0rd
KAVSHELL MDR /DISABLE /PWD:p@ssw0rd
KAVSHELL MDR /SHOW
```

OMSINFO. Erstellen einer JSON-Datei mit Informationen über das Programm

Mit dem Befehl `KAVSHELL OMSINFO` können Sie eine JSON-Datei mit Informationen über den aktuellen Status des Programms und erkannte Bedrohungen erstellen, die Sie anschließend in Überwachungssysteme hochladen können.

Syntax des Befehls

```
KAVSHELL OMSINFO <oms_info_json_file_name>
```

Befehlsoptionen

Einstellung	Beschreibung
`<oms_info_json_file_name>`	Vollständiger Pfad der JSON-Datei, einschließlich Name und Erweiterung.

Beispiel

```
KAVSHELL OMSINFO "C:\Dumps and others\omsinfo.json"
```

Kennwort. Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security

Mit dem Befehl `KAVSHELL PASSWORD` können Sie den passwortgeschützten Zugang zu den Funktionen von Kaspersky Embedded Systems Security verwalten. Ist diese Funktion aktiviert, so fragt das Programm den Benutzernamen und das Kennwort ab, wenn das Programm gelöscht, geändert oder wiederhergestellt werden soll, oder wenn über die Befehlszeile Aktionen ausgeführt werden, die die Schutzstufe des Geräts verringern können.

Syntax des Befehls

```
KAVSHELL PASSWORD /SET /NEW:<new password> | /RESET /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/SET`	Aktiviert die Kennwortabfrage zur Bestätigung kritischer Aktionen.
`/NEW:<new password>`	Erforderlich, wenn `/SET` angegeben wird. Legt ein neues Kennwort fest. Wenn Sie ein Kennwort erstellen, sollten Sie folgende Empfehlungen beachten: • Das Kennwort darf weder Kontoname noch Computername enthalten. • Das Kennwort ist mindestens 8 Zeichen lang. • Das Kennwort enthält Zeichen aus mindestens drei der folgenden Kategorien: • Lateinische Großbuchstaben (A–Z) • Lateinische Kleinbuchstaben (a–z) • Ziffern (0–9) • Ausrufezeichen (!), Dollarzeichen ($), Raute (#) und Prozentzeichen (%)
`/RESET`	Deaktiviert die Kennwortabfrage zur Bestätigung kritischer Aktionen.

`/PWD:<password>`	Obligatorisches Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

PATCHCOMPATIBILITYRESET. Entfernen eines Patches aus der Liste der inkompatiblen Patches

Mit dem Befehl `KAVSHELL PATCHCOMPATIBILITYRESET` können Sie einen Patch mit der angegebenen GUID aus der Liste der inkompatiblen Patches entfernen. Sie können mehrere durch Leerzeichen getrennte GUIDs angeben.

Syntax des Befehls

```
KAVSHELL PATCHCOMPATIBILITYRESET <GUID> [GUID...]
```

Beispiel

```
KAVSHELL PATCHCOMPATIBILITYRESET 01234567-890A-BCDE-F012-34567890ABCD
```

REMOTEACCESS. Verwalten der Einstellungen für die Remote-Verbindung der Programmkonsole

Mit dem Befehl `KAVSHELL REMOTEACCESS` können Sie die Einstellungen für die Remote-Verbindung der Programmkonsole mit dem Gerät verwalten, auf dem Kaspersky Embedded Systems Security installiert ist.

Syntax des Befehls

```
KAVSHELL REMOTEACCESS /SET /PORT=<new_port> [/PWD:<password>] [/LOGIN:<user name>] | /RESET UIKLPORT [/PWD:
<password>] [/LOGIN:<user name>] | /SHOW
```

Befehlsoptionen

Einstellung	Beschreibung
`/SET [UIPORT | UIKLPORT]`	Legen Sie die Portnummer fest: • `UIPORT` ist der Port für die Verbindung mit Windows-Anmeldeinformationen. • `UIKLPORT` ist der Port für die Verbindung mit den Anmeldeinformationen manuell erstellter Benutzer.
`/PORT=<new_port>`	Erforderlich, wenn `/SET` angegeben wird. Portnummer. Bereich der möglichen Werte: 1–65535.
`/RESET UIKLPORT`	Schließen Sie den Port für die Verbindung mit den Anmeldeinformationen manuell erstellter Benutzer.
`/SHOW`	Geben Sie die aktuellen Portnummern aus.

`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL REMOTEACCESS /SET UIPORT /PORT=50000
KAVSHELL REMOTEACCESS /RESET UIKLPORT
KAVSHELL REMOTEACCESS /SHOW
```

RESETMDRMACHINEID. Zurücksetzen der Geräte-ID

Mit dem Befehl `KAVSHELL RESETMDRMACHINEID` können Sie die Geräte-ID zurücksetzen, die von der Lösung Managed Detection and Response verwendet wird.

Syntax des Befehls

```
KAVSHELL RESETMDRMACHINEID [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

ROLLBACK. Rollback des letzten Updates

Der Befehl `KAVSHELL ROLLBACK` startet die Aufgabe *Rollback des letzten Updates*.

Syntax des Befehls

```
KAVSHELL ROLLBACK [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.

`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL ROLLBACK
```

Rückgabewerte des Befehls:

- 0: Der Vorgang wurde erfolgreich abgeschlossen.
- -2: Der Dienst wird nicht ausgeführt.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.
- -99: Unbekannter Fehler.
- -221: Die Backup-Kopie der Datenbank wurde nicht gefunden oder ist beschädigt.
- -222: Die Backup-Kopie der Datenbank ist beschädigt.

RTP. Echtzeitschutz für Dateien

Mit dem Befehl `KAVSHELL RTP` können Sie die Komponente Echtzeitschutz für Dateien aktivieren oder deaktivieren.

Syntax des Befehls

```
KAVSHELL RTP </START|/STOP> [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`</START|/STOP>`	Aktivieren oder deaktivieren Sie die Komponente Echtzeitschutz für Dateien: • `/START` aktiviert die Komponente. • `/STOP` deaktiviert die Komponente.
`/PWD:<password>`	Erforderliche Option für den Befehl `KAVSHELL RTP /STOP`. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL RTP STOP /PWD:p@ssw0rd
```

SCAN. Untersuchung auf Befehl

Mit dem Befehl `KAVSHELL SCAN` können Sie die Aufgabe *Untersuchung auf Befehl* erstellen und starten. Um eine vorhandene Aufgabe zur Untersuchung auf Befehl über die Befehlszeile zu starten, verwenden Sie den Befehl `KAVSHELL TASK`.

