KASPERSKY lab

Kaspersky Embedded Systems Security

Administratorhandbuch

Programmversion: 2.3.0.754

Sehr geehrter Benutzer!

Vielen Dank, dass Sie sich für Kaspersky Lab als Anbieter von Sicherheitssoftware entschieden haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein kann.

Redaktionsdatum des Dokuments: 26.04.2019

https://www.kaspersky.de
https://support.kaspersky.com/de

Inhalt

Über dieses Handbuch

Das Administratorhandbuch für Kaspersky Embedded Systems Security 2.3 (im Weiteren "Kaspersky Embedded Systems Security", "das Programm") richtet sich an die Experten, die für die Installation und die Verwaltung von Kaspersky Embedded Systems Security auf allen geschützten Geräten zuständig sind, sowie an die Experten für den technischen Support der Unternehmen, die Kaspersky Embedded Systems Security verwenden.

Dieses Handbuch enthält Informationen über die Konfiguration und Verwendung von Kaspersky Embedded Systems Security.

Außerdem finden Sie hier Hinweise auf Informationsquellen zum Programm und auf Möglichkeiten für den Technischen Support.

In diesem Kapitel

In diesem Dokument

Das Administratorhandbuch für Kaspersky Embedded Systems Security enthält folgende Abschnitte.

Informationsquellen über Kaspersky Embedded Systems Security

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

Kaspersky Embedded Systems Security

Dieser Abschnitt beschreibt Funktionen, Komponenten und Lieferumfang von Kaspersky Embedded Systems Security sowie die Hard- und Software-Voraussetzungen für Kaspersky Embedded Systems Security.

Programm installieren und deinstallieren

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

Programmoberfläche

Dieser Abschnitt enthält Informationen zu den Elementen der Programmoberfläche von Kaspersky Embedded Systems Security.

Lizenzverwaltung für das Programm

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für das Programm zusammenhängen.

Starten und Beenden von Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen über das Verwaltungs-Plug-in von Kaspersky Embedded Systems Security (im Weiteren "Verwaltungs-Plug").

Über Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen über die Rechte zur Verwaltung von Kaspersky Embedded Systems Security und der Windows®-Dienste, die das Programm registriert, sowie eine Anleitung zur Konfiguration dieser Rechte.

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 Computern.

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.

Programmeinstellungen verwalten

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

Echtzeit-Computerschutz

Dieser Abschnitt enthält Informationen über die Komponenten für den Echtzeit-Computerschutz: "Echtzeitschutz für Dateien", "Verwendung von KSN" und "Exploit-Prävention". Er bietet außerdem eine Anleitung zum Konfigurieren von Aufgaben für den Echtzeit-Computerschutz und zum Verwalten der Sicherheitseinstellungen eines geschützten Computers.

Überwachung der Desktop-Aktivitäten

Dieser Abschnitt enthält Informationen über die Funktionalität von Kaspersky Embedded Systems Security zur Kontrolle von Programmstarts und Verbindungen externer Geräte über USB.

Netzwerküberwachung

Dieser Abschnitt informiert über die Aufgabe zur Firewall-Verwaltung.

System-Diagnose

Dieser Abschnitt enthält Informationen über die Aufgabe "Überwachung der Datei-Integrität" sowie über Funktionen zur Analyse des Betriebssystemprotokolls.

Integration mit Drittherstellern-Systemen

Dieser Abschnitt beschreibt die Integration von Kaspersky Embedded Systems Security mit Funktionen und Technologien von Drittherstellern.

Arbeiten mit Kaspersky Embedded Systems Security aus der Befehlszeile

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Embedded Systems Security aus der Befehlszeile.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Informationen darüber, wie und zu welchen Bedingungen Sie technischen Support erhalten.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen von Begriffen, die in diesem Dokument vorkommen.

AO Kaspersky Lab

Dieser Abschnitt bietet Informationen über AO Kaspersky Lab.

Informationen über den Code von Drittherstellern

Dieser Abschnitt enthält Informationen über den Code von Drittherstellern, der im Programm verwendet wird.

Markenrechtliche Hinweise

In diesem Abschnitt werden die Marken von Drittanbietern (Rechteinhabern) genannt.

Sachregister

Dieser Abschnitt ermöglicht das schnelle Auffinden bestimmter Angaben im Dokument.

Formatierung mit besonderer Bedeutung

In diesem Dokument werden Formatierungen mit besonderer Bedeutung verwendet (s. Tabelle unten).

Tabelle 1. Formatierung mit besonderer Bedeutung

Textbeispiel	Beschreibung der Formatierung
Beachten Sie, dass...	Warnungen sind rot hervorgehoben und eingerahmt. Warnungen informieren über Aktionen, die unerwünschte Folgen haben können.
Es wird empfohlen...	Hinweise sind eingerahmt. Hinweise enthalten zusätzliche und hilfreiche Informationen.
Beispiel: …	Beispiele befinden sich in blau unterlegten Blöcken und sind mit "Beispiel" überschrieben.
Update bedeutet... Das Ereignis *Die Datenbanken sind veraltet* tritt ein.	Folgende Textelemente sind *kursiv* hervorgehoben: • neue Begriffe • Namen von Statusvarianten und Programmereignissen
Drücken Sie die Taste **EINGABE**. Drücken Sie die Tastenkombination **ALT**+**F4**.	Bezeichnungen von Tasten sind **fett** und in Großbuchstaben geschrieben. Tastenbezeichnungen, die durch ein Pluszeichen verbunden sind, bedeuten eine Tastenkombination. Die genannten Tasten müssen gleichzeitig gedrückt werden.

Textbeispiel	Beschreibung der Formatierung
Klicken Sie auf die Schaltfläche "**Aktivieren**".	Die Namen von Elementen der Programmoberfläche sind **fett** geschrieben (z. B. Eingabefelder, Menüpunkte, Schaltflächen).
► *Um den Aufgabenzeitplan anzupassen, gehen Sie wie folgt vor:*	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch ein Pfeilsymbol markiert.
Geben Sie in der Befehlszeile den Text `help` ein. Es erscheint folgende Meldung: Geben Sie das Datum im Format `TT:MM:JJ` an.	Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben: • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt. • Daten, die über die Tastatur eingegeben werden müssen.
<Benutzername>	Variable stehen in eckigen Klammern. Der Name der Variablen muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

Informationsquellen über Kaspersky Embedded Systems Security

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

In diesem Kapitel

Quellen für die selbstständige Informationssuche

Für Kaspersky Embedded Systems Security stehen Ihnen folgende Informationsquellen zur Verfügung:

- Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky Lab
- Seite von Kaspersky Embedded Systems Security auf der Webseite des Technischen Supports (Wissensdatenbank)
- Dokumentation

Sollten Sie ein aufgetretenes Problem nicht selbst lösen können, wenden Sie sich bitte an den Technischen Support von Kaspersky Lab https://support.kaspersky.com/.

Für die Nutzung der Informationsquellen auf den Webseiten ist ein Internetzugang notwendig.

Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky Lab

Auf der von Kaspersky Embedded Systems Security https://www.kaspersky.de/enterprise-security/embedded-systems stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

Auf der Seite für Kaspersky Embedded Systems Security befindet sich ein 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 http://support.kaspersky.com/de/kess2 finden Sie Artikel, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Erwerb, zur Installation und zur Anwendung des Programms enthalten.

Artikel der Wissensdatenbank beantworten Fragen nicht nur in Bezug auf Kaspersky Embedded Systems Security, sondern auch auf andere Programme von Kaspersky Lab. Außerdem können Artikel der Wissensdatenbank auch Neuigkeiten über den Technischen Support enthalten.

Dokumentation für Kaspersky Embedded Systems Security

Das Administratorhandbuch von Kaspersky Embedded Systems Security enthält Informationen über die Installation, Deinstallation, Konfiguration und Nutzung des Programms.

Diskussion über die Programme von Kaspersky Lab in der Community

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserer Community https://community.kaspersky.com/ diskutieren.

In dieser Community können Sie sich zu bestehenden Themen informieren, Ihre Meinung mitteilen und neue Diskussionsthemen erstellen.

Kaspersky Embedded Systems Security

Dieser Abschnitt beschreibt Funktionen, Komponenten und Lieferumfang von Kaspersky Embedded Systems Security sowie die Hard- und Software-Voraussetzungen für Kaspersky Embedded Systems Security.

In diesem Kapitel

Über Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security schützt Computer und sonstige eingebettete Systeme unter Microsoft® Windows gegen Viren und andere Bedrohungen. Als Benutzer von Kaspersky Embedded Systems Security gelten Netzwerkadministratoren des Unternehmens und Mitarbeiter, die für den Antiviren-Schutz des Unternehmensnetzwerks zuständig sind.

Sie können Kaspersky Embedded Systems Security auf einer Vielzahl eingebetteter Systeme unter Windows installieren, einschließlich der folgenden Gerätetypen:

- Geldautomaten
- Verkaufsorte

Kaspersky Embedded Systems Security kann auf folgende Arten verwaltet werden:

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

Sie können das Programm Kaspersky Security Center verwenden, das der zentralisierten Verwaltung des Schutzes mehrerer Computer dient, auf denen jeweils eine Exemplar von Kaspersky Embedded Systems Security installiert ist.

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**. 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)
  - MBRs 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. Das Programm prüft die Dateien, den Arbeitsspeicher sowie die Autostart-Objekte des geschützten Computers.
- **Kontrolle des Programmstarts**. Diese Komponente überwacht die Versuche der Benutzer, das Programm zu starten, und regelt den Programmstart auf einem geschützten Computer.
- **Gerätekontrolle**. Diese Komponente ermögliche eine Kontrolle der Registrierung und der Verwendung von Massenspeichergeräten und CD-/DVD-Geräten, um den Computer vor Bedrohungen zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können.
- **Firewall-Verwaltung**. Diese Komponente ermöglicht die Verwaltung der Windows Firewall: Sie erlaubt die Anpassung der Einstellungen und Regeln der Firewall des Betriebssystems und sperrt sämtliche Möglichkeiten zur externen Konfiguration der Firewall.
- **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 Computers 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 der Programm-Datenbanken" und "Update der Programm-Module"**. Für den Download von Updates der Programm-Datenbanken und Programm-Module verwendet Kaspersky Embedded Systems Security die FTP- oder HTTP-Kaspersky Lab Update-Server, den Administrationsserver von Kaspersky Security Center 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 Objekte desinfiziert oder gelöscht werden, speichert Kaspersky Embedded Systems Security verschlüsselte Kopien der als *Infiziert* eingestuften Objekte im *Backup*.
- **Benachrichtigungen an den Administrator und die Benutzer**. Sie können die Benachrichtigung des Administrators und der Benutzer, die auf den geschützten Computer zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Embedded Systems Security und dem Status des Antiviren-Schutzes auf dem Computer zusammenhängen, anpassen.
- **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 Computers manuell konfigurieren und die Werte der angepassten Einstellungen in einer Vorlage speichern. Sie können diese Vorlage später bei der Konfiguration 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.
- **Schreiben von Ereignissen in das Ereignisprotokoll des Programms**. 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 Echtzeitschutz anwenden wird.
- **Exploit-Prävention**. Sie können den Prozess-Speicher mithilfe des in die Prozesse eingebetteten Schutz-Agenten vor Exploits schützen.