Syntax des Befehls

```
KAVSHELL SCAN <scan_scope> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<file_name>][/F<A|C|E>]
[/NEWONLY][/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|DELETE]
[/E:<ABMSPO>] [/EM:<"masks">] [/ES:<size>] [/ET:<s>][/TZOFF] [/NOICHECKER][/NOISWIFT][/NOCHECKMSSIGN]
[/ANALYSERLEVEL] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`<scan_scope>`	Obligatorisches Argument. Durch Leerzeichen getrennte Liste von Dateien, Ordnern, Netzwerkpfaden oder Standard-Untersuchungsbereichen. Standard-Untersuchungsbereiche: • `/MEMORY` untersucht alle Prozesse im Arbeitsspeicher. • `/SHARED` untersucht freigegebene Ordner. • `/STARTUP` untersucht Autostart-Objekte. • `/REMDRIVES` untersucht Wechseldatenträger. • `/FIXDRIVES` untersucht alle lokalen Festplatten. • `/MYCOMP` untersucht den gesamten Computer. Sie können mehrere durch Leerzeichen getrennte Werte angeben.
`/L:<file_name>`	Optionales Argument. Pfad zur Datei mit einer Liste von Untersuchungsbereichen. Die Datei muss manuell erstellt und im TXT-Format gespeichert werden. Die Datei muss in UTF-8-Kodierung ohne BOM gespeichert werden.
`/F<A|C|E>`	Optionales Argument. Objekte, die in den Untersuchungsbereich aufgenommen werden sollen: • `/FA`: Alle Objekte untersuchen. Das Programm untersucht ausnahmslos alle Dateien (alle Formate und Erweiterungen). • `/FC`: Objekte nach Format untersuchen. Das Programm untersucht nur Objekte, deren Formate in der Liste der als infizierbar geltenden Objekte enthalten sind. • `/FE`: Objekte nach Erweiterung untersuchen. Das Programm untersucht nur Objekte, die der Erweiterung nach als infizierbar gelten.
`/NEWONLY`	Optionales Argument. Nur neue und veränderte Dateien untersuchen. Wird dieses Argument nicht übergeben, untersucht Kaspersky Embedded Systems Security alle Objekte.
`/AI:` `<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>`	Optionales Argument. Die Aktion, die das Programm mit infizierten und anderen Objekten ausführen soll: • `DISINFECT`: Desinfizieren – Informieren, wenn Desinfektion fehlschlägt. • `DISINFDEL`: Desinfizieren – Löschen, wenn Desinfektion fehlschlägt. • `DELETE`: Löschen. • `REPORT` (Standardwert): Informieren. • `AUTO`: Empfohlen.

Einstellung	Beschreibung
`/AS:<QUARANTINE|DELETE|REPORT|AUTO>`	Optionales Argument. Die Aktion, die das Programm mit infizierten Objekten ausführen soll: • `QUARANTINE`: In Quarantäne verschieben. • `DELETE`: Löschen. • `REPORT` (Standardwert): Informieren. • `AUTO`: Empfohlen.
`/E:<ABMSPO>`	Angegebene Objekttypen ausschließen. Mögliche Werte: • `A`: Archive in den Formaten ZIP, CAB, RAR, ARJ und anderen Formaten. • `B`: Dateien in Mail-Datenbanken für Microsoft Outlook und Microsoft Outlook Express. • `M`: Dateien in Mail-Formaten, beispielsweise Nachrichten von Microsoft Outlook und Microsoft Outlook Express. • `S`: selbstentpackende Archive. • `P`: ausführbare Dateien, die mit Packprogrammen für Binärcode wie UPX oder ASPack gepackt wurden. • `O`: in Dateien eingebettete Objekte (beispielsweise Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten). Sie können mehrere Parameterwerte angeben.
`/EM=<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.
`/ET=<scan duration in seconds>`	Dateien, deren Untersuchung die in Sekunden vorgegebene Dauer überschreitet, von der Untersuchung ausschließen. Als Standard gilt der Wert 60 Sek.
`/ES=<size in megabytes>`	Dateien, deren Größe den in Megabyte vorgegebenen Wert überschreitet, von der Untersuchung ausschließen. Der Standardwert ist 100 MB.
`/TZOFF`	Ausnahmen für die vertrauenswürdige Zone nicht anwenden.
`/NOICHECKER`	iChecker-Technologie deaktivieren (standardmäßig aktiviert).
`/NOISWIFT`	iSwift-Technologie deaktivieren (standardmäßig aktiviert).
`/NOCHECKMSSIGN`	Dateien, die von Microsoft digital signiert sind, nicht untersuchen.
`/ANALYSERLEVEL`	Verwendung der heuristischen Analyse aktivieren, Analyseniveau einstellen. Die folgenden Ebenen der heuristischen Analyse verfügbar: • `1`: oberflächlich. • `2`: mittel. • `3`: tief. Wenn dieses Argument nicht angegeben wird, verwendet die Anwendung die heuristische Analyse nicht.
`/EXCLUDE=<list of exlusion`	Liste der Dateien, Ordner oder Netzwerkpfade, die aus dem Untersuchungsbereich der Aufgabe ausgeschlossen werden. Sie können mehrere durch Leerzeichen getrennte Werte angeben.
`/W=<file path>`	Pfad und Name der Datei mit dem Protokoll der Aufgabenausführung. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben.
`/ANSI`	Verwenden Sie die ANSI-Codierung für Ereignisse, die in das Protokoll der Aufgabenausführung geschrieben werden. Der Parameter `/ANSI` wird nicht angewendet, wenn der Parameter `/W` nicht übergeben wird. Wenn der Parameter `/ANSI` nicht angegeben ist, wird Unicode zum Erstellen des Protokolls der Aufgabenausführung verwendet.
`/ALIAS:<alternate name>`	Weisen Sie der Aufgabe einen temporären Namen zu, über den während der Ausführung auf sie verwiesen werden kann. Mit dem Befehl `KAVSHELL TASK` können Sie beispielsweise eine Aufgabenstatistik anzeigen lassen. Der alternative Aufgabenname muss unter allen alternativen Aufgabennamen im Programm eindeutig sein. Wenn dieses Argument nicht übergeben wird, wird der Aufgabenname wie folgt zugewiesen: scan_<kavshell_pid>. Beispiel: scan_1234.

Beispiel

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\003.exe "\\another server\Shared\"
```

```
F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER
/NOISWIFT /W:log.log
KAVSHELL SCAN /L:scan_objects.lst /W:log.log
```

Rückgabewerte des Befehls:

- 0: Vorgang erfolgreich ausgeführt (keine Bedrohungen gefunden).
- 1: Vorgang abgebrochen.
- -2: Der Dienst wird nicht ausgeführt.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.
- -4: Objekt nicht gefunden (Datei mit der Liste der Untersuchungsbereiche nicht gefunden).
- -5: Syntaxfehler oder Untersuchungsbereich nicht festgelegt.
- -80: Infizierte Objekte gefunden.
- -81: Möglicherweise infizierte Objekte gefunden.
- -82: Fehler bei der Objektverarbeitung während der Untersuchung.
- -83: Nicht untersuchte Objekte gefunden.
- -84: Beschädigte Objekte gefunden.
- -85: Fehler beim Erstellen des Protokolls der Aufgabenausführung.
- -99: Unbekannter Fehler.
- -301: Die Lizenz ist ungültig.

SCANCRITICAL. Untersuchung wichtiger Bereiche

Der Befehl `KAVSHELL SCANCRITICAL` startet die Aufgabe *Untersuchung wichtiger Bereiche*.

Syntax des Befehls

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>] [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/W`	Optionales Argument. Geben Sie für das exportierte Protokoll der Aufgabenausführung einen Dateinamen mit der Erweiterung .LOG an. Sie können auch den Dateipfad angeben. Wenn im Befehl nur ein Dateiname angegeben ist, versucht das Programm, die Datei im Installationsordner des Programms abzulegen. Wenn die Selbstschutzmechanismen des Programms aktiviert sind, schlägt der Export fehl, da der Selbstschutz des Programms das Erstellen einer neuen Datei im Programmordner blockiert. Geben Sie zum Exportieren des Protokolls den Dateipfad an.
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.

`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

SERVERBINDINGDISABLE. Schutz der Verbindung zum Administrationsserver deaktivieren

Der Befehl `KAVSHELL SERVERBINDINGDISABLE` deaktiviert lokal den Schutz der Verbindung zum Administrationsserver. Der Befehl startet die Aufgabe *Schutz der Verbindung zum Administrationsserver*, die das Kennwort für die Verbindung des Computers zum Administrationsserver entfernt.

Syntax des Befehls

```
KAVSHELL SERVERBINDINGDISABLE [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

START. Starten des Programmdienstes

Der Befehl `KAVSHELL START` startet den Dienst Kaspersky Embedded Systems Security Service.

Syntax des Befehls

```
KAVSHELL START
```

STARTPOLICY. Richtlinie aktivieren

Der Befehl `KAVSHELL STARTPOLICY` aktiviert die Kaspersky Security Center-Richtlinie auf dem geschützten Gerät. Die Programmeinstellungen werden gemäß der Richtlinie angepasst.

Syntax des Befehls

```
KAVSHELL STARTPOLICY
```

STOP. Beenden des Programmdienstes

Der Befehl `KAVSHELL STOP` beendet den Dienst Kaspersky Embedded Systems Security Service.

Syntax des Befehls

```
KAVSHELL STOP [/PWD:<password>] [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Rückgabewerte des Befehls:

- 0: Der Vorgang wurde erfolgreich abgeschlossen.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.
- -5: Syntaxfehler.
- -6: Ungültiger Vorgang (Kaspersky Embedded Systems Security Service wurde bereits beendet).
- -7: Dienst ist nicht registriert
- -8: Automatischer Dienststart ist deaktiviert.
- -9: Der Versuch, das verwaltete Gerät unter einem anderen Benutzerkonto auszuführen, ist fehlgeschlagen.
- -99: Unbekannter Fehler.

AUFGABE. Verwalten von Aufgaben

Mit dem Befehl `KAVSHELL TASK` können Sie die Aufgaben von Kaspersky Embedded Systems Security verwalten: die Aufgabe starten, anhalten, fortsetzen und beenden sowie den aktuellen Aufgabenstatus und die Aufgabenstatistik anzeigen.

Syntax des Befehls

```
KAVSHELL TASK [<alternative name> </START | /STOP | /STATE | /STATISTICS>] /PWD:<password> [/LOGIN:<user name>]
```

Befehlsoptionen

Einstellung	Beschreibung
Keine Parameter	Zeigt die Liste aller vorhandenen Aufgaben von Kaspersky Embedded Systems Security an. Die Liste enthält die folgenden Felder: den alternativen Namen der Aufgabe (einen zusätzlichen Kurznamen, den Kaspersky Embedded Systems Security für Windows Aufgaben zuweist), die Kategorie der Aufgabe (System oder Benutzer) und den aktuellen Status der Aufgabe.
`<alternative name>`	Alternativer Name für die Aufgabe, die Sie verwalten möchten. Um die alternativen Namen der Aufgaben von Kaspersky Embedded Systems Security anzuzeigen, geben Sie den Befehl `KAVSHELL TASK` ohne Parameter ein.
`/START`	Starten einer Aufgabe.
`/STOP`	Beenden einer Aufgabe.
`/STATE`	Anzeigen des aktuellen Status der Aufgabe.
`/STATISTICS`	Anzeigen der Aufgabenstatistik.
`/PWD:<password>`	Erforderliche Option für den Befehl `KAVSHELL TASK /STOP`. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Syntax des Befehls

```
KAVSHELL TASK on-access /START
KAVSHELL TASK user-task_1 /STOP
KAVSHELL TASK scan-critical /STATE
```

Rückgabewerte des Befehls:

- 0: Der Vorgang wurde erfolgreich abgeschlossen.
- -2: Der Dienst wird nicht ausgeführt.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.
- -4: Objekt nicht gefunden (Aufgabe nicht gefunden).
- -5: Syntaxfehler oder Untersuchungsbereich nicht festgelegt.
- -6: Ungültiger Vorgang (zum Beispiel wurde die Aufgabe nicht gestartet, bereits gestartet oder kann nicht angehalten werden).
- -99: Unbekannter Fehler.