Neuerungen

Kaspersky Embedded Systems Security bietet folgende Neuerungen und Verbesserungen:

- Unterstützung von neuen Versionen von Microsoft Windows-Betriebssystemen.

  Windows 10 Redstone 6 (x32 und x64).
- Der vollständige Aktivierungscode kann nicht auf der Programmoberfläche dargestellt werden.

  Der bereits eingefügte Aktivierungscode wird auf der Programmoberfläche nicht vollständig dargestellt und kann auch von keinem Benutzer vollständig angezeigt werden.

Lieferumfang

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

- Installationsassistent für Kaspersky Embedded Systems Security starten
- Installationsassistent für die Konsole für Kaspersky Embedded Systems Security starten.
- Starten Sie den Installationsassistent für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security, um das Programm über Kaspersky Security Center zu verwalten.
- Lesen Sie das Administratorhandbuch.
- Wechseln Sie zur Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky Lab.
- Website des Technischen Supports (https://support.kaspersky.com/de) aufrufen.
- Informationen über die aktuelle Version von Kaspersky Embedded Systems Security lesen

Der Ordner "\console" enthält Dateien für die Installation der Programmkonsole (Komponentengruppe "Administrations-Tools von Kaspersky Embedded Systems Security").

Der Ordner "\product" enthält Folgendes:

- Dateien für die Installation der Serverkomponenten von Kaspersky Embedded Systems Security auf einem Computer, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows läuft.
- Installationsdatei für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security über das Kaspersky Security Center.
- Archivdatei der zum Zeitpunkt der Veröffentlichung des Programms aktuellen Antiviren-Datenbanken
- Datei mit dem Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.

Der Ordner "\product_no_avbases" enthält Installationsdateien für die Komponenten von Kaspersky Embedded Systems Security und das Verwaltungs-Plug-in ohne Antiviren-Datenbanken.

Der Ordner \setup enthält Dateien, die für den Start des Begrüßungsprogramms erforderlich sind.

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

Tabelle 2. Dateien im Lieferumfang von Kaspersky Embedded Systems Security

Datei	Ziel
autorun.inf	Autostart-Datei des Installationsassistenten von Kaspersky Embedded Systems Security bei der Programminstallation von Wechseldatenträgern
ess_admin_guide_de.pdf	Administratorhandbuch.
release_notes.txt	Datei enthält Ausgabedaten.
setup.exe	Startdatei des Begrüßungsprogramms (startet setup.hta).
\console\esstools_x86(x64).msi	Paket des Dienstes Windows Installer; installiert die Programmkonsole auf dem geschützten Computer.
\console\setup.exe	Startdatei für den Assistenten zur Installation des Komponentensatzes "Administrationswerkzeuge" (dazu gehört die Programmkonsole); startet die Datei des Installationspakets esstools.msi mit den im Assistenten gewählten Installationsparametern.
\product\bases.cab	Archiv der zum Zeitpunkt der Veröffentlichung des Programms aktuellen Antiviren-Datenbanken.
\product\setup.exe	Die Datei für die Installation von Kaspersky Embedded Systems Security auf dem geschützten Computer mithilfe des Assistenten; startet die Installationspaketdatei "ess.msi" mit den im Assistenten angegebenen Installationseinstellungen.
\product\ess_x86(x64).msi	Paket des Dienstes Windows Installer; installiert Kaspersky Embedded Systems Security auf dem geschützten Computer.
\product\ess.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center.

Datei	Ziel
\product\klcfginst.exe	Installationsprogramm für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security über das Kaspersky Security Center. Installieren Sie das Verwaltungs-Plug-in auf jedem Computer, auf dem die Verwaltungskonsole von Kaspersky Security Center installiert ist, wenn Sie Kaspersky Embedded Systems Security mit dieser Konsole verwalten möchten.
\product\license.txt	Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
\product\migration.txt	Diese Datei beschreibt die Migration von vorherigen Programmversionen.
\setup\setup.hta	Datei für den Start des Begrüßungsprogramms.

Hard- und Software-Voraussetzungen

Vor der Installation von Kaspersky Embedded Systems Security müssen andere Virenschutzprogramme vom Computer deinstalliert werden.

Software-Voraussetzungen für den geschützten Computer

Sie können Kaspersky Embedded Systems Security auf einem Computer installieren, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows läuft.

Windows Installer 3.1 ist für die ordnungsgemäße Programminstallation und Funktion eines Computers unter Microsoft Windows XP erforderlich.

Um Kaspersky Embedded Systems Security auf Computern mit eingebetteten Betriebssystem verwenden zu können, muss die Komponente "Filter Manager" installiert sein.

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

- Windows XP Embedded SP3 (32-Bit)
- Windows Embedded POSReady 2009 (32-Bit)
- Windows XP Professional SP2 / SP3 (32-Bit, 64-Bit)
- Windows Embedded Standard 7 SP1 (32-Bit, 64-Bit)
- Windows Embedded Enterprise 7 SP1 (32-Bit, 64-Bit)
- Windows Embedded POSReady 7 (32-Bit, 64-Bit)
- Windows 7 Professional / Enterprise SP1 (32-Bit, 64-Bit)
- Windows Embedded 8.1 Industry Professional / Enterprise (32-Bit, 64-Bit)
- Windows Embedded 8.0 Standard (32-Bit, 64-Bit)
- Windows 8 Professional / Enterprise (32-Bit, 64-Bit)
- Windows 8,1 Professional / Enterprise (32-Bit, 64-Bit)
- Windows 10 Professional / Enterprise (32-Bit, 64-Bit)
- Windows 10 IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)

- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 Redstone 6 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)

Hardware-Voraussetzungen für den geschützten Computer

Die Hardware-Voraussetzungen für den geschützten Computer hängen vom installierten Windows-Betriebssystem ab:

- Hardware-Voraussetzungen für einen Computer unter Windows 7 (64-Bit), Windows 8 (64-Bit), Windows 10 (64-Bit), Windows Embedded 7, Windows Embedded 8:
  - Minimalkonfiguration:
    - Benötigter Speicherplatz:
      - Installation der Komponente "Kontrolle des Programmstarts" – 50 MB.
      - Installation aller Komponenten von Kaspersky Embedded Systems Security – 2 GB.
    - Arbeitsspeicher:
      - 256 MB für die ausschließliche Installation der Komponente "Kontrolle des Programmstarts" auf dem Computer, der unter dem Betriebssystem Microsoft Windows läuft.
      - 512 MB für die vollständige Installation aller Komponenten.
    - Prozessorvoraussetzungen:
      - für 32-Bit-Betriebssysteme von Microsoft Windows: Intel® Pentium® III-Einzelkernprozessor, 1,4 GHz.
      - Für 64-Bit-Betriebssysteme von Microsoft Windows: Intel Pentium IV Einzelkernprozessor, 1,4 GHz.
  - Empfohlene Konfiguration:
    - Benötigter Speicherplatz:
      - Installation der Komponente "Kontrolle des Programmstarts" – 2 GB.
      - Installation aller Komponenten von Kaspersky Embedded Systems Security – 4 GB.
    - Arbeitsspeicher: 2 GB.
    - Prozessorvoraussetzungen: Quad-Core-Prozessor, 2,4 GHz.
- Hardware-Voraussetzungen für einen Computer unter Windows 7 (64-Bit), Windows 8 (64-Bit), Windows 10 (64-Bit), Windows Embedded 7 oder Windows Embedded 8:
  - Minimalkonfiguration:
    - Benötigter Speicherplatz:
      - Installation der Komponente "Kontrolle des Programmstarts" – 50 MB.
      - Installation aller Komponenten von Kaspersky Embedded Systems Security – 2 GB.
    - Arbeitsspeicher: 1 GB.
    - Prozessorvoraussetzungen:
      - Für 32-Bit-Betriebssysteme von Microsoft Windows: Intel Pentium III Einzelkernprozessor, 1,4 GHz.
      - Für 64-Bit-Betriebssysteme von Microsoft Windows: Intel Pentium IV Einzelkernprozessor, 1,4 GHz.

- Empfohlene Konfiguration:
  - Benötigter Speicherplatz:
    - Installation der Komponente "Kontrolle des Programmstarts" – 2 GB.
    - Installation aller Komponenten von Kaspersky Embedded Systems Security – 4 GB.
  - Arbeitsspeicher: 2 GB.
  - Prozessorvoraussetzungen: Quad-Core-Prozessor, 2,4 GHz.

Funktionale Anforderungen und Einschränkungen

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

In diesem Abschnitt

Installation und Deinstallation

- Während der Programminstallation erscheint eine Warnung, wenn der Pfad zum Installationsordner von Kaspersky Embedded Systems Security mehr als 150 Zeichen enthält. Die Warnung hat keine Auswirkung auf den Installationsvorgang: Kaspersky Embedded Systems Security wird ordnungsgemäß installiert und ausgeführt.
- Um die Komponente "Unterstützung des SNMP-Protokolls" zu installieren, muss der SNMP-Dienst neu gestartet werden, falls dieser läuft.
- Für die Installation und Funktionsweise von Kaspersky Embedded Systems Security auf dem Gerät, das vom eingebetteten Betriebssystem verwaltet wird, muss die Komponente "Filter Manager" installiert sein.
- Die Installation der Administrations-Tools für Kaspersky Embedded Systems Security über die Gruppenrichtlinien von Microsoft Active Directory® ist nicht verfügbar.
- Bei der Installation des Programms auf Computern mit älteren Betriebssystemen, die keine regelmäßigen Updates beziehen können, müssen Sie folgende Stammzertifikate überprüfen: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Das Fehlen der aufgezählten Zertifikate kann zu Fehlern in der Funktionsweise des Programms führen. Es wird empfohlen, diese Zertifikate mit einer beliebigen, Ihnen verfügbaren Methode zu installieren.
- Die Konsole für Kaspersky Embedded Systems Security kann nicht über das Menü **Start** deinstalliert werden. Verwenden Sie zur Deinstallation der Konsole den Link im Fenster "Software".

Überwachung der Datei-Integrität

Standardmäßig überwacht die Komponente "Überwachung der Datei-Integrität" keine Änderungen in Systemordnern oder in den Housekeeping-Dateien des Dateisystems, damit Informationen über Routinevorgänge, die das Betriebssystem kontinuierlich mit Dateien ausführt, nicht in den Aufgabenberichten protokolliert werden. Der Benutzer kann solche Ordner nicht manuell zum Überwachungsbereich hinzufügen.

Die folgenden Ordner/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 usw.).

Firewall-Verwaltung

- Die Verwendung von IP-Adressen im IPv6-Format ist nicht verfügbar, wenn der festgelegte angewendete Regelbereich aus einer einzigen Adresse besteht.
- Die vorkonfigurierten Richtlinienregeln der Firewall ermöglichen die Ausführung grundlegender Interaktionsszenarien zwischen lokalen Computern und dem Administrationsserver. Um die Funktionen von Kaspersky Security Center vollständig zu verwenden, müssen manuell Regeln für Ports eingerichtet werden. Informationen über Portnummern, Protokolle und deren Funktionen finden Sie in der Wissensdatenbank von Kaspersky Security Center (Artikel-ID: 9297).
- Das Programm kontrolliert während der minutenweisen Abfragen durch die Aufgabe "Firewall-Verwaltung" keine Änderungen in den Windows Firewall-Regeln und Regelgruppen, wenn diese Regeln während der Programminstallation nicht zur Konfiguration der Aufgabe hinzugefügt wurden. Um den Status zu aktualisieren und solche Regeln einzuschließen, muss die Aufgabe "Firewall-Verwaltung" neu gestartet werden.
- Wenn die Aufgabe "Firewall-Verwaltung" gestartet wird, werden die folgenden Regeltypen automatisch aus den Einstellungen des Betriebssystems entfernt:
  - Verbotsregeln
  - Regeln zur Überwachung von ausgehendem Datenverkehr

Andere Einschränkungen

Untersuchung auf Befehl, Echtzeitschutz für Dateien:

- Die Untersuchung von über das MTP-Protokoll angeschlossenen Geräten ist nicht verfügbar.
- Die Untersuchung von Archivobjekten ist ohne die Untersuchung von SFX-Archiven nicht verfügbar: Wenn die Untersuchung von Archiven in den Schutzeinstellungen von Kaspersky Embedded Systems Security aktiviert ist, untersucht das Programm automatisch Objekte in Archiven und SFX-Archiven. Die Untersuchung von SFX-Archiven ist auch ohne die Untersuchung von Archiven verfügbar.

Lizenzverwaltung:

- Die Programmaktivierung mit einem Schlüssel über den Installationsassistenten ist nicht verfügbar, wenn sich die Schlüsseldatei auf einem Laufwerk befindet, das mithilfe des Befehls SUBST erstellt wurde, oder wenn für die Schlüsseldatei ein Netzwerkpfad angegeben wurde.

Updates:

- Nach der Installation von Updates für kritische Module von Kaspersky Embedded Systems Security wird das Programmsymbol standardmäßig ausgeblendet.
- KLRAMDISK wird auf Computern unter Windows XP oder Windows 2003 nicht unterstützt.

Oberfläche:

- Wenn Sie die Filterfunktion in der Programmkonsole in der Quarantäne, dem Backup, dem Systemaudit-Protokoll oder dem Protokoll der Aufgabenausführung verwenden, berücksichtigen Sie die Groß-/Kleinschreibung.
- Bei der Konfiguration des Schutz- oder Untersuchungsbereichs in der Programmkonsole können Sie nur eine einzige Maske verwenden und sie nur am Pfadende platzieren. Beispiele für die korrekte Verwendung der Maske: "C:\Temp\Temp*" oder "C:\Temp\Temp???.doc" oder "C:\Temp\Temp*.doc". Diese Einschränkung betrifft nicht die Konfiguration der vertrauenswürdigen Zone.

Sicherheit:

- Wenn im Betriebssystem die Benutzerkontensteuerung (User Account Control) aktiviert ist, muss das Benutzerkonto zur Gruppe KAVWSEE Administrators gehören, um die Programmkonsole mit einem Doppelklick auf das Programmsymbol im Infobereich der Taskleiste öffnen zu können. In anderen Fällen wird es erforderlich sein, sich als Benutzer anzumelden. Sie haben dann die Berechtigung, das kompakte Diagnosefenster oder das Microsoft Management Console-Snap-in zu öffnen.
- Die Deinstallation über das Microsoft Windows-Fenster **Programme und Features** ist nicht verfügbar, wenn die Benutzerkontensteuerung aktiviert ist.

Integration in Kaspersky Security Center:

- Der Administrationsserver überprüft die Gültigkeit der Datenbanken-Updates beim Erhalt der Update-Pakete und vor dem Versand der Updates an die Computer im Netzwerk. Der Administrationsserver überprüft nicht die Gültigkeit der empfangenen Updates der Programm-Module.
- Stellen Sie sicher, dass die Kontrollkästchen in den Einstellungen für "Interaktion mit Administrationsserver" aktiviert sind, wenn Sie Komponenten verwenden, die mithilfe von Netzwerklisten (Quarantäne, Backup) dynamisch veränderte Daten an Kaspersky Security Center übermitteln.

Exploit-Prävention:

- Die Exploit-Prävention ist nicht verfügbar, wenn die Bibliotheken apphelp.dll in der aktuellen Umgebungskonfiguration nicht geladen sind.
- Die Komponente "Exploit-Prävention" ist auf Computern mit dem Betriebssystem Microsoft Windows 10 nicht mit dem Microsoft-Dienstprogramm EMET kompatibel: Kaspersky Embedded Systems Security blockiert EMET, wenn die Komponente "Exploit-Prävention" auf einem Computer installiert wird, auf dem EMET bereits installiert ist.

Programm installieren und deinstallieren

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

In diesem Kapitel

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

Standardmäßig sind die Dateien "\product\ess_x86.msi" und "\product\ess_x64.msi" dazu vorgesehen, alle Programmkomponenten von Kaspersky Embedded Systems Security zu installieren. Sie können diese Komponenten installieren, indem Sie sie bei einer benutzerdefinierten Installation auswählen.

Durch die Dateien "\console\esstools_x86.msi" und "\console\esstools_x64.msi" werden alle Programmkomponenten im Paket "Administrations-Tools" installiert.

Die folgenden Abschnitte enthalten die Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer. Sie können diese Codes verwenden, um die Liste der zu installierenden Komponenten festzulegen, wenn Kaspersky Embedded Systems Security aus der Befehlszeile installiert wird.

In diesem Abschnitt

Programmkomponenten von Kaspersky Embedded Systems Security

Die folgende Tabelle enthält Codes und Beschreibungen der Programmkomponenten von Kaspersky Embedded Systems Security.

Tabelle 3. Beschreibung der Programmkomponenten von Kaspersky Embedded Systems Security

Komponente	Identifikator	Ausgeführte Funktion
Hauptfunktionen	core	Diese Komponente beinhaltet ein Paket von Basisfunktionen des Programms und gewährleistet deren Ausführung.
Kontrolle des Programmstarts	AppCtrl	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. Die Komponente wird in der Aufgabe "Kontrolle des Programmstarts" realisiert.
Gerätekontrolle	DevCtrl	Diese Komponente überwacht die Verbindungsversuche von USB-Massenspeichergeräten auf einem geschützten Computer und verbietet oder erlaubt deren Verwendung entsprechend den festgelegten Regeln zur Gerätekontrolle. Die Komponente wird in der Aufgabe Gerätekontrolle realisiert.
Antiviren-Schutz	AVProtection	Diese Komponente stellt den Antiviren-Schutz bereit und beinhaltet die folgenden Komponenten: • Untersuchung auf Befehl • Echtzeitschutz für Dateien

Komponente	Identifikator	Ausgeführte Funktion
Untersuchung auf Befehl	Ods	Diese Komponente installiert die Systemdateien von Kaspersky Embedded Systems Security und stellt Aufgaben zur Untersuchung auf Befehl bereit (Untersuchung von Objekten des geschützten Computers auf Anforderung). Wenn Sie beim Installieren von Kaspersky Embedded Systems Security aus der Befehlszeile andere Komponenten von Kaspersky Embedded Systems Security angeben, ohne die Core-Komponente zu nennen, wird die Core-Komponente automatisch installiert.
Echtzeitschutz für Dateien	Oas	Diese Komponente führt auf dem geschützten Computer eine Untersuchung von Dateien auf Viren durch, sobald auf diese Dateien zugegriffen wird. Sie setzt die Aufgabe Echtzeitschutz für Dateien um.
Verwendung von Kaspersky Security Network.	KSN	Diese Komponente gewährleistet den Schutz auf Basis der Cloud-Technologien von Kaspersky Lab. Sie setzt die Aufgabe Verwendung von KSN um (Versand von Anfragen und Erhalt von Einstufungen von den Diensten von Kaspersky Security Network).
Überwachung der Datei-Integrität	Fim	Diese Komponente ermöglicht es, Dateioperationen im festgelegten Überwachungsbereich zu protokollieren. Die Komponente wird in der Aufgabe Überwachung der Datei-Integrität umgesetzt.
Exploit-Prävention	AntiExploit	Diese Komponente ermöglicht die Verwaltung der Einstellungen zum Schutz des Prozess-Speichers im Speicher des geschützten Computers.
Firewall-Verwaltung	Firewall	Diese Komponente ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Embedded Systems Security zu verwalten. Die Komponente wird in der Aufgabe Firewall-Verwaltung umgesetzt.

Komponente	Identifikator	Ausgeführte Funktion
Modul für die Integration in den Administrationsagenten von Kaspersky Security Center	AKIntegration	Diese Komponente stellt eine Verbindung zwischen Kaspersky Embedded Systems Security und dem Administrationsagenten von Kaspersky Security Center bereit. Sie können diese Komponente auf dem geschützten Computer 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.
Satz von Leistungsindikatoren der Anwendung "Systemmonitor"	PerfMonCounters	Diese Komponente installiert Leistungsindikatoren des Programms Systemmonitor. Leistungsindikatoren messen die Leistungsfähigkeit von Kaspersky Embedded Systems Security und finden mögliche Engpässe bei gleichzeitiger Ausführung von Kaspersky Embedded Systems Security und anderen Programme.
SNMP-Indikator und Traps	SnmpSupport	Die Komponente veröffentlicht die Indikatoren und Traps für Kaspersky Embedded Systems Security über den Dienst Simple Network Management Protocol (SNMP) von Microsoft Windows. Sie können diese Komponente nur auf dem geschützten Computer installieren, wenn der Dienst Microsoft SNMP auf diesem Computer installiert ist.
Symbol für Kaspersky Embedded Systems Security im Infobereich	TrayApp	Die Komponente zeigt das Symbol für Kaspersky Embedded Systems Security im Infobereich der Taskleiste des geschützten Computers an. Das Symbol für Kaspersky Embedded Systems Security zeigt den Status des Computerschutzes an und ermöglicht, die Konsole für Kaspersky Embedded Systems Security in der Microsoft Management Console (falls installiert) und das Fenster **Über das Programm** zu öffnen.

Programmkomponenten des Pakets "Administrations-Tools"

Die folgende Tabelle enthält Codes und Beschreibungen der Programmkomponenten des Pakets "Administrations-Tools".