- -301: Die Lizenz ist ungültig.
- 401: Aufgabe nicht gestartet (für den Befehl `KAVSHELL TASK <task name> /STATE`).
- 402: Aufgabe bereits gestartet (für den Befehl `KAVSHELL TASK <task name> /STATE`).
- 403: Aufgabe angehalten (für den Befehl `KAVSHELL TASK <task name> /STATE`).
- -404: Vorgang fehlgeschlagen (eine Änderung des Aufgabenstatus führte zu einem Absturz).

TRACE. Protokollierung der Anwendungsausführung

Mit dem Befehl `KAVSHELL TRACE` können Sie die Protokollierung für die Anwendung aktivieren oder deaktivieren.

Syntax des Befehls

```
KAVSHELL TRACE </ON /F:<traces_folder:>[/S:<traces_size_in_MB>] [/LVL:<debug|info|warning|error|critical>] /R:<max
trace files to rotate> | /OFF > [/LOGIN:<user name>] [/PWD:<password>]
```

Befehlsoptionen

Einstellung	Beschreibung
`</ON | /OFF>`	Obligatorisches Argument. Aktivieren oder deaktivieren Sie die Protokollierung für die Anwendung.
`/F:<traces_folder>`	Erforderlich, wenn `/ON` angegeben wird. Pfad zum Ordner, in dem die Protokolldateien gespeichert werden.
`/S:<traces_size_in_MB>`	Optionales Argument. Maximale Größe der Protokolldatei in Megabyte. Verfügbare Werte: von 1 bis 4095 MB. Der Standardwert ist 100 MB.
`/LVL: <debug|info|warning|error|critical>`	Optionales Argument. Protokollierungsstufe für Debug-Informationen. • `critical` bedeutet: In der Protokolldatei werden nur Meldungen über schwerwiegende Fehler gespeichert. • `error` bedeutet: In der Protokolldatei werden Meldungen über alle Fehler sowie Warnungen gespeichert. • `warning` bedeutet: In der Protokolldatei werden Meldungen über alle Fehler, Warnungen sowie zusätzliche Informationen gespeichert. • `info` (Standardwert) bedeutet: In der Protokolldatei werden Meldungen über alle Fehler, Warnungen sowie Informationen über den normalen Betrieb des Programms gespeichert. • `debug` bedeutet: In der Protokolldatei werden alle Informationen über den Betrieb des Programms gespeichert.
`/R:<max trace files to rotate>`	Optionales Argument. Maximale Anzahl von Dateien in einem Ablaufprotokoll. Verfügbare Werte: von 1 bis 999. Der Standardwert ist 5.
`/PWD:<password>`	Optionales Argument. Kennwort des KL Admin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.

`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KL Admin-Kennwort angegeben haben.

Beispiel

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:info /R:50 /PWD:p@ssw0rd
KAVSHELL TRACE /OFF
```

UPDATE. Update der Datenbanken und Programm-Module

Mit dem Befehl `KAVSHELL UPDATE` können Sie die Aufgabe *Update* verwalten.

Syntax des Befehls

```
KAVSHELL UPDATE <update_source | /AK | /KL> [/NOUSEKL] [/PROXY:<IP address>:<port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:
<user_name>] [/PROXYPWD:<password>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<s>] [/REG:<code_by_iso3166>] [/W:<report_file>] [/ANSI] [/ALIAS:<alternate name>]
```

Befehlsoptionen

Einstellung	Beschreibung
`<update_source | /AK | /KL>`	Obligatorisches Argument. Wählen Sie die Update-Quelle aus: • `<update_source>`, um benutzerdefinierte Update-Quellen zu verwenden. Sie können den Pfad zu einem Ordner auf dem geschützten Gerät, den Pfad zu einem Netzwerkordner im UNC-Format oder die Adresse eines HTTP- oder FTP-Servers angeben, auf dem sich der Ordner mit den Updates befindet. • `/AK`, um den Kaspersky Security Center Administrationsserver als Update-Quelle zu verwenden. • `/KL`, um die Kaspersky-Update-Server als Update-Quelle zu verwenden. Sie können mehrere durch Leerzeichen getrennte Werte angeben.
`/NOUSEKL`	Optionales Argument. Kaspersky-Update-Server nicht verwenden, wenn andere Update-Quellen nicht verfügbar sind (Standardwert).
`/PROXY:<IP address>:<port>`	Optionales Argument. IP-Adresse oder symbolischer Name des Proxyservers und Portnummer.
`/AUTHTYPE:<0-2>`	Optionales Argument. Authentifizierungstyp des Proxyservers: • `0` für die NTLM-Authentifizierung mit dem aktuellen Benutzerkonto. • `1` für die NTLM-Authentifizierung mit einem Benutzerkonto, dessen Benutzername und Kennwort mit den Optionen `/PROXYUSER` und `/PROXYPWD` angegeben werden. • `2` für die Authentifizierung mit dem Benutzernamen und Kennwort, die mit den Optionen `/PROXYUSER` und `/PROXYPWD` angegeben werden.
`/PROXYUSER:<user_name>`	Erforderlicher Parameter, wenn der Parameter `/AUTHTYPE:1` oder `/AUTHTYPE:2` übergeben wird. Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn `/AUTHTYPE:0` angegeben ist, werden die Optionen `/PROXYUSER:<user_name>` und `/PROXYPWD:<password>` ignoriert.
`/PROXYPWD:<password>`	Erforderlicher Parameter, wenn der Parameter `/AUTHTYPE:1` oder `/AUTHTYPE:2` übergeben wird. Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn `/AUTHTYPE:0` angegeben ist, werden die Optionen `/PROXYUSER:<user_name>` und `/PROXYPWD:<password>` ignoriert. Wenn der Parameter `/PROXYUSER` angegeben und der Parameter `/PROXYPWD` ausgelassen wird, wird das Kennwort als leere Zeichenfolge betrachtet.
`/NOPROXYFORKL`	Optionales Argument. Proxyserver-Einstellungen für die Verbindung mit Kaspersky-Update-Servern nicht verwenden.

`/USEPROXYFORCUSTOM`	Optionales Argument. Proxyserver-Einstellungen für die Verbindung mit benutzerdefinierten Update-Quellen verwenden.
`/USEPROXYFORLOCAL`	Optionales Argument. Proxyserver-Parameter für die Verbindung zu lokalen Update-Quellen verwenden.
`/NOFTPPASSIVE`	Optionales Argument. Wenn diese Option angegeben ist, verwendet Kaspersky Embedded Systems Security den aktiven Modus für die Verbindung mit dem FTP-Server. Wenn diese Option nicht übergeben wird, verwendet Kaspersky Embedded Systems Security nach Möglichkeit den passiven Verbindungsmodus.
`/TIMEOUT:<s>`	Optionales Argument. Zeitüberschreitung für die Verbindung mit einem FTP- oder HTTP-Server in Sekunden. Standardwert: 10 Sekunden
`/REG:<code_by_iso3166>`	Optionales Argument. Der Code des Landes, in dem sich das geschützte Gerät befindet, gemäß der Norm ISO 3166-1. Beispiel: `/REG:GR`. Wenn dieser Parameter nicht übergeben wird oder ein ungültiger Ländercode angegeben ist, ermittelt Kaspersky Embedded Systems Security den Standort anhand der regionalen Einstellungen des geschützten Geräts, auf dem die Programmkonsole installiert ist. Bei der Auswahl eines Update-Servers verwendet das Programm Standortinformationen.
`/W=<file path>`	Pfad und Name der Datei mit dem Protokoll der Aufgabenausführung. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben.
`/ANSI`	Verwenden Sie die ANSI-Codierung für Ereignisse, die in das Protokoll der Aufgabenausführung geschrieben werden. Der Parameter `/ANSI` wird nicht angewendet, wenn der Parameter `/W` nicht übergeben wird. Wenn der Parameter `/ANSI` nicht angegeben ist, wird Unicode zum Erstellen des Protokolls der Aufgabenausführung verwendet.
`/ALIAS:<alternate name>`	Weisen Sie der Aufgabe einen temporären Namen zu, über den während der Ausführung auf sie verwiesen werden kann. Mit dem Befehl `KAVSHELL TASK` können Sie beispielsweise eine Aufgabenstatistik anzeigen lassen. Der alternative Aufgabenname muss unter allen alternativen Aufgabennamen im Programm eindeutig sein. Wenn dieses Argument nicht übergeben wird, wird der Aufgabenname wie folgt zugewiesen: update_<kavshell_pid>. Beispiel: update_1234.
`/PWD:<password>`	Optionales Argument. Kennwort des KLAdmin-Benutzerkontos oder eines Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Kennworts auf.
`/LOGIN:<user name>`	Optionales Argument. Name des Benutzerkontos mit ausreichenden Berechtigungen. Wenn diese Option nicht angegeben ist, fordert das Programm Sie in der nächsten Zeile zur Eingabe des Benutzernamens auf. Sie müssen diesen Wert nicht eingeben, wenn Sie das KLAdmin-Kennwort angegeben haben.

Syntax des Befehls