Tabelle 4. Beschreibung der Programmkomponenten des Satzes Administrationswerkzeuge

Komponente	Code	Funktionen der Komponente
Snap-ins von Kaspersky Embedded Systems Security	MmcSnapin	Die Komponente installiert das Microsoft Management Console Snap-in für die Verwaltung über die Konsole für Kaspersky Embedded Systems Security. Wenn Sie beim Installieren von "Administrations-Tools" aus der Befehlszeile andere Komponenten angeben, ohne die MmcSnapin-Komponente zu nennen, wird die Komponente automatisch installiert.
Help	Help	Dies ist eine chm-Hilfedatei; die im Ordner mit den Dateien der Administrations-Tools für Kaspersky Embedded Systems Security gespeichert wird. Sie können die Hilfedatei aus dem Menü **Start** oder in einem geöffneten Fenster der Programmkonsole mithilfe der Taste **F1** öffnen.
Dokumentation	Help	Kaspersky Embedded Systems Security fügt eine Verknüpfung zur Website von Kaspersky hinzu, auf welcher das Administratorhandbuch im PDF-Format bereitgestellt wird. Die Verknüpfung steht im Menü **Start** zur Verfügung.

Systemänderungen nach der Installation von Kaspersky Embedded Systems Security

Wenn Kaspersky Embedded Systems Security und das Paket der "Administrations-Tools" (einschließlich der Programmkonsole) gemeinsam installiert werden, nimmt der Dienst Windows Installer auf dem geschützten Computer folgende Veränderung vor:

- Auf dem geschützten Computer sowie auf dem Computer, auf dem die Programmkonsole installiert ist, werden Ordner für Kaspersky Embedded Systems Security erstellt.
- Die Dienste von Kaspersky Embedded Systems Security werden registriert.
- Eine Benutzergruppe für Kaspersky Embedded Systems Security wird erstellt.
- Die Schlüssel für Kaspersky Embedded Systems Security werden in der Systemregistrierung registriert.

Diese Änderungen sind nachfolgend beschrieben.

Ordner für Kaspersky Embedded Systems Security auf einem geschützten Computer

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

- Standardinstallationsordner für Kaspersky Embedded Systems Security mit den ausführbaren Dateien von Kaspersky Embedded Systems Security, abhängig vom Bit-Satz des Betriebssystems. Daher lauten die Installationsordner wie folgt:
  - In der 32-Bit-Version von Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
  - In der 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- 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.
  - %Kaspersky Embedded Systems Security%\mibs
- 64-Bit-Version der ausführbaren Dateien von Kaspersky Embedded Systems Security (dieser Ordner wird nur erstellt, wenn Kaspersky Embedded Systems Security unter einer 64-Bit-Version von Microsoft Windows installiert wird):
  - %Kaspersky Embedded Systems Security%\x64
- Dienstdateien für Kaspersky Embedded Systems Security
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Data\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Settings\
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Dskm\
- Dateien mit Einstellungen für Update-Quellen:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\
- Datenbanken-Updates und Updates der Programm-Module, die mithilfe der Aufgabe zur Update-Verteilung empfangen wurden (der Ordner wird erstellt, wenn zum ersten Mal Updates mithilfe der Aufgabe zur Update-Verteilung empfangen werden):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Update\Distribution\
- Protokolle der Aufgabenausführung und Systemaudit-Protokoll:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\
- Derzeit verwendetes Datenbankpaket:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Current\
- Backup-Kopien der Datenbanken; werden bei jedem Datenbanken-Update überschrieben:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Backup\

- Temporäre Dateien, die beim Ausführen der Update-Aufgabe angelegt werden:
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Bases\Temp\
- Objekte in der Quarantäne (Standardordner):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\
- Objekte im Backup (Standardordner):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\
- Objekte, die aus dem Backup oder der Quarantäne wiederhergestellt wurden (Standardordner für die Wiederherstellung von Objekten):
  - %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\

Ordner, der bei der Installation der Programmkonsole erstellt wird

Die Standardinstallationsordner der Programmkonsole mit den Dateien der "Administrations-Tools" hängen vom Bit-Satz des Betriebssystems ab. Daher lauten die Installationsordner wie folgt:

- In der 32-Bit-Version von Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\
- In der 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\

Dienste von Kaspersky Embedded Systems Security

Die folgenden Dienste von Kaspersky Embedded Systems Security werden unter dem lokalen Systemkonto (SYSTEM) gestartet:

- Kaspersky Security Service (KAVFS): wichtiger Dienst von Kaspersky Embedded Systems Security, der die Aufgaben und Workflows von Kaspersky Embedded Systems Security verwaltet.
- Kaspersky Security Management Service (KAVFSGT): Dieser Dienst ist zur Programmverwaltung von Kaspersky Embedded Systems Security durch die Programmkonsole vorgesehen.
- Kaspersky Security Exploit Prevention Service (KAVFSSLP): ein Dienst, der als Verteiler fungiert, um Sicherheitseinstellung an externe Sicherheitsagenten weiterzugeben und Daten über Sicherheitsereignisse zu empfangen.

Gruppe in Kaspersky Embedded Systems Security

"ESS Administrators" ist eine Gruppe auf dem geschützten Computer, deren Benutzer Vollzugriff auf den Dienst Kaspersky Security Management Service sowie auf alle Funktionen von Kaspersky Embedded Systems Security haben.

Schlüssel der Systemregistrierung

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

- Eigenschaften von Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Einstellungen des Ereignisprotokolls von Kaspersky Embedded Systems Security (Kaspersky Ereignisprotokoll): [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Eigenschaften des Management Service von Kaspersky Embedded Systems Security: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Einstellungen für den Leistungsindikator:
  - In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Parameter für die Komponente Unterstützung des SNMP-Protokolls:
  - In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\SnmpAgent]
  - In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\SnmpAgent]
- Einstellungen für die Dump-Datei:
  - In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
  - In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\2.3\CrashDump]
- Einstellungen für Protokolldateien:
  - In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
  - In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace]
- Konfiguration der Aufgaben und Funktionen des Programms: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Environment]

Prozesse von Kaspersky Embedded Systems Security

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

Tabelle 5. Prozesse von Kaspersky Embedded Systems Security

Dateiname	Ziel
kavfswp.exe	Workflow von Kaspersky Embedded Systems Security
kavtray.exe	Prozess für das Taskleistensymbol
kavfsmui.exe	Prozess für die Komponente "Kompaktes Diagnosefenster"
kavshell.exe	Prozess der Befehlszeilen-Utility
kavfsrcn.exe	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security
kavfs.exe	Dienstprozess von Kaspersky Security Service
kavfsgt.exe	Prozess des Verwaltungsdienstes Kaspersky Security Management Service
kavfswh.exe	Prozess von Kaspersky Security Exploit Prevention Service

Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer

Dieser Abschnitt enthält Beschreibungen der Einstellungen für die Installation und Deinstallation von Kaspersky Embedded Systems Security, ihrer Standardwerte und der Schlüssel für die Änderung der Einstellungswerte sowie deren mögliche Werte. 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 Optionen für die Befehlszeile im Windows Installer

- Akzeptieren der Bedingungen des Endbenutzer-Lizenzvertrags: Sie müssen die Bedingungen akzeptieren, damit Sie Kaspersky Embedded Systems Security installieren können.

  Die möglichen Werte für die Befehlszeilenoption `EULA=<Wert>` lauten wie folgt:

  - `0` – Sie lehnen die Bedingungen des Endbenutzer-Lizenzvertrags ab (Standardwert).
  - `1` – Sie akzeptieren die Bedingungen des Endbenutzer-Lizenzvertrags.
- Akzeptieren der Bedingungen der Datenschutzrichtlinie: Sie müssen die Bedingungen akzeptieren, damit Sie Kaspersky Embedded Systems Security installieren können.

Die möglichen Werte für die Befehlszeilenoption `PRIVACYPOLICY=<Wert>` lauten wie folgt:

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

- Installation von Kaspersky Embedded Systems Security und vorherige Untersuchung der aktiven Prozesse und Bootsektoren der lokalen Computerlaufwerke.

  Die möglichen Werte für die Befehlszeilenoption `PRESCAN=<Wert>` lauten wie folgt:

  - `0` – die aktiven Prozesse und die Bootsektoren der lokalen Computerlaufwerke während der Installation vorher nicht untersuchen (Standardwert).
  - `1` – die aktiven Prozesse und die Bootsektoren der lokalen Computerlaufwerke während der Installation vorher untersuchen.

- 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=<vollständiger Pfad des Ordners>` lauten wie folgt:

  - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - Administrations-Tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools
  - In der x64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%

- Die Aufgabe zum Echtzeitschutz für Dateien startet unmittelbar nach dem Start von Kaspersky Embedded Systems Security. Aktivieren Sie diese Einstellung, damit der Echtzeitschutz für Dateien beim Starten von Kaspersky Embedded Systems Security gestartet werden (empfohlen).

  Die möglichen Werte für die Befehlszeilenoption `RUNRTP=<Wert>` lauten wie folgt:

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

- Von Microsoft Corporation empfohlene Ausnahmen vom Schutz. In der Aufgabe Echtzeitschutz für Dateien werden jene Objekte auf dem Computer vom Schutzbereich ausgenommen, deren Ausnahme die Firma Microsoft empfiehlt. Einige Programme auf dem Computer laufen möglicherweise nicht stabil, wenn Antiviren-Anwendungen Dateien abfangen oder ändern, die von diesen Programmen verwendet werden. Zu solchen Programmen zählt Microsoft beispielsweise einige Anwendungen wie Domain-Controller.

  Die möglichen Werte für die Befehlszeilenoption `ADDMSEXCLUSION=<Wert>` lauten wie folgt:

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

- Gemäß den Empfehlungen von Kaspersky Lab vom Schutzbereich ausgeschlossene Objekte. In der Aufgabe zum Echtzeitschutz für Dateien werden Objekte auf dem Computer in Übereinstimmung mit der Empfehlung von Kaspersky Lab aus dem Schutzbereich ausgeschlossen.

  Die möglichen Werte für die Befehlszeilenoption `ADDKLEXCLUSION=<Wert>` lauten wie folgt:

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

- Remote-Verbindung zur Programmkonsole erlauben. Standardmäßig wird die Remote-Verbindung zu einer auf dem geschützten Computer installierten Programmkonsole nicht erlaubt. Während der Installation können Sie die Verbindung erlauben. Kaspersky Embedded Systems Security erstellt Erlaubnisregeln für den Prozess kavfsgt.exe gemäß TCP-Protokoll für alle Ports.