```
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /USEPROXYFORCUSTOM /PROXY:proxy.company.com:8080
/AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd /TIMEOUT:100 /REG:ru /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE "\\Server\kav bases\" ftp://bases.company.com /NOUSEKL /USEPROXYFORCUSTOM
/PROXY:proxy.company.com:8080 /AUTHTYPE:2 /PROXYUSER:inetuser /PROXYPWD:p@ssw0rd
KAVSHELL UPDATE /AK /NOUSEKL
KAVSHELL UPDATE /KL /W:"C:\KAVREPORTS\daily update.log"
KAVSHELL UPDATE /AK /W:"C:\KAVREPORTS\daily update.log"
```

Rückgabewerte des Befehls:

- 0: Der Vorgang wurde erfolgreich abgeschlossen.
- 200: Alle Objekte sind aktuell.
- -2: Der Dienst wird nicht ausgeführt.
- -3: Unzureichende Berechtigungen zum Ausführen des Befehls.

- -5: Syntaxfehler.
- -99: Unbekannter Fehler.
- -206: Erweiterungsdateien fehlen in der angegebenen Quelle oder weisen ein unbekanntes Format auf.
- -209: Fehler beim Herstellen der Verbindung mit der Update-Quelle.
- -232: Authentifizierungsfehler beim Herstellen der Verbindung mit dem Proxyserver.
- -234: Verbindungsfehler bei Kaspersky Security Center.
- -235: Kaspersky Embedded Systems Security konnte beim Herstellen der Verbindung mit der Update-Quelle nicht authentifiziert werden.
- -236: Die Programmdatenbanken sind beschädigt.
- -301: Die Lizenz ist ungültig.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Informationen darüber, wie und zu welchen Bedingungen Sie technischen Support erhalten.

Wie Sie technischen Support erhalten

Wenn Sie in der Dokumentation oder in den anderen Informationsquellen zu Kaspersky Embedded Systems 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 Embedded Systems Security.

Kaspersky unterstützt Kaspersky Embedded Systems 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

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Programme von Kaspersky verwenden. Über das Portal Kaspersky CompanyAccount können Benutzer mit Kaspersky-Experten mithilfe von Online-Anfragen kommunizieren. Über das Portal Kaspersky CompanyAccount kann der Status der Verarbeitung elektronischer Anfragen durch Kaspersky-Spezialisten nachverfolgt sowie eine Chronik der elektronischen Anfragen gespeichert werden.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Ein Benutzerkonto ermöglicht Ihnen die zentralisierte Verwaltung von elektronischen Anfragen aller registrierten Mitarbeiter an Kaspersky sowie die Verwaltung der Rechte dieser Mitarbeiter in Kaspersky CompanyAccount.

Das Portal Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch

- Portugiesisch
- Russisch
- Französisch
- Japanisch

Mehr über Kaspersky CompanyAccount erfahren Sie auf der Website des Technischen Supports.

Bereitstellung erweiterter Diagnoseinformationen für die Spezialisten des Technischen Supports

Zur Optimierung von Support und Fehlerbehebung bei Programmproblemen fordern die Spezialisten des Technischen Supports Sie möglicherweise auf, die Programmeinstellungen vorübergehend zu Diagnosezwecken zu ändern. Dazu sind möglicherweise folgende Aktionen erforderlich:

- Aktivierung der Funktionalität, mit der erweiterte Diagnoseinformationen verarbeitet und gespeichert werden.
- Genaue Anpassung von Einstellungen bestimmter Softwarekomponenten, die nicht über die standardmäßige Benutzeroberfläche verfügbar sind.
- Änderung der Einstellungen für die Speicherung und Übertragung von verarbeiteten Diagnoseinformationen.
- Anpassen von Einstellungen für das Abfangen und für die Speicherung des Netzwerkverkehrs

Die Spezialisten des Technischen Supports teilen Ihnen alle Informationen mit, die zur Ausführung der genannten Aktionen erforderlich sind (Beschreibung der notwendigen Schritte, veränderbare Einstellungen, Konfigurationsdateien, Skripte, zusätzliche Befehlszeilenfunktionen, Debug-Module, spezielle Dienstprogramme usw.), und informieren Sie über die Zusammensetzung der für die Fehlersuche analysierten Daten. Die erweiterten Diagnoseinformationen werden auf dem Benutzercomputer gespeichert. Die gespeicherten Daten werden nicht automatisch an Kaspersky übertragen.

Wenn Sie sich mit einem Problem an die Experten des Technischen Supports wenden, werden Sie möglicherweise darum gebeten, einen Bericht über Kaspersky Embedded Systems Security zu erstellen und den Bericht an den Technischen Support von zu schicken. Die Experten des Technischen Supports von Kaspersky fordern Sie möglicherweise auf, eine Ablaufverfolgungsdatei zu erstellen, eine Speicherabbilddatei zu senden und mit dem Dienstprogramm „Kaspersky Get System Info“ einen Bericht zu erstellen.

Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Experten des Technischen Supports von ein AVZ-Skript erstellen, das dann an Sie geschickt wird. Mithilfe von AVZ-Skripten können Sie laufende Prozesse auf Bedrohungen analysieren, den Computer auf Bedrohungen untersuchen, infizierte Dateien desinfizieren oder entfernen und einen Bericht über die Untersuchungsergebnisse erstellen.

Die oben genannten Aktionen dürfen nur unter Anleitung von Spezialisten des Technischen Supports ausgeführt werden, wobei die Anweisungen genau befolgt werden müssen. Wenn die Programmeinstellungen auf eine andere Weise geändert werden, als in der Programmdokumentation oder in den Anleitungen des Technischen Supports beschrieben, kann es Verzögerungen und Störungen im Betriebssystem kommen, das Niveau des Computerschutzes kann sinken und der Zugriff auf und die Integrität von verarbeiteten Informationen können beeinträchtigt werden.

Protokollierung der Anwendungsausführung

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 das Programm eine Reihe von Dateien mit Daten über den Betrieb verschiedener Programmkomponenten.

Die Anwendungsnachverfolgung sollte nur unter Anleitung des Technischen Supports von Kaspersky ausgeführt werden.

Ablaufverfolgungsdateien ermöglichen eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

So aktivieren oder konfigurieren Sie die Anwendungsnachverfolgung (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Diagnose von Störungen**.
4. Klicken Sie im Block **Einstellungen der Diagnose von Störungen** auf **Einstellungen**.

   Das Fenster **Einstellungen der Diagnose von Störungen** wird auf der Registerkarte **Einstellungen der Programm-Ablaufverfolgung** des Dateiintegritätsmonitors geöffnet.
5. Verwenden Sie das Kontrollkästchen **Protokollierung aktivieren**, um die Ablaufverfolgung von Programmvorgängen zu aktivieren oder zu deaktivieren.

   Die Ablaufverfolgung von Programmvorgängen ist standardmäßig deaktiviert.
6. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Geben Sie dazu im Feld **Ordner für Protokolldateien** den vollständigen Pfad des lokalen Ordners an.

   Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

   Für die Protokolldateien erstellt Kaspersky Embedded Systems Security im ausgewählten Ordner einen Unterordner namens logs-Kaspersky Embedded Systems Security-<uid>, wobei <uid> eine eindeutige Protokoll-ID aus 8 Zeichen ist.
7. Wählen Sie die Protokollierungsstufe für die Debug-Informationen aus:

   - **Normal** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie Informationen über den normalen Betrieb des Programms gespeichert (Standard).
   - **Kritisch** bedeutet: In der Ablaufverfolgungsdatei werden nur Meldungen über schwerwiegende Fehler gespeichert.

- **Diagnose** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler sowie Warnungen gespeichert.
- **Wichtig** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie zusätzliche Informationen gespeichert.
- **Detailliert** bedeutet: In der Ablaufverfolgungsdatei werden alle Informationen über den Betrieb des Programms gespeichert.

Ein Mitarbeiter des technischen Supports bestimmt den Detailgrad, der zur Lösung möglicher Probleme erforderlich ist.

8. Um alte Protokolldateien zu löschen, aktivieren Sie die Funktionalität **Älteste Protokolldateien entfernen**.

   Wenn diese Funktionalität aktiviert ist, können Sie die maximale Größe und die Anzahl der Protokolldateien anpassen:

   a. Geben Sie die **Maximale Größe einer Protokolldatei (MB)** an.

      Verfügbare Werte: von 1 bis 4095 MB. Der Standardwert ist 100 MB.

   b. Geben Sie die **Maximale Anzahl der Dateien für ein Protokoll** an.

      Verfügbare Werte: von 1 bis 999. Der Standardwert ist 5.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder konfigurieren Sie die Anwendungsnachverfolgung (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Eigenschaften des Programms**.
   - Wählen Sie im Kontextmenü des Knotens den Punkt **Eigenschaften des Programms** aus.

   Das Fenster **Eigenschaften des Programms** wird geöffnet.

2. Wählen Sie die Registerkarte **Diagnose von Störungen** aus.

3. Klicken Sie im Block **Einstellungen der Diagnose von Störungen** auf **Einstellungen**.

   Das Fenster **Einstellungen der Diagnose von Störungen** wird geöffnet.

4. Wählen Sie die Registerkarte mit den Einstellungen der Ablaufverfolgung aus:

   - **Einstellungen der Programm-Ablaufverfolgung**. Kaspersky Embedded Systems Security startet die Ablaufverfolgung für das Programm.
   - **Einstellungen der Ablaufverfolgung für die Programmkonsole**. Wenn die Programmkonsole und Kaspersky Embedded Systems Security auf verschiedenen Computern installiert sind, können Sie die Ablaufverfolgung nur für die Programmkonsole starten.

5. Verwenden Sie das Kontrollkästchen **Protokollierung aktivieren**, um die Ablaufverfolgung von Programmvorgängen zu aktivieren oder zu deaktivieren.

   Die Ablaufverfolgung von Programmvorgängen ist standardmäßig deaktiviert.

6. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Klicken Sie dazu auf **Durchsuchen** und wählen Sie den gewünschten Ordner aus.

Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

Für die Protokolldateien erstellt Kaspersky Embedded Systems Security im ausgewählten Ordner einen Unterordner namens logs-Kaspersky Embedded Systems Security-<uid>, wobei <uid> eine eindeutige Protokoll-ID aus 8 Zeichen ist.

7. Wählen Sie die Protokollierungsstufe für die Debug-Informationen aus:

   - **Normal** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie Informationen über den normalen Betrieb des Programms gespeichert (Standard).
   - **Kritisch** bedeutet: In der Ablaufverfolgungsdatei werden nur Meldungen über schwerwiegende Fehler gespeichert.
   - **Diagnose** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler sowie Warnungen gespeichert.
   - **Wichtig** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie zusätzliche Informationen gespeichert.
   - **Detailliert** bedeutet: In der Ablaufverfolgungsdatei werden alle Informationen über den Betrieb des Programms gespeichert.

   Ein Mitarbeiter des technischen Supports bestimmt den Detailgrad, der zur Lösung möglicher Probleme erforderlich ist.

8. Um alte Protokolldateien zu löschen, aktivieren Sie die Funktionalität **Älteste Protokolldateien entfernen**.

   Wenn diese Funktionalität aktiviert ist, können Sie die maximale Größe und die Anzahl der Protokolldateien anpassen:

   a. Geben Sie die **Maximale Größe einer Protokolldatei (MB)** an.

      Verfügbare Werte: von 1 bis 4095 MB. Der Standardwert ist 100 MB.

   b. Geben Sie die **Maximale Anzahl der Dateien für ein Protokoll** an.

      Verfügbare Werte: von 1 bis 999. Der Standardwert ist 5.

9. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder konfigurieren Sie die Anwendungsnachverfolgung (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.

3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Diagnose von Störungen** aus.

5. Verwenden Sie im Block **Einstellungen für die Diagnose von Störungen** das Kontrollkästchen **Programm-Ablaufverfolgung aktivieren**, um die Programm-Ablaufverfolgung zu aktivieren oder zu deaktivieren.

   Die Ablaufverfolgung von Programmvorgängen ist standardmäßig deaktiviert.

6. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Geben Sie dazu im Feld **Ordner für Protokolle (vollständiger Ordnerpfad, z. B. C:\\Protokolle\\)** den vollständigen Pfad des lokalen Ordners an.

   > Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

   Für die Protokolldateien erstellt Kaspersky Embedded Systems Security im ausgewählten Ordner einen Unterordner namens logs-Kaspersky Embedded Systems Security-<uid>, wobei <uid> eine eindeutige Protokoll-ID aus 8 Zeichen ist.

7. Wählen Sie die Protokollierungsstufe für die Debug-Informationen aus:

   - **Normal** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie Informationen über den normalen Betrieb des Programms gespeichert (Standard).
   - **Kritisch** bedeutet: In der Ablaufverfolgungsdatei werden nur Meldungen über schwerwiegende Fehler gespeichert.
   - **Diagnose** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler sowie Warnungen gespeichert.
   - **Wichtig** bedeutet: In der Ablaufverfolgungsdatei werden Meldungen über alle Fehler, Warnungen sowie zusätzliche Informationen gespeichert.
   - **Detailliert** bedeutet: In der Ablaufverfolgungsdatei werden alle Informationen über den Betrieb des Programms gespeichert.

   Ein Mitarbeiter des technischen Supports bestimmt den Detailgrad, der zur Lösung möglicher Probleme erforderlich ist.

8. Um alte Protokolldateien zu löschen, aktivieren Sie die Funktionalität **Alte Protokolldateien löschen**.

   Wenn diese Funktionalität aktiviert ist, können Sie die maximale Größe und die Anzahl der Protokolldateien anpassen:

   a. Geben Sie die **Maximale Größe der Protokolldateien (MB)** an.

      Verfügbare Werte: von 1 bis 4095 MB. Der Standardwert ist 100 MB.

   b. Geben Sie die **Maximale Anzahl an Protokolldateien** an.

      Verfügbare Werte: von 1 bis 999. Der Standardwert ist 5.

9. Speichern Sie die vorgenommenen Änderungen.

Sie können die Ablaufverfolgung der Programmausführung auch in der kompakten Diagnoseoberfläche und über die Befehlszeile aktivieren und konfigurieren.

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 folgenden Ordner gespeichert: %ProgramData%\Kaspersky Lab\KESS.4.1\Traces.

Protokolldateien werden nach folgendem Muster benannt: KESS<4.1_DatumXX.XX_UhrzeitXX.XX_pidXXX.><Typ der Protokolldatei>.log.

Sie können die Daten einsehen, die in Protokolldateien aufgezeichnet wurden.

Alle Protokolldateien enthalten folgende allgemeinen Daten:

- Ereigniszeitpunkt
- Thread-Nummer
- 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.
- 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.

- 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
- Daten über den Netzwerkverkehr. Diese Daten werden in einer Ablaufverfolgungsdatei aufgezeichnet, wenn die Komponenten zur Überwachung des Datenverkehrs aktiviert sind.
- Daten, die von den Kaspersky-Servern stammen (z. B. Version der Antiviren-Datenbanken).
- Status der Komponenten von Kaspersky Embedded Systems 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 der Protokolldatei für die Komponente „AMSI-Scanner“

Die Protokolldatei AMSI.log enthält neben allgemeinen Daten auch Informationen über die Ergebnisse von Untersuchungen, die von Drittanbieter-Anwendungen angefordert wurden.

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 Protokolldateien des Programm-Web-Plug-ins werden nach folgendem Muster benannt: logs-ess_windows-<Typ der Protokolldatei>.DESKTOP-<Datum der Update-Datei>.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:

- KLAdmin-Benutzerkennwort zum Entsperren der Benutzeroberfläche von Kaspersky Embedded Systems Security.
- Temporäres Kennwort zum Entsperren der Benutzeroberfläche von Kaspersky Embedded Systems Security.
- Benutzername und Kennwort für den SMTP-Mail-Server.
- Benutzername und Kennwort für den Proxyserver.
- Benutzername und Kennwort für die Aufgabe *Auswahl der Programmkomponenten ändern*.
- Anmeldedaten und Pfade, die in den Richtlinieneigenschaften und in den Aufgaben von Kaspersky Embedded Systems Security angegeben sind.

Speicherabbilder aufzeichnen

Eine Speicherabbilddatei enthält alle Informationen über den Arbeitsspeicher der Prozesse von Kaspersky Embedded Systems Security zum Zeitpunkt eines Programmfehlers.

Speicherabbilddateien bleiben auf dem Gerät gespeichert, solange das Programm verwendet wird. Bei der Deinstallation des Programms werden sie dauerhaft gelöscht.

Gespeicherte Dump-Dateien können vertrauliche Daten enthalten. Sie müssen selbst für den Schutz der Speicherabbilddateien sorgen, um die Zugriffskontrolle auf diese Daten zu gewährleisten.

Standardmäßig werden Speicherauszugsdateien im folgenden Ordner gespeichert: %ProgramData%\Kaspersky Lab\KESS.4.1\Traces.

So aktivieren oder deaktivieren Sie die Aufzeichnung von Speicherabbildern (in der Kaspersky Security Center-Verwaltungskonsole)

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Diagnose von Störungen**.
4. Klicken Sie im Block **Einstellungen der Diagnose von Störungen** auf **Einstellungen**.

   Das Fenster **Einstellungen der Diagnose von Störungen** wird auf der Registerkarte **Einstellungen der Programm-Ablaufverfolgung** des Dateiintegritätsmonitors geöffnet.
5. Wählen Sie die Registerkarte **Einstellungen für Programm-Dumps** aus.

6. Verwenden Sie das Kontrollkästchen **Dump-Datei erstellen**, um die Ablaufverfolgung von Programmvorgängen zu aktivieren oder zu deaktivieren.

   Die Speicher-Dump-Aufzeichnung ist standardmäßig deaktiviert.

7. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Geben Sie dazu im Feld **Ordner für Dump-Dateien** den vollständigen Pfad des lokalen Ordners an.

   Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

8. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Aufzeichnung von Speicherabbildern (in der Anwendungskonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Eigenschaften des Programms**.
   - Wählen Sie im Kontextmenü des Knotens den Punkt **Eigenschaften des Programms** aus.

   Das Fenster **Eigenschaften des Programms** wird geöffnet.