  Die möglichen Werte für die Befehlszeilenoption `ALLOWREMOTECON=<Wert>` lauten wie folgt:

  - `1` – erlauben
  - `0` – verbieten (Standardwert)

- Pfad der Schlüsseldatei. Der Windows Installer sucht standardmäßig in dem im Lieferumfang enthaltenen Ordner "\product" nach einer Datei mit der Erweiterung ".key". Wenn der Ordner "\product" mehrere Schlüsseldateien enthält, wählt der Windows Installer die Schlüsseldatei aus, deren Gültigkeitsdauer zuletzt abläuft. Sie können die Schlüsseldatei zuvor im Ordner "\product" speichern oder mit dem Installationsparameter **Schlüssel hinzufügen** einen anderen Pfad für die Schlüsseldatei angeben. 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=<Name der Konfigurationsdatei>` ist nicht festgelegt.

- Netzwerkverbindungen für die Programmkonsole aktivieren. Verwenden Sie diese Option, um Kaspersky Embedded Systems Security installieren auf einem anderen Computer zu installieren. Mit der Konsole für Kaspersky Embedded Systems Security können Sie den Computerschutz über einen anderen Computer ferngesteuert verwalten. Auf dem Computer wird in der Microsoft-Windows Firewall Port 135 (TCP) geöffnet, Netzwerkverbindungen werden für die ausführbare Datei kavfsrcn.exe zur Fernverwaltung von Kaspersky Embedded Systems Security erlaubt und der Zugriff auf DCOM-Programme wird zugelassen. Fügen Sie nach Abschluss der Installation Benutzer zur Gruppe "ESS Administrators" hinzu, damit diese das Programm ferngesteuert verwalten können, und erlauben Sie Netzwerkverbindungen zum Dienst Kaspersky Security Management Service (Datei "kavfsgt.exe") auf dem Computer. Mehr zur weiteren Konfiguration bei Installation der Konsole für Kaspersky Embedded Systems Security auf einem anderen Computer finden Sie im Abschnitt "Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Computer" auf Seite 53.

  Die möglichen Werte für die Befehlszeilenoption `ADDWFEXCLUSION=<Wert>` lauten wie folgt:

  - `1` – erlauben
  - `0` – verbieten (Standardwert)

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

  Die möglichen Werte für die Befehlszeilenoption `SKIPINCOMPATIBLESW=<Wert>` lauten wie folgt:

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

Deinstallationsparameter und Optionen für die Befehlszeile für den Dienst Windows Installer

- Wiederherstellen von Objekten aus der Quarantäne

  Die möglichen Werte für die Befehlszeilenoption `RESTOREQTN=<Wert>` lauten wie folgt:

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

- Wiederherstellen des Backup-Inhalts

  Die möglichen Werte für die Befehlszeilenoption `RESTOREBCK=<Wert>` lauten wie folgt:

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

- Aktuelles Kennwort eingeben, um die Deinstallation zu bestätigen (wenn der Kennwortschutz aktiviert ist)

  Der Standardwert für `UNLOCK_PASSWORD=<festgelegtes Kennwort>` ist nicht festgelegt.

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

  Der Standardwert für die Befehlszeilenoption `RESTOREPATH=<vollständiger Pfad des Ordners>` lautet %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored.

Installations- und Deinstallationsprotokolle für Kaspersky Embedded Systems Security

Wenn Sie die Installation oder Deinstallation von Kaspersky Embedded Systems Security mit Hilfe des Assistenten zur Installation (Deinstallation) starten, erstellt der Dienst Windows Installer ein Protokoll über die Installation (Deinstallation). Eine Log-Datei mit dem Namen ess_install_<uid>.log (wobei <uid> eine eindeutige Protokoll-ID mit 8 Zeichen ist) wird im Ordner %temp% des Benutzers gespeichert, dessen Konto für den Start der Datei setup.exe verwendet wurde.

Wenn Sie für die Programmkonsole oder für Kaspersky Embedded Systems Security über das Menü **Start** die Option Ändern oder Löschen ausführen, wird im Ordner %temp% automatisch eine Log-Datei mit dem Namen ess_2.3_maintenance.log erstellt.

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

► *Gehen Sie wie folgt vor, um Kaspersky Embedded Systems Security zu installieren und eine Log-Datei auf dem Laufwerk C:\ zu erstellen:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

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 (siehe Abschnitt "Installation und Deinstallation des Programms mit dem Assistenten" auf Seite 48), der Befehlszeile (siehe Abschnitt "Installation und Deinstallation des Programms aus der Befehlszeile" auf Seite 63), über Kaspersky Security Center (siehe Abschnitt "Installation und Deinstallation von Kaspersky Anti-Virus mit Kaspersky Security Center" auf Seite 68) und mittels einer Active Directory-Gruppenrichtlinie (siehe Abschnitt "Installation und Deinstallation mittels Active Directory-Gruppenrichtlinien" auf Seite 74).

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 (siehe Abschnitt "Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer" auf S. 34).
3. Wählen Sie die Installationsmethode aus.

In diesem Abschnitt

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 Verwaltungskonsole von Kaspersky Security Center 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 Computer oder auf einem anderen Computer 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 Computer mit installiertem Kaspersky Embedded Systems Security zu verwalten.

Die Programmkonsole ist Teil des Programmkomponentenpakets "Administrations-Tools".

Befehlszeilen-Utility

Sie können Kaspersky Embedded Systems Security aus der Befehlszeile eines geschützten Computers 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 Computer in Ihrem Unternehmen Kaspersky Security Center verwenden, können Sie Kaspersky Embedded Systems Security über die Verwaltungskonsole von Kaspersky Security Center verwalten.

Die folgenden Programmkomponenten müssen installiert werden:

- **Modul für die Integration in den Administrationsagenten von Kaspersky Security Center**. 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 Administrationsagenten von Kaspersky Security Center auf dem geschützten Computer.
- **Administrationsagent von Kaspersky Security Center**. Installieren Sie ihn auf jedem geschützten Computer. Diese Komponente koordiniert die Interaktion zwischen dem auf dem Computer installierten Programm Kaspersky Embedded Systems Security und der Verwaltungskonsole von Kaspersky Security Center. Die Installationsdatei des Administrationsagenten gehört zum Lieferumfang von Kaspersky Security Center.
- Verwaltungs-Plug-in für Kaspersky Embedded Systems Security. Installieren Sie außerdem auf dem Computer, auf dem der Kaspersky Security Center-Administrationsserver installiert ist, über die Verwaltungskonsole das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security. Dadurch wird eine Schnittstelle zur Programmverwaltung über Kaspersky Security Center bereitgestellt. Die Installationsdatei für das Verwaltungs-Plug-in, \product\klcfginst.exe, gehört zum Lieferumfang von Kaspersky Embedded Systems Security.

Installationstyp auswählen

Nachdem Sie die Softwarekomponenten für die Installation von Kaspersky Embedded Systems Security (siehe Abschnitt "Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer" auf S. 34) 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 (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 42).
- Ob die Installationseinstellungen für alle Computer einheitlich oder für jedem Computer 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.

Kaspersky Embedded Systems Security kann auf einem einzelnen Computer installiert und konfiguriert werden. Die Konfigurationsdatei, in der die Einstellungen gespeichert werden, kann anschließend zur Installation von Kaspersky Embedded Systems Security auf anderen Computern verwendet werden. Beachten Sie, dass dies nicht möglich ist, wenn zur Installation des Programms Active Directory-Gruppenrichtlinien verwendet werden.

Installationsassistent starten

Mit dem Installationsassistenten können Sie installieren:

- Die Komponenten von Kaspersky Embedded Systems Security (siehe Abschnitt "Programmkomponenten von Kaspersky Embedded Systems Security" auf Seite 35) auf einem geschützten Computer aus der Datei "\product\setup.exe", die im Lieferumfang enthalten ist.
- Konsole für Kaspersky Embedded Systems Security (siehe Abschnitt "Konsole für Kaspersky Embedded Systems Security installieren" auf Seite 52) aus der im Lieferumfang enthaltenen Datei "\console\setup.exe" auf dem geschützten Computer oder einem anderen LAN-Host.

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 Computer 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 (siehe Abschnitt "Installation und Deinstallation des Programms aus der Befehlszeile" auf Seite 63).

Zentrale Installation über Kaspersky Security Center

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

Die Computer, auf denen Sie Kaspersky Embedded Systems Security mittels Kaspersky Security Center installieren möchten (siehe Abschnitt "Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center" auf Seite 68), 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 Computer installieren. Sie können auch die Programmkonsole auf dem geschützten Computer oder auf dem Administrator-Arbeitsplatz installieren.

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

Die Computer, auf denen Kaspersky Embedded Systems Security mithilfe von Active Directory-Gruppenrichtlinien installiert wird (siehe Abschnitt "Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory" auf Seite 74) müssen sich in derselben Domäne und derselben Organisationseinheit befinden. Die Installation erfolgt beim Start des Computers 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.

In diesem Abschnitt

Installation mit dem Installationsassistenten

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

► *Gehen Sie folgendermaßen vor, um Kaspersky Embedded Systems Security zu installieren und zu verwenden:*

1. Installieren Sie Kaspersky Embedded Systems Security auf einem geschützten Computer.
2. Installieren Sie die Programmkonsole auf den Computern, von denen Sie Kaspersky Embedded Systems Security verwalten möchten.
3. Wenn Sie die Programmkonsole im Netzwerk auf einem anderen als dem geschützten Computer installiert haben, sind zusätzliche Einstellungen erforderlich, damit Kaspersky Embedded Systems Security von den Programmkonsolenbenutzern ferngesteuert verwaltet werden kann.
4. Führen Sie Aktionen nach der Installation von Kaspersky Embedded Systems Security durch.

In diesem Abschnitt

Installation von Kaspersky Embedded Systems Security

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

Vergewissern Sie sich, dass auf dem Computer keine anderen Antiviren-Anwendungen installiert sind.

- Vergewissern Sie sich, dass das Benutzerkonto, mit dessen Berechtigungen Sie den Installationsassistenten starten, zur Administratorengruppe auf dem geschützten Computer gehört.

Wechseln Sie nach der Durchführung der oben beschriebenen Aktionen zum Installationsvorgang. Folgen Sie den Anweisungen des Installationsassistenten und geben Sie die Installationseinstellungen für Kaspersky Embedded Systems Security an. Sie können die Installation von Kaspersky Embedded Systems Security in jedem Schritt des Installationsassistenten abbrechen. Klicken Sie dazu im Fenster des Installationsassistenten auf die Schaltfläche Abbrechen.

Mehr über die Installations- bzw. Deinstallationseinstellungen finden Sie im Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 42.

► *So installieren Sie Kaspersky Embedded Systems Security mithilfe des Installationsassistenten:*

1. Starten Sie auf dem Computer die Datei "setup.exe".
2. Klicken Sie im folgenden Fenster im Abschnitt Installation auf den Link Kaspersky Embedded Systems Security installieren.
3. Klicken Sie im Begrüßungsfenster des Installationsassistenten von Kaspersky Embedded Systems Security auf die Schaltfläche Weiter.

   Das Fenster Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie wird geöffnet.
4. Lesen Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
5. Wenn Sie mit den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie die Kontrollkästchen Bedingungen dieses Endbenutzer-Lizenzvertrags und Datenschutzrichtlinie, die den Umgang mit Daten beschreibt, um mit der Installation fortzufahren.