2. Wählen Sie die Registerkarte **Diagnose von Störungen** aus.

3. Klicken Sie im Block **Einstellungen der Diagnose von Störungen** auf **Einstellungen**.

   Das Fenster **Einstellungen der Diagnose von Störungen** wird geöffnet.

4. Wählen Sie die Registerkarte mit den Einstellungen für Dump-Dateien aus:

   - **Einstellungen für Programm-Dumps**. Kaspersky Embedded Systems Security zeichnet alle Programm-Dumps auf.
   - **Einstellungen der Dumps für die Programmkonsole**. Wenn die Programmkonsole und Kaspersky Embedded Systems Security auf verschiedenen Computern installiert sind, können Sie Dumps nur für die Programmkonsole aufzeichnen.

5. Verwenden Sie das Kontrollkästchen **Dump-Datei erstellen**, um die Ablaufverfolgung von Programmvorgängen zu aktivieren oder zu deaktivieren.

   Die Speicher-Dump-Aufzeichnung ist standardmäßig deaktiviert.

6. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Klicken Sie dazu auf **Durchsuchen** und wählen Sie den gewünschten Ordner aus.

   Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren oder deaktivieren Sie die Aufzeichnung von Speicherabbildern (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 Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.
4. Wählen Sie den Abschnitt **Diagnose von Störungen** aus.
5. Verwenden Sie im Block **Einstellungen für Dump-Dateien** das Kontrollkästchen **Dump-Datei erstellen**, um die Programm-Ablaufverfolgung zu aktivieren oder zu deaktivieren.

   Die Speicher-Dump-Aufzeichnung ist standardmäßig deaktiviert.
6. Ändern Sie bei Bedarf den Standardordner, in dem Kaspersky Embedded Systems Security die Protokolldateien speichert. Geben Sie dazu im Feld **Ordner für Dump-Dateien (vollständiger Ordnerpfad, z. B. C:\\Dumps\\)** den vollständigen Pfad des lokalen Ordners an.

   > Der Ordner muss im Voraus erstellt werden und für das Benutzerkonto SYSTEM beschreibbar sein. Sie können keine Netzwerkordner, Laufwerke oder Umgebungsvariablen angeben.
7. Speichern Sie die vorgenommenen Änderungen.

Sie können die Aufzeichnung von Speicherabbildern auch im kompakten Diagnosefenster aktivieren oder deaktivieren

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 den Schutz für Dump-Dateien und Protokolldateien (in der Kaspersky Security Center Verwaltungskonsole)

1. Wählen Sie im „Web Console"-Hauptfenster den Punkt **Asset-Verwaltung** → **Richtlinien** aus.
2. Klicken Sie auf den Namen der Richtlinie von Kaspersky Embedded Systems Security.

   Das Fenster mit den Richtlinieneigenschaften wird geöffnet.
3. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

4. Wählen Sie den Abschnitt **Diagnose von Störungen** aus.

5. Verwenden Sie das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Schutz für Dump-Dateien und Protokolldateien zu aktivieren oder zu deaktivieren.

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. Gehen Sie im Fenster mit den Richtlinieneigenschaften zum Abschnitt **Diagnose von Störungen**.

4. Klicken Sie im Block **Einstellungen der Diagnose von Störungen** auf **Einstellungen**.

5. Das Fenster **Einstellungen der Diagnose von Störungen** wird geöffnet.

6. Verwenden Sie das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Schutz für Dump-Dateien und Protokolldateien zu aktivieren oder zu deaktivieren.

7. Speichern Sie die vorgenommenen Änderungen.

So aktivieren Sie den Schutz für Dump-Dateien und Ablaufverfolgungsdateien (in der Programmkonsole)

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Eigenschaften des Programms**.
   - Wählen Sie im Kontextmenü des Knotens den Punkt **Eigenschaften des Programms** aus.

   Das Fenster **Eigenschaften des Programms** wird geöffnet.

2. Wählen Sie die Registerkarte **Diagnose von Störungen** aus.

3. Klicken Sie im Block **Einstellungen der Diagnose von Störungen** auf **Einstellungen**.

   Das Fenster **Einstellungen der Diagnose von Störungen** wird geöffnet.

4. Verwenden Sie das Kontrollkästchen **Schutz für Dump-Dateien und Ablaufverfolgungsdateien aktivieren**, um den Schutz für Dump-Dateien und Protokolldateien zu aktivieren oder zu deaktivieren.

5. Speichern Sie die vorgenommenen Änderungen.

Sie können den Schutz für Dump-Dateien und Protokolldateien auch in der kompakten Diagnose-Benutzeroberfläche aktivieren oder deaktivieren.

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 Embedded Systems 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.

Informationsquellen über Kaspersky Embedded Systems Security

Für Kaspersky Embedded Systems Security stehen Ihnen folgende Informationsquellen zur Verfügung:

- Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky
- Seite von Kaspersky Embedded Systems Security auf der Webseite des Technischen Supports (Wissensdatenbank)
- Online-Hilfe
- In unserem Forum über das Programm diskutieren

Für die Nutzung der Informationsquellen auf den Webseiten ist ein Internetzugang notwendig.

Die Online-Hilfe kann möglicherweise nicht in einem Browser angezeigt werden, der moderne Verschlüsselungsprotokolle nicht unterstützt.

Sollten Sie ein aufgetretenes Problem nicht selbst lösen können, wenden Sie sich bitte an den Technischen Support von Kaspersky.

Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky

Auf der Seite von Kaspersky Embedded Systems Security stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

Die Seite Kaspersky Embedded Systems Security enthält einen Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite von Kaspersky Embedded Systems Security in der Wissensdatenbank

Die Wissensdatenbank ist ein spezieller Bereich auf der Website des Technischen Supports.

Auf der Seite von Kaspersky Embedded Systems Security in der Wissensdatenbank finden Sie Artikel mit nützlichen Informationen und Tipps sowie FAQs zum Kauf, zur Installation und zur Nutzung des Programms.

Artikel der Wissensdatenbank beantworten Fragen nicht nur in Bezug auf Kaspersky Embedded Systems Security, sondern auch auf andere Programme von Kaspersky. Außerdem können Artikel der Wissensdatenbank auch Neuigkeiten über den Technischen Support enthalten.

Hilfe zu Kaspersky Embedded Systems Security

Die Online-Hilfe enthält Informationen zur Konfiguration und Verwendung von Kaspersky Embedded Systems Security.

In unserem Forum über das Programm diskutieren

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.

Anhänge

Die Informationen in diesem Abschnitt ergänzen den allgemeinen Text des Dokuments.

Dateierweiterungen für die schnelle Untersuchung

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

Benutzerkonten in Regeln für App-Komponenten

Zum Konfigurieren einiger Programmkomponenten müssen Sie spezielle Regeln hinzufügen, mit denen Sie die Benutzer auswählen können, für die das Programm die Regel anwenden soll.

Regeln müssen hinzugefügt werden, um die folgenden App-Komponenten zu konfigurieren:

- Kontrolle des Programmstarts
- Gerätekontrolle
- Verhaltensanalyse
- Überwachung der Systemintegrität

Sie können Benutzer auf folgende Weise hinzufügen:

- Aus Active Directory auswählen (empfohlen)
- Aus der Benutzerliste von Kaspersky Security Center auswählen
- Manuell hinzufügen

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 zählt insbesondere die Verantwortung für die Kontrolle und Beschränkung des Zugriffs auf die Programmeinstellungen.

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.

Kaspersky Embedded Systems Security unterstützt eingebettete Benutzer- und Gruppenkonten (z. B. die Gruppe „Alle“) in den Regeln. Aufgrund von Besonderheiten bei der Erkennung von Benutzer-SIDs erlaubt das Programm nur die Verwendung eingebetteter Benutzerkonten, die aus Active Directory oder aus der Benutzerliste von Kaspersky Security Center hinzugefügt wurden. Regeln, bei denen das eingebettete Benutzerkonto manuell hinzugefügt wird, funktionieren nicht.

Rechtliche Informationen

Bereitstellung von Daten

Dieser Abschnitt enthält Informationen über die Daten, die Kaspersky Embedded Systems Security während des Betriebs auf dem Gerät speichern und 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

Im Endbenutzer-Lizenzvertrag für Kaspersky Embedded Systems Security 3, insbesondere im Abschnitt "Bedingungen für die Datenverarbeitung", sind die Bedingungen, die Haftung und das Verfahren für die Übermittlung und Verarbeitung der in diesem Handbuch angegebenen Daten festgelegt. Bevor Sie den Endbenutzer-Lizenzvertrag akzeptieren, lesen Sie die Bedingungen sowie alle Dokumente, die mit dem Endbenutzer-Lizenzvertrag verknüpft sind, sorgfältig.

Die Daten, die Kaspersky von Ihnen erhält, wenn Sie die Anwendung verwenden, sind geschützt und werden gemäß der Datenschutzrichtlinie verarbeitet, die Sie unter www.kaspersky.com/Products-and-Services-Privacy-Policy abrufen können.

Die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie stehen während der Installation von Kaspersky Embedded Systems Security im Lieferumfang und über das Menü **Start** (**Alle Programme** > **Kaspersky Embedded Systems Security** > **EULA und Datenschutzrichtlinie**) zur Verfügung.