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

   Das Fenster Schnelle Untersuchung des Computers vor dem Start der Installation wird geöffnet.
7. Aktivieren Sie im Fenster Schnelle Untersuchung des Computers vor dem Start der Installation das Kontrollkästchen Computer auf Viren untersuchen, um die Bootsektoren von lokalen Datenträgern des Computers und den Systemspeicher auf Bedrohungen zu untersuchen. Klicken Sie auf Weiter. Nach der Untersuchung öffnet sich das Fenster mit den Ergebnissen der Untersuchung.

   Sie können Informationen über untersuchte Objekte des Computers anzeigen: Anzahl der untersuchten Objekte, Anzahl der gefundenen Bedrohungen, Anzahl der gefundenen infizierten und möglicherweise infizierten Objekte, Anzahl der infizierten oder verdächtigen Prozesse, die Kaspersky Embedded Systems Security aus dem Arbeitsspeicher entfernt hat, und Anzahl der infizierten oder verdächtigen Prozesse, die das Programm nicht löschen konnte.

   Um anzuzeigen, welche Objekte genau untersucht worden sind, klicken Sie auf die Schaltfläche Liste der verarbeiteten Objekte.
8. Klicken Sie im Fenster Schnelle Untersuchung des Computers vor dem Start der Installation auf die Schaltfläche Weiter.

   Das Fenster Benutzerdefinierte Installation wird geöffnet.
9. Wählen Sie die Komponente, die Sie installieren wollen.

   Standardmäßig umfasst die empfohlene Installation alle Komponenten von Kaspersky Embedded Systems Security, mit Ausnahme der Komponenten "Firewall-Verwaltung".

Die Komponente Unterstützung des SNMP-Protokolls von Kaspersky Embedded Systems Security wird nur auf dem geschützten Computer installiert, wenn auf dem Server der Dienst SNMP Microsoft Windows installiert ist.

10. Um alle Änderungen im Fenster Benutzerdefinierte Installation zu verwerfen, klicken Sie auf die Schaltfläche Zurücksetzen. Klicken Sie auf Weiter.
11. Gehen Sie im Fenster Zielordner auswählen 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.
12. Passen Sie im Fenster Erweiterte Einstellungen für die Installation folgende Installationseinstellungen an:
    - Echtzeitschutz nach der Installation des Programms aktivieren.
    - Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen.
    - Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen.

    Klicken Sie auf Weiter.
13. Gehen Sie im Fenster Einstellungen aus einer Konfigurationsdatei importieren wie folgt vor:
    a. Um die Einstellungen für Kaspersky Embedded Systems Security aus einer vorhandenen Konfigurationsdatei zu importieren, die in einer kompatiblen Vorgängerversion der Anwendung erstellt wurde, geben Sie die Konfigurationsdatei an.
    b. Klicken Sie auf Weiter.
14. 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 "\product" (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.

      Nach dem Hinzufügen der Schlüsseldatei werden im Fenster die Lizenzinformationen angezeigt. Kaspersky Embedded Systems Security zeigt die berechnete Gültigkeitsdauer 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 die Schaltfläche Weiter, um die Schlüsseldatei für das Programm zu übernehmen.
15. Klicken Sie im Fenster Bereit zur Installation auf die Schaltfläche Installieren. Der Assistent installiert nun die Komponenten von Kaspersky Embedded Systems Security.
16. Sobald die Installation abgeschlossen wurde, öffnet sich das Fenster Die Installation wurde erfolgreich abgeschlossen.

17. Aktivieren Sie das Kontrollkästchen Versionshinweise lesen, um nach Fertigstellung des Installationsassistenten die Informationen zur Version anzusehen.
18. 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.

► *Um die Programmkonsole zu installieren, gehen Sie wie folgt vor:*

1. Vergewissern Sie sich, dass das Benutzerkonto, das Sie verwenden, um den Installationsassistenten starten, zur Administratorengruppe auf dem geschützten Computer gehört.
2. Starten Sie auf dem Computer die Datei "setup.exe".

   Das Fenster des Willkommen-Programms wird geöffnet.
3. Klicken Sie auf den Link Konsole für Kaspersky Embedded Systems Security installieren.

   Es öffnet sich das Begrüßungsfenster des Installationsassistenten.
4. Klicken Sie auf Weiter.
5. Lesen Sie die Bedingungen des Endbenutzer-Lizenzvertrags im geöffneten Fenster und aktivieren Sie das Kontrollkästchen **Ich bestätige die vollständige Kenntnis, das Verständnis und das Einverständnis bezüglich der Bedingungen dieser EULA**, um mit der Installation fortfahren zu können.
6. Klicken Sie auf Weiter.

   Das Fenster Erweiterte Einstellungen für die Installation wird geöffnet.
7. Gehen Sie im folgenden Fenster Erweiterte Einstellungen für die Installation wie folgt vor:
   - Wenn Sie planen, Kaspersky Embedded Systems Security auf einem Remote-Computer mithilfe der Programmkonsole zu verwalten, aktivieren Sie das Kontrollkästchen Remote-Zugriff erlauben.
   - Um das Fenster Benutzerdefinierte Installation zu öffnen und Komponenten auszuwählen, gehen Sie wie folgt vor:
     a. Klicken Sie auf die Schaltfläche Erweitert.

        Das Fenster Benutzerdefinierte Installation wird geöffnet.
     b. Wählen Sie die "Administrations-Tools" aus der Liste aus.

        Standardmäßig werden alle Komponenten installiert.
     c. Klicken Sie auf Weiter.

Detailliertere Informationen über die Komponenten von Kaspersky Embedded Systems Security finden Sie im Abschnitt "Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer" auf Seite 34.

8. Gehen Sie im Fenster Zielordner auswählen wie folgt vor:
   a. Geben Sie bei Bedarf einen anderen Ordner an, in dem die zu installierenden Dateien gespeichert werden sollen.
   b. Klicken Sie auf Weiter.
9. Klicken Sie im Fenster Bereit zur Installation auf die Schaltfläche Installieren.

   Der Assistent installiert nun die ausgewählten Komponenten.
10. Klicken Sie auf **Fertig**.

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

Wenn Sie das Paket "Administrations-Tools" nicht auf dem geschützten Computer, sondern auf einem anderen Netzwerkcomputer installiert haben, passen Sie die Erweiterten Einstellungen an (siehe Abschnitt "Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Computer" auf Seite 53).

Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Computer

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

- Fügen Sie auf dem geschützten Computer die Benutzer von Kaspersky Embedded Systems Security zur Gruppe "ESS Administrators" hinzu.
- Erlauben Sie Netzwerkverbindungen für den Dienst Kaspersky Security Management Service (kavfsgt.exe) (siehe Abschnitt "Über Zugriffsrechte für den Verwaltungsdienst Kaspersky Security Management Service" auf Seite 243), wenn auf dem geschützten Computer die Windows Firewall oder die Firewall eines Drittherstellers verwendet wird.
- Wenn das Kontrollkästchen Remote-Zugriff erlauben während der Installation der Programmkonsole auf einem Computer unter Microsoft Windows nicht aktiviert ist, müssen Sie Netzwerkverbindungen für die Programmkonsole manuell über die Firewall auf diesem Computer erlauben.

Die Programmkonsole auf dem Remote-Computer verwendet das Protokoll DCOM, um Informationen über die Ereignisse für Kaspersky Embedded Systems Security, zum Beispiel untersuchte Objekte oder abgeschlossene Aufgaben, vom Verwaltungsdienst für Kaspersky Security Management Service auf dem geschützten Computer zu erhalten. Sie müssen die Netzwerkverbindungen in der Windows-Firewall für die Programmkonsole freigeben, um die Verbindung zwischen der Programmkonsole und dem Kaspersky Security Management Service herzustellen.

Gehen Sie auf dem Remote-Computer, auf dem die Programmkonsole installiert ist, wie folgt vor:

- Vergewissern Sie sich, dass der anonyme Remote-Zugriff auf COM-Anwendungen erlaubt ist (nicht aber der Remote-Start und die Remote-Aktivierung von COM-Anwendungen).
- Schalten Sie in der Windows-Firewall den TCP-Port 135 frei und erlauben Sie Netzwerkverbindungen für kavfsrcn.exe, die ausführbare Datei des Fernverwaltungsprozesses für Kaspersky Embedded Systems Security.

  Der Client-Computer, auf dem die Programmkonsole installiert ist, verwendet TCP-Port 135, um auf den geschützten Computer zuzugreifen und eine Antwort zu empfangen.
- Konfigurieren Sie eine ausgehende Regel für die Windows-Firewall, um die Verbindung zu erlauben.

  Im Gegensatz zu den herkömmlichen TCP/IP- und UDP/IP-Diensten, bei denen ein einzelnes Protokoll einen festen Port hat, weist DCOM den ferngesteuerten COM-Objekten dynamisch Ports zu. Wenn eine Firewall zwischen dem Client (auf dem die Programmkonsole installiert ist) und dem DCOM-Endpunkt (dem geschützten Computer) existiert, muss ein großer Bereich von Ports geöffnet werden.

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 Computer und dem Computer 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 (kavfsrcn.exe) abgeschlossen ist.
3. Starten Sie die Programmkonsole neu.

   Die neuen Verbindungseinstellungen werden übernommen.

In diesem Abschnitt

Anonymen Remote-Zugriff auf COM-Anwendungen erlauben

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

► *Um den anonymen Fernzugang zu COM-Anwendungen freizugeben, gehen Sie wie folgt vor:*

1. Öffnen Sie auf dem Remote-Computer, auf dem die Konsole für Kaspersky Embedded Systems Security installiert ist, die Komponentendienste-Konsole.
2. Wählen Sie **Start** → **Ausführen**.
3. Führen Sie den Befehl `dcomcnfg` aus.
4. Klicken Sie auf **OK**.
5. Öffnen Sie in der Konsole **Komponentendienste** Ihres Computers den Knoten **Computer**.
6. Öffnen Sie das Kontextmenü im Knoten **Arbeitsplatz**.
7. Wählen Sie den Menüpunkt **Eigenschaften**.
8. Klicken Sie auf der Registerkarte **COM-Sicherheit** im Fenster **Eigenschaften** auf die Schaltfläche **Beschränkungen ändern** in der Einstellungsgruppe **Zugriffsrechte**.
9. Vergewissern Sie sich im Fenster **Remote-Zugriff erlauben**, dass für den Benutzer ANONYMOUS LOGON das Kontrollkästchen **Remote-Zugriff erlauben** aktiviert ist.
10. 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 die ausführbare Datei des Prozesses 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-Computer.
2. Führen Sie eine der Aktionen durch:
   - In Microsoft Windows XP SP2 oder höher:
     a. Klicken Sie auf **Start** > **Windows-Firewall**.
     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**).

Ausgehende Regel für die Windows-Firewall hinzufügen

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

► *Um die ausgehende Regel für die Windows-Firewall hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie **Start** > **Systemsteuerung** > **Windows Firewall**.
2. Klicken Sie im Fenster **Windows-Firewall** auf den Link **Erweiterte Einstellungen**.

   Das Fenster **Windows-Firewall mit erweiterter Sicherheit** wird geöffnet.
3. Aktivieren Sie den untergeordneten Knoten **Ausgehende Regeln**.
4. Klicken Sie im Bereich **Aktionen** auf die Option **Neue Regel**.
5. Wählen Sie im nächsten Fenster des **Assistenten für neue Ausgangsregeln** die Option **Port** aus und klicken Sie auf **Weiter**.
6. Wählen Sie das Protokoll **TCP**.
7. Geben Sie im Feld **Bestimmte Remote-Ports** den folgenden Bereich für Ports an, um ausgehende Verbindungen zuzulassen: 1024-65535.
8. Wählen Sie im Fenster **Aktion** die Option **Verbindung zulassen** aus.
9. Speichern Sie die neue Regel und schließen Sie das Fenster **Windows-Firewall mit erweiterter Sicherheit**.

Die Windows-Firewall lässt jetzt keine Netzwerkverbindungen zwischen der Programmkonsole und Kaspersky Security Management Service zu.

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 während der Installation von Kaspersky Embedded Systems Security die Option Echtzeitschutz nach der Installation des Programms aktivieren (Standardoption) ausgewählt ist, untersucht das Programm die Objekte des Dateisystems des Computers, wenn darauf zugegriffen wird. Jeden Freitag um 20:00 Uhr führt Kaspersky Embedded Systems Security die Aufgabe zur Untersuchung wichtiger Bereiche aus.

Es wird empfohlen, nach der Installation von Kaspersky Embedded Systems Security folgende Aktionen 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 auf dem Computer durch, wenn vor der Installation von Kaspersky Embedded Systems Security auf dem geschützten Computer kein Virenschutzprogramm mit aktivierter Funktion zum Echtzeitschutz für Dateien installiert war.
- Passen Sie Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security an.

In diesem Abschnitt

Aufgabe zum Update der Datenbank von Kaspersky Embedded Systems Security starten und anpassen

► *Um die Programm-Datenbanken nach der Installation zu aktualisieren, gehen Sie wie folgt vor:*

1. Konfiguration einer Verbindung zu einer Update-Quelle (HTTP- oder FTP-Update-Server von Kaspersky Lab) in den Einstellungen der Aufgabe für das Update der Programm-Datenbanken.
2. Start der Aufgabe zum Update der Programm-Datenbanken.

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.

► *Um die optionalen Proxyservereinstellungen und Authentifizierungseinstellungen für den Zugriff auf den Proxyserver festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Kontextmenü des Knotens Kaspersky Security.
2. Wählen Sie das Element **Eigenschaften** aus.

   Das Fenster Programmeinstellungen wird geöffnet.
3. Wählen Sie die Registerkarte Verbindungseinstellungen aus.
4. Wählen Sie im Abschnitt Proxyservereinstellungen das Kontrollkästchen Einstellungen des angegebenen Proxyservers 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. Wählen Sie im Abschnitt Einstellungen für die Authentifizierung auf dem Proxyserver die erforderliche Authentifizierungsmethode aus der Dropdown-Liste:
   - NTLM-Authentifizierung verwenden, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung (NTLM-authentication) unterstützt. Kaspersky Embedded Systems Security benutzt für den Zugriff auf den Proxyserver das Benutzerkonto, das in den Aufgabeneinstellungen angegeben ist (standardmäßig läuft die Aufgabe unter dem Benutzerkonto **Lokales System** (**SYSTEM**)).
   - NTLM-Authentifizierung mit Benutzername und Kennwort verwenden, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung unterstützt. Kaspersky Embedded Systems Security verwendet das von Ihnen vorgegebene Benutzerkonto für den Zugriff auf den Proxyserver. Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.
   - Benutzername und Kennwort verwenden, um die übliche Authentifizierung auszuwählen (Basic authentication). Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.

7. Klicken Sie im Fenster Programmeinstellungen auf **OK**.

► *Um die Verbindung zu den Kaspersky-Lab-Update-Servern in der Aufgabe zum Update der Programm-Datenbanken anzupassen, gehen Sie wie folgt vor:*

1. Starten Sie die Programmkonsole mit einer der folgenden Methoden:
   - Öffnen Sie die Programmkonsole auf dem geschützten Computer. Wählen Sie dazu **Start** > **Alle Programme** > Kaspersky Embedded Systems Security > Administrations-Tools > Konsole für Kaspersky Embedded Systems Security.
   - Wenn die Programmkonsole nicht auf dem geschützten, sondern auf einem anderen Computer gestartet wurde, stellen Sie eine Verbindung mit dem geschützten Server her:
     a. Öffnen Sie das Kontextmenü des Knotens Kaspersky Embedded Systems Security in der Struktur der Programmkonsole.
     b. Wählen Sie den Punkt Verbindung mit anderem Computer herstellen aus.
     c. Wählen Sie im Fenster Computer auswählen die Option Anderer Computer und geben Sie im Eingabefeld den Netzwerknamen des geschützten Computers an.

   Wenn das Benutzerkonto, mit dem Sie sich in Microsoft Windows angemeldet haben, über keine Zugriffsrechte für den Verwaltungsdienst Kaspersky Security Management Service verfügt (siehe Abschnitt "Über Zugriffsrechte für Kaspersky Security Management Service" auf S. 243), geben Sie ein Benutzerkonto mit den erforderlichen Rechten an.

   Das Fenster "Programmkonsole" wird geöffnet.
2. Öffnen Sie in der Struktur der Programmkonsole den Knoten Update.
3. Wählen Sie den untergeordneten Knoten Update der Programm-Datenbanken aus.
4. Klicken Sie im Ergebnisbereich auf den Link Eigenschaften.
5. Öffnen Sie im nächsten Fenster Aufgabeneinstellungen die Registerkarte Verbindungseinstellungen.
6. Aktivieren Sie Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Lab-Update-Servern verwenden.
7. Klicken Sie im Fenster Aufgabeneinstellungen auf **OK**.

Die Verbindungseinstellungen mit der Update-Quelle werden in der Aufgabe zum Update der Programm-Datenbanken gespeichert.

► *Um die Aufgabe Update der Programm-Datenbanken zu starten, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten Update.
2. Wählen Sie im Kontextmenü des untergeordneten Knotens Update der Programm-Datenbanken den Punkt Starten.

Die Aufgabe zum Update der Programm-Datenbanken wird gestartet.

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

Untersuchung wichtiger Bereiche

Nachdem Sie die Datenbanken von Kaspersky Embedded Systems Security aktualisiert haben, untersuchen Sie den Computer mit der Aufgabe Untersuchung wichtiger Bereiche auf Schadsoftware.

► *Um die Aufgabe Untersuchung wichtiger Bereiche anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten Untersuchung auf Befehl.
2. Wählen Sie im Kontextmenü des untergeordneten Knotens Untersuchung wichtiger Bereiche den Befehl Starten.

Die Aufgabe wird gestartet. Im Detailbereich wird der Aufgabenstatus Läuft angezeigt.

► *Um das Protokoll der Aufgabenausführung anzuzeigen, machen Sie Folgendes,*

klicken Sie im Ergebnisbereich des Knotens Untersuchung wichtiger Bereiche auf den Link Protokoll der Aufgabenausführung öffnen.

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

Komponenten von Kaspersky Embedded Systems Security können hinzugefügt oder entfernt werden. Wenn Sie die Komponente Echtzeitschutz für Dateien deinstallieren wollen, müssen Sie vorsichtshalber zuerst die Aufgabe Echtzeitschutz für Dateien entfernen. In den übrigen Fällen ist es nicht erforderlich, die Aufgabe zum Echtzeitschutz für Dateien oder Kaspersky 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 **Startmenü** den Punkt **Alle Programme** > **Kaspersky Embedded Systems Security** > Ändern oder Löschen aus.

   Das Fenster Installation ändern, reparieren oder entfernen des Installationsassistenten für das Programm wird geöffnet.
2. Wählen Sie Auswahl der Programmkomponenten ändern aus. Klicken Sie auf Weiter.

   Das Fenster Benutzerdefinierte Installation wird geöffnet.

3. 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 auf der lokalen Festplatte installiert, wenn Sie eine Gruppe von Komponenten installieren möchten.
   - Um zuvor installierte Komponenten zu entfernen, klicken Sie auf die Schaltfläche neben dem Namen der ausgewählten Komponente. Wählen Sie dann im Kontextmenü Die Komponente wird nicht verfügbar sein.

   Klicken Sie auf Weiter.

4. Bestätigen Sie im Fenster Bereit zur Installation den Vorgang zur Änderung der Zusammensetzung der Programmkomponenten, indem Sie auf die Schaltfläche Installieren klicken.
5. Klicken Sie im Fenster, das nach Abschluss der Installation geöffnet wird, auf OK.

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

Wenn bei der Ausführung von Kaspersky Embedded Systems Security Probleme aufgetreten sind (Kaspersky Embedded Systems Security stürzt ab, Aufgaben stürzen ab oder werden nicht gestartet), können Sie versuchen, Kaspersky Embedded Systems Security zu reparieren. 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.

► *Um Kaspersky Embedded Systems Security nach einer fehlerhaften Beendigung des Programms oder einer Aufgabe zu reparieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Menü **Start** die Option **Alle Programme**.
2. Wählen Sie **Kaspersky Embedded Systems Security**.
3. Wählen Sie Ändern oder löschen.

   Das Fenster Installation ändern, reparieren oder entfernen des Installationsassistenten für das Programm wird geöffnet.

4. Wählen Sie den Punkt Installierte Komponenten reparieren aus. Klicken Sie auf Weiter.

   Das Fenster Installierte Komponenten reparieren wird geöffnet.

5. Aktivieren Sie im Fenster Installierte Komponenten reparieren das Kontrollkästchen Empfohlene Programmeinstellungen wiederherstellen, wenn Sie die Einstellungen des Programms zurücksetzen und Kaspersky Embedded Systems Security mit den vorinstallierten Standardeinstellungen wiederherstellen möchten. Klicken Sie auf Weiter.
6. Bestätigen Sie im Fenster Bereit zur Wiederherstellung den Vorgang zur Wiederherstellung der Zusammensetzung des Programms, indem Sie auf die Schaltfläche Installieren klicken.
7. Klicken Sie im Fenster, das nach Abschluss des Reparaturvorgangs geöffnet wird, auf OK.

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 Computer mithilfe des Installations-/Deinstallationsassistenten.

In diesem Abschnitt

Deinstallation von Kaspersky Embedded Systems Security

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

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

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

Deinstallation, Reparatur und Installation des Programms ist über die Windows-Systemsteuerung nicht möglich, wenn das Betriebssystem die UAC-Funktion (User Account Control) verwendet oder der Zugriff auf das Programm kennwortgeschützt ist.

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.

► *So deinstallieren Sie Kaspersky Embedded Systems Security:*

1. Wählen Sie im Menü **Start** die Option **Alle Programme**.
2. Wählen Sie **Kaspersky Embedded Systems Security**.
3. Wählen Sie Ändern oder löschen.

   Das Fenster Installation ändern, reparieren oder entfernen des Installationsassistenten für das Programm wird geöffnet.
4. Wählen Sie den Punkt Entfernen von Programmkomponenten aus. Klicken Sie auf Weiter.

   Das Fenster Erweiterte Einstellungen für die Deinstallation des Programms wird geöffnet.

5. Gehen Sie im Fenster Erweiterte Einstellungen für die Deinstallation des Programms erforderlichenfalls wie folgt vor:

   a. Aktivieren Sie das Kontrollkästchen Quarantäne-Objekte exportieren, damit Kaspersky Embedded Systems Security die Quarantäneobjekte exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Aktivieren Sie das Kontrollkästchen Backup-Objekte exportieren, damit Kaspersky Embedded Systems Security Objekte aus dem Backup exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   c. Klicken Sie auf die Schaltfläche Speichern unter 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\Kaspersky Embedded Systems Security\Uninstall.

   Klicken Sie auf Weiter.

6. Bestätigen Sie im Fenster Bereit zur Deinstallation den Löschvorgang, indem Sie auf die Schaltfläche Entfernen klicken.
7. Klicken Sie im Fenster, das nach Abschluss der Deinstallation geöffnet wird, auf OK.

Kaspersky Embedded Systems Security wird vom geschützten Computer deinstalliert.

Deinstallation der Konsole für Kaspersky Embedded Systems Security

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

Sie können die Programmkonsole mithilfe des Installations-/Deinstallationsassistenten vom Computer deinstallieren.

Nach der Deinstallation der Programmkonsole ist kein Neustart des Computers erforderlich.

► *Um die Programmkonsole zu deinstallieren:*

1. Wählen Sie im Menü **Start** die Option **Alle Programme**.
2. Wählen Sie **Kaspersky Embedded Systems Security**.
3. Wählen Sie Kaspersky Embedded Systems Security **ändern oder löschen**.

   Das Fenster Ändern oder löschen des Assistenten wird geöffnet.
4. Wählen Sie die Variante Entfernen von Programmkomponenten und klicken Sie auf Weiter.
5. Das Fenster Bereit zur Deinstallation wird geöffnet. Klicken Sie auf die Schaltfläche Deinstallieren.

   Das Fenster Die Deinstallation wurde abgeschlossen wird geöffnet.
6. Klicken Sie 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.

In diesem Abschnitt

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

Sie können Kaspersky Embedded Systems Security installieren oder deinstallieren sowie seine Komponenten hinzufügen oder entfernen, indem Sie die Dateien des Installationspakets "\product\ess_x86(x64).msi" aus der Befehlszeile starten und die Installationseinstellungen mithilfe von Schlüsseln angeben.

Sie können den Satz "Administrations-Tools" auf dem geschützten Computer oder auf einem anderen Computer im Netzwerk installieren, damit Sie mit der Programmkonsole lokal oder im Remote-Betrieb arbeiten können. Sie können dazu das Installationspaket "\console\esstools.msi" verwenden.

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

Wenn Sie auf dem geschützten Computer eine der Dateien "\product\ess_x86.msi" oder "\product\ess_x64.msi" ohne Reserveschlüssel starten, wird Kaspersky Embedded Systems Security mit den empfohlenen Installationseinstellungen 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.

Beispiele von Befehlen für die Installation von Kaspersky Embedded Systems Security

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

Starten Sie Dateien auf einem Computer mit der 32-Bit-Version von Microsoft Windows mit dem Suffix x86 des Lieferumfangs. Starten Sie Dateien auf einem Computer mit der 64-Bit-Version von Microsoft Windows mit dem Suffix x64 des Lieferumfangs.

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.exe

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security ohne Benutzerbeteiligung mit den empfohlenen Installationseinstellungen zu installieren:*

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

Sie können Kaspersky Embedded Systems Security mit den folgenden Einstellungen installieren:

- Installieren Sie nur die Komponenten "Echtzeitschutz für Dateien" und "Untersuchung auf Befehl".
- Starten Sie beim Start von Kaspersky Embedded Systems Security nicht den Echtzeitschutz für Dateien.
- Schließen Sie Dateien, die Microsoft Corporation für den Ausschluss aus dem Untersuchungsbereich empfiehlt.

Führen Sie dazu den folgenden Befehl aus:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Beispiele für Befehle zur Installation: eine msi-Datei starten

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security ohne Benutzerbeteiligung mit den empfohlenen Installationseinstellungen zu installieren:*

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

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

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

► *Um Kaspersky Embedded Systems Security zu installieren und vorher die aktiven Prozesse und die Bootsektoren der lokalen Computerlaufwerke zu untersuchen, geben Sie folgenden Befehl ein:*

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

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security*

in den Installationsordner C:\E SS zu installieren:

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

- *Um Kaspersky Embedded Systems Security zu installieren und eine Installations-Log-Datei mit dem Namen ess.log im Ordner zu speichern, in dem die msi-Datei von Kaspersky Embedded Systems Security gespeichert ist, führen Sie folgenden Befehl aus:*

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

- *Führen Sie folgenden Befehl aus, um die Konsole für Kaspersky Embedded Systems Security mit den folgenden Einstellungen zu installieren:*

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

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

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

- *Um einen Programmpatch zu installieren, wenn Kaspersky Embedded Systems Security kennwortgeschützt ist, führen Sie den folgenden Befehl aus:*

```
msiexec /p "<msp Dateiname mit Pfad>" UNLOCK_PASSWORD=<Kennwort>
```

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 Sie während der Installation von Kaspersky Embedded Systems Security die Option Echtzeitschutz nach der Installation des Programms aktivieren auswählen, untersucht das Programm die Objekte des Dateisystems des Servers, wenn darauf zugegriffen wird. Jeden Freitag um 20:00 Uhr führt Kaspersky Embedded Systems Security die Aufgabe zur Untersuchung wichtiger Bereiche aus.

Es wird empfohlen, nach der Installation von Kaspersky Embedded Systems Security folgende Aktionen auszuführen:

- Aufgabe zum Update der Programm-Datenbanken von Kaspersky Embedded Systems Security starten. Nach der Installation untersucht Kaspersky Embedded Systems Security Objekte anhand von Datenbanken, die im Lieferumfang enthalten sind. Es wird empfohlen, die sofort ein Datenbanken-Update für Kaspersky Embedded Systems Security durchzuführen. Dazu müssen Sie die Aufgabe Update der Programm-Datenbanken starten. Danach wird das Datenbanken-Update gemäß dem standardmäßigen Zeitplan stündlich ausgeführt.

  Mit dem folgenden Befehl können Sie beispielsweise die Aufgabe Update der Programm-Datenbanken starten:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

Dabei werden die Datenbanken-Updates für Kaspersky Embedded Systems Security von den Kaspersky-Lab-Update-Servern heruntergeladen. Die Verbindung mit der Update-Quelle erfolgt über einen Proxyserver (Adresse des Proxyservers: proxy.company.com, Port: 8080), wobei für den Serverzugriff die integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung) unter einem Benutzerkonto (Benutzername: inetuser; Kennwort:123456) verwendet wird.

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

► *Um die Aufgabe zur Untersuchung wichtiger Bereiche mithilfe der Befehlszeile auszuführen, führen Sie den folgenden Befehl aus:*

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

Die Komponente "Untersuchung auf Befehl" wird automatisch installiert. Sie müssen sie nicht in der Liste mit den Werten des Schlüssels ADDLOCAL angeben, um die Komponenten von Kaspersky Embedded Systems Security hinzuzufügen oder zu entfernen.

► *Um die Komponente Kontrolle des Programmstarts zu den bereits installierten Komponenten hinzufügen, führen Sie folgenden Befehl aus:*

```
msiexec /i ess.msi ADDLOCAL=Oas,AppCtrl /qn
```

oder

```
\product\setup.exe /s /p "ADDLOCAL=Oas,AppCtrl"
```

Wenn Sie nicht nur Komponenten, die Sie installieren möchten, sondern auch bereits installierte Komponenten angeben, installiert Kaspersky Embedded Systems Security die angegebenen Komponenten neu.

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

```
msiexec /i ess.msi.msi
"ADDLOCAL=Oas,Ods,Ksn,AntiExploit,DevCtrl,Firewall,AntiCryptor,LogInspecto
r,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVProtection,Ram
Disk REMOVE=AppCtrl,Fim" /qn
```

Deinstallation von Kaspersky Embedded Systems Security. Beispiele für Befehle

► *Um Kaspersky Embedded Systems Security vom geschützten Computer zu deinstallieren, führen Sie folgenden Befehl aus:*

```
msiexec /x ess.msi /qn
```

oder

- Für 32-Bit-Betriebssysteme:

```
msiexec /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} /qn
```

► *Um die Konsole für Kaspersky Embedded Systems Security zu deinstallieren, führen Sie folgenden Befehl aus:*

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

oder

- Für 32-Bit-Betriebssysteme:

```
msiexec /x {26E7C356-E535-4434-9AB1-F1EA4E8A70F4} /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec /x {7EC1A40D-52F4-4F8F-93BA-F6E68B152C26} /qn
```

► *Um Kaspersky Embedded Systems Security von einem geschützten Computer zu deinstallieren, auf dem der Kennwortschutz aktiviert ist, führen Sie folgenden Befehl aus:*

- Für 32-Bit-Betriebssysteme:

```
msiexec.exe /x {51AACF7F-421E-40FA-B2B7-FCFE0BACF505} UNLOCK_PASSWORD=*** /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec.exe /x {673F3697-9D6C-4CF4-BB28-478492F45DDC} UNLOCK_PASSWORD=*** /qn
```

Rückgabecodes

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

Tabelle 6. Rückgabecodes

Code	Beschreibung
1324	Der Name des Zielordners enthält unzulässige Zeichen.
25001	Unzureichende Rechte für die Installation von Kaspersky Embedded Systems Security. Um das Programm zu installieren, starten Sie den Installationsassistenten mit den Rechten des lokalen Administrators.
25003	Kaspersky Embedded Systems Security kann nicht auf Computern unter der Verwaltung dieser Version von Microsoft Windows installiert werden. Bitte starten Sie den Installationsassistenten, der für die 64-Bit-Version von Microsoft Windows vorgesehen ist.
25004	Inkompatible Software wurde gefunden. Um die Installation fortzusetzen, löschen Sie die folgenden Programme vom geschützten Computer: <Liste mit inkompatibler Software>.
25010	Der angegebene Pfad