Bei der Deinstallation von Kaspersky Embedded Systems Security werden alle Daten gelöscht, die von Kaspersky Embedded Systems Security auf dem geschützten Gerät gespeichert wurden.

Indem Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren, erklären Sie sich damit einverstanden, die folgenden Daten automatisch an Kaspersky zu senden:

- Um den Mechanismus für den Empfang von Updates zu unterstützen - Informationen über das installierte Programm und seine Aktivierung: Identifikator des zu installierenden Programms und dessen Vollversion, einschließlich Versionsnummer, Typ und Lizenz-ID, Installations-Identifikator, ID der Update-Aufgabe.

- Um die Möglichkeit zu nutzen, zu Wissensdatenbankartikeln zu navigieren, wenn Programmfehler auftreten (Redirectordienst): Informationen über das Programm und den Verknüpfungstyp: Name, Gebietsschema und vollständige Versionsnummer des Programms, Typ des Umleitungslinks und Fehler-ID.

- Zur Verwaltung von Bestätigungen für die Datenverarbeitung: Informationen über den Status der Annahme von Endbenutzer-Lizenzverträgen und anderer Dokumente, die die Bedingungen für die Datenübermittlung festlegen: ID und Version des Lizenzvertrags oder eines anderen Dokuments, als Teil dessen die Bedingungen für die Datenverarbeitung akzeptiert oder abgelehnt werden; ein Attribut, das die Handlung des Benutzers (Bestätigung oder Rückruf der Akzeptanz der Bedingungen) kennzeichnet; Datum und Uhrzeit der Statusänderungen der Annahme der Bedingungen für die Datenverarbeitung.

Lokale Datenverarbeitung

Während der Ausführung der Hauptfunktionen des Programms, die in diesem Handbuch beschrieben werden, verarbeitet und speichert Kaspersky Embedded Systems Security lokal eine Reihe von Daten auf dem geschützten Gerät.

Die Tabelle unten enthält Informationen zur lokalen Verarbeitung und Speicherung von Daten in Berichten durch Kaspersky Embedded Systems Security.

Verarbeitung und Speicherung von Daten in Berichten

Funktionsbereich	Registrierung von Ereignissen
Nutzungsart	Kaspersky Embedded Systems Security speichert Daten lokal und sendet diese Daten an den Administrationsserver. Die Datenbank des Administrationsservers speichert Informationen zu Programmereignissen, die bei verwalteten geschützten Geräten auftreten.
Speicher	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<product version>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Datenbank des Administrationsservers
Sicherheitsmaßnahmen	Liste der Zugriffskontrolle
Aufbewahrungsdauer	Kaspersky Embedded Systems Security speichert die Daten, bis Kaspersky Embedded Systems Security deinstalliert wird. Bei der Deinstallation von Kaspersky Embedded Systems Security werden alle Daten gelöscht, die von Kaspersky Embedded Systems Security auf dem geschützten Gerät gespeichert wurden.
Ziel	Bereitstellen der Hauptfunktionen.

Kaspersky Embedded Systems Security löscht keine Ereignisse im Windows-Ereignisprotokoll, auch nicht die Ereignisse, die bei der Deinstallation von Kaspersky Embedded Systems Security auftreten.

Um die Funktion der Ereignisregistrierung zu gewährleisten, verarbeitet Kaspersky Embedded Systems Security lokal die folgenden Daten:

- Namen, Prüfsummen (MD5, SHA-256) und Attribute der verarbeiteten Dateien sowie die vollständigen Pfade auf den untersuchten Medien zu diesen Dateien.

- Aktionen an den von Kaspersky Embedded Systems Security untersuchten Dateien.

- Benutzeraktionen, die für gescannte Dateien auf dem geschützten Gerät durchgeführt wurden.
- Informationen zu Konten von Benutzern, die Aktionen am geschützten Netzwerk bzw. Gerät vornehmen.
- Werte des Geräteinstanzpfads für Geräte, die den Regeln für die Gerätekontrolle hinzugefügt wurden.
- Informationen zu Prozessen und Skripten, die auf dem System ausgeführt werden: Prüfsummen (MD5, SHA-256) und vollständige Pfade zu ausführbaren Dateien, Informationen zu digitalen Zertifikaten.
- Windows Firewall-Einstellungen.
- Windows-Ereignisprotokolleinträge.
- Namen von Benutzerkonten, die Aktionen für gescannte Dateien auf dem geschützten Gerät durchführen.
- Exemplarklasse der gestarteten ausführbaren Dateien und die Typen, Namen, Prüfsummen und Attribute dieser Dateien.
- Informationen zur Netzwerkaktivität:
  - Die IP-Adressen der blockierten externen Geräte.
  - Verarbeitete IP-Adressen.
- Informationen zum Status des Windows USN-Protokolls.

Die folgende Tabelle enthält Informationen zu Dienstdaten die von Kaspersky Embedded Systems Security verarbeitet wurden. Die Dienstdaten umfassen: Programmparameter, Quarantäne- und Backup-Dateien, Informationen in den Dienstdatenbanken des Programms, Lizenzdaten.

Die Tabelle unten enthält Informationen zur lokalen Verarbeitung und Speicherung von benutzerdefinierten Parameterdaten durch Kaspersky Embedded Systems Security.

Verarbeitung und Speicherung von benutzerdefinierten Parameterdaten

Funktionsbereich	Alle Funktionen von Kaspersky Embedded Systems Security
Nutzungsart	Kaspersky Embedded Systems Security speichert Daten lokal und sendet diese Daten an den Administrationsserver. Die Daten sind in der Datenbank des Administrationsservers gespeichert. Die vom Programm lokal verarbeiteten Daten werden nicht automatisch an Kaspersky oder sonstige Drittthersteller-Systeme gesendet.
Speicher	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<product version>\ • Datenbank des Administrationsservers
Sicherheitsmaßnahmen	Liste der Zugriffskontrolle
Verarbeitungszeitraum	Kaspersky Embedded Systems Security speichert die Daten, bis Kaspersky Embedded Systems Security deinstalliert wird. Bei der Deinstallation von Kaspersky Embedded Systems Security werden alle Daten gelöscht, die von Kaspersky Embedded Systems Security auf dem geschützten Gerät gespeichert wurden. Kaspersky Embedded Systems Security löscht keine Daten zu Parametern, die in die Konfigurationsdatei exportiert wurden. Kaspersky Embedded Systems Security löscht keine Quarantäne- oder Backup-Objekte, wenn die Kontrollkästchen **Quarantäne-Objekte exportieren** und **Backup-Objekte exportieren** im Installationsassistenten aktiviert wurden.
Ziel	Bereitstellen der Hauptfunktionen.

Für die genannten Zwecke verarbeitet Kaspersky Embedded Systems Security lokal folgende Daten:

- Quarantäne- oder Backup-Objekte.
- Informationen über Benutzerkonten (Benutzernamen und Kennwörter), unter denen Kaspersky Embedded Systems Security Aufgaben ausführt.
- Kennwort für Kaspersky Embedded Systems Security.
- IP-Adressen und IDs von blockierten Anmeldesitzungen.
- Einstellungen für Windows Firewall und Windows Firewall-Regeln.
- Prüfsummen (MD5, SHA-256) und Pfade der ausführbaren Dateien, die den Regeln zur Kontrolle des Programmstarts hinzugefügt wurden.
- Werte des Geräteinstanzpfads für Geräte, die den Regeln für die Gerätekontrolle hinzugefügt wurden.
- Informationen zu Dateien und Ordnern in den Aufgabenbereichen für Kaspersky Embedded Systems Security.
- IP-Adressen im oder außerhalb des Schutzbereichs.
- Informationen zu Ereignissen im Windows-Ereignisprotokoll.
- Informationen zu Funden, die mit der iSwift- oder iChecker-Technologie erkannt wurden.
- Prüfsummen (MD5, SHA-256), vollständige Pfade und Masken, die in Ausnahmeeinstellungen definiert wurden.
- Informationen zu Prozessen, die der vertrauenswürdigen Zone hinzugefügt wurden.
- Informationen zu hinzugefügten Lizenzschlüsseln.
- Informationen zu digitalen Zertifikaten.
- Nicht entpackte Dateien aus einem Archiv oder andere zusammengesetzte Objekte während der Untersuchung.

Kaspersky Embedded Systems Security verarbeitet und speichert Daten als Teil der Grundfunktionalität des Programms, einschließlich der Protokollierung von Programmereignissen und des Empfangs von Diagnosedaten. Lokal verarbeitete Daten werden entsprechend den konfigurierten und angewandten Programmeinstellungen geschützt.

In Kaspersky Embedded Systems Security können Sie die Schutzstufe für lokal verarbeitete Daten konfigurieren. Sie können die Benutzerrechte für den Zugriff auf verarbeitete Daten ändern, die Datenaufbewahrungszeiträume für diese Daten ändern, Funktionen, die die Datenprotokollierung beinhalten, ganz oder teilweise deaktivieren und den Pfad und die Attribute des Ordners auf dem Laufwerk ändern, in dem die Daten protokolliert werden.

Die vom Programm lokal verarbeiteten Daten werden nicht automatisch an Kaspersky oder sonstige Drittherstellersysteme gesendet.

Wenn Kaspersky Embedded Systems Security vom geschützten Gerät deinstalliert wird, werden standardmäßig alle Daten, die das Programm während des Betriebs lokal verarbeitet hat, entfernt.

Eine Ausnahme bilden Dateien mit Diagnoseinformationen (Protokoll- und Dump-Dateien), Programmereignisse im Windows-Ereignisprotokoll und Dateien mit exportierten Einstellungen von Kaspersky Embedded Systems Security. Es wird empfohlen, diese Dateien manuell zu löschen.

Lesen Sie detaillierte Informationen über die Arbeit mit Dateien, die Diagnosedaten des Programms enthalten, in den entsprechenden Abschnitten dieses Handbuchs.

Sie können die Windows-Ereignisprotokolldateien, die die Ereignisse des Programms Kaspersky Embedded Systems Security enthalten, mithilfe der Standardtools des Betriebssystems löschen.

Lokale Datenverarbeitung mithilfe von Hilfskomponenten des Programms

Das Installationspaket von Kaspersky Embedded Systems Security enthält Hilfskomponenten des Programms, die auf Ihrem Gerät installiert werden können. Dies ist auch dann möglich, wenn Kaspersky Embedded Systems Security nicht installiert ist. Zu diesen Hilfskomponenten zählen folgende:

- Die Programmkonsole. Die Komponente ist ein Snap-in der Microsoft-Management-Konsole.
- Das Verwaltungs-Plug-in Diese Komponente bietet eine vollständige Integration in Kaspersky Security Center.

Bei der Ausführung der in diesem Handbuch beschriebenen Hauptfunktionen des Programms wird von den Hilfskomponenten des Programms ein Satz von Daten auf dem geschützten Gerät verarbeitet und gespeichert, d. h. dort, wo die Daten installiert sind, auch wenn die Hilfskomponenten nachträglich zu Kaspersky Embedded Systems Security installiert werden.

Von den Programmkomponenten werden die folgenden Daten lokal verarbeitet und gespeichert:

- Programmkonsole: Name des geschützten Geräts, auf dem Kaspersky Embedded Systems Security installiert ist (IP-Adresse oder Domänenname), zu dem die Anwendungskonsole zuletzt eine Remote-Verbindung hergestellt hat; Anzeigeparameter, die in der Snap-In Microsoft Management Console konfiguriert wurden; Daten über den letzten Ordner, in dem der Benutzer Objekte über die Anwendungskonsole ausgewählt hat (über ein Systemdialogfeld, das durch Klicken auf die Schaltfläche **Durchsuchen** geöffnet wird. Die Protokolldateien der Anwendungskonsole können auch folgende Daten enthalten: den Namen des geschützten Geräts, auf dem Kaspersky Embedded Systems Security installiert ist und zu dem die Remote-Verbindung hergestellt wurde, den Namen des Benutzerkontos, unter dem die Remote-Verbindung hergestellt wurde.
- Das Administrations-Plug-in kann Daten verarbeiten und temporär speichern, die von Kaspersky Embedded Systems Security verarbeitet werden, z. B. konfigurierte Einstellungen von Programmaufgaben und -komponenten, Einstellungen von Kaspersky Security Center-Richtlinien, in Netzwerklisten gesendete Daten.

Die Tabelle unten enthält Informationen zu von Kaspersky Embedded Systems Security lokal verarbeiteten und gespeicherten Daten in Dump- und Protokolldateien.

Kaspersky Embedded Systems Security verarbeitet und speichert lokal die folgenden Dump- und Protokolldateien:

- Informationen zu Aktionen auf dem geschützten Gerät durch Kaspersky Embedded Systems Security.
- Informationen zu Objekten, die von Kaspersky Embedded Systems Security verarbeitet wurden.
- Informationen über Aktivitäten auf dem geschützten Gerät, die von Kaspersky Embedded Systems Security verarbeitet werden.
- Informationen zu Fehlern, die während der Ausführung von Kaspersky Embedded Systems Security aufgetreten sind.

Die von den Hilfskomponenten verarbeiteten Daten werden nicht automatisch an Kaspersky oder sonstige Dritthersteller-Systeme gesendet.

Standardmäßig werden alle hierbei lokal von den Hilfskomponenten des Programms verarbeiteten Daten nach dem Entfernen dieser Komponenten gelöscht.

Eine Ausnahme bilden Protokolldateien von Hilfskomponenten des Programms. Es wird empfohlen, diese Dateien manuell zu löschen.

Daten in Protokoll- und Dump-Dateien

Kaspersky Embedded Systems Security kann gemäß den Einstellungen Debug-Informationen in Protokolldateien für den technischen Support schreiben, während Kaspersky Embedded Systems Security ausgeführt wird.

Dump-Dateien für Kaspersky Embedded Systems Security werden vom Betriebssystem bei Programmabstürzen erstellt und beim nächsten Absturz überschrieben.

Protokoll- und Dump-Dateien können persönliche Daten des Benutzers oder vertrauliche Daten Ihres Unternehmens enthalten.

Verwenden Sie Kaspersky Embedded Systems Security nicht auf Geräten, für die eine Datenübertragung durch die Richtlinien Ihres Unternehmens verboten ist.

Kaspersky Embedded Systems Security zeichnet standardmäßig keine Debug-Informationen auf.

Protokoll- und Dump-Dateien werden nicht automatisch weiter als bis auf den Host übertragen, auf dem sie generiert wurden. Der Inhalt von Protokolldateien kann mit Standardanzeigeprogrammen für Textdateien angezeigt werden. Protokoll- und Dump-Dateien werden auf unbestimmte Zeit aufbewahrt und werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht.

Debug-Informationen können für den technischen Support von Nutzen sein.

Es werden keine speziellen Verfahren bereitgestellt, um den Zugriff auf Protokoll- und Dump-Dateien einzuschränken. Der Administrator kann das Programm so anpassen, dass Daten in einen geschützten Ordner geschrieben werden.

Der Pfad zum Protokoll- und Dump-Dateiordner wird nicht standardmäßig konfiguriert. Der Administrator muss den Pfad angeben, damit der Protokoll- und Dump-Ordner verwendet werden kann.

Daten in Protokoll- und Dump-Dateien können Folgendes enthalten:

- Informationen zu Aktionen auf dem geschützten Gerät durch Kaspersky Embedded Systems Security.
- Informationen zu Objekten, die von Kaspersky Endpoint Agent verarbeitet wurden.
- Fehler bei der Ausführung von Kaspersky Endpoint Agent.

Datenbereitstellung bei der Verwendung von Kaspersky Security Network

Der Datensatz, den Kaspersky Embedded Systems 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.

Einhaltung der Gesetzgebung der Europäischen Union (DSGVO)

Kaspersky Embedded Systems 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
- Verwendung von Links in der Anwendungskonsole

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.

Bitte lesen Sie vor der Verwendung von Kaspersky Embedded Systems Security aufmerksam die Beschreibung der übertragenen Daten. Diese Informationen finden Sie im Endbenutzer-Lizenzvertrag und in der Erklärung zu Kaspersky Security Network (Liste in der Erklärung zu Kaspersky Security Network). Wenn bestimmte Daten, die von Kaspersky Embedded Systems 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.

Aktivieren des Programms mit einem Aktivierungscode

Wenn Sie einen Aktivierungscode verwenden, 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 Embedded Systems Security eine Schlüsseldatei verwendet werden.

Aktualisierung von Programm-Modulen und Antiviren-Datenbanken

Wenn Sie die Kaspersky-Server verwenden, 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 Embedded Systems Security rechtmäßig verwendet wird. Wenn Sie nicht damit einverstanden sind, diese Informationen an Kaspersky weiterzugeben, verwenden Sie das Kaspersky Security Center für Datenbanken-Updates.

Verwendung von Links in der Anwendungskonsole

Wenn Sie Links in der Anwendungskonsole verwenden, erklären Sie sich damit einverstanden, die im Endbenutzer-Lizenzvertrag aufgeführten Daten automatisch zur Verfügung zu stellen. Die genaue Liste der Daten, die bei Verwendung eines spezifischen Links übertragen werden, hängt davon ab, wo sich der Link in der Anwendungskonsole befindet und welches Problem damit gelöst werden soll. Wenn Sie nicht damit einverstanden sind, dass Kaspersky diese Informationen zur Verfügung stellt, deaktivieren Sie die Anzeige der Programmoberfläche.

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.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Apache ist ein eingetragenes Markenzeichen oder ein Markenzeichen der Apache Software Foundation in den USA und/oder anderen Ländern.

Citrix, XenApp und XenDesktop sind eingetragene Markenzeichen oder Markenzeichen der Cloud Software Group, Inc. und/oder ihrer Tochterunternehmen in den USA und/oder anderen Ländern.

CVE ist ein eingetragenes Markenzeichen von The MITRE Corporation.

Dell Technologies, Dell, Dell Compellent und andere Markenzeichen sind Markenzeichen von Dell Inc. oder deren Tochterunternehmen.

EMC, Celerra, Isilon, OneFS und VNX sind eingetragene Markenzeichen oder Markenzeichen der EMC Corporation in den USA und/oder anderen Ländern.

Hitachi ist ein Markenzeichen von Hitachi, Ltd.

Linux ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Linus Torvalds.

Microsoft, Active Directory, Internet Explorer, Excel, Hyper-V, JScript, MultiPoint, Outlook, PowerShell, Windows, Windows Server und Windows Vista sind Markenzeichen der Microsoft-Unternehmensgruppe.

NetApp und Data ONTAP sind Markenzeichen oder eingetragene Markenzeichen von NetApp, Inc. in den USA und/oder anderen Ländern.

Oracle ist ein eingetragenes Markenzeichen von Oracle und/oder der verbundenen Unternehmen.

UNIX ist ein in den USA und in anderen Ländern eingetragenes Markenzeichen, das ausschließlich durch die X/Open Company Limited lizenziert wird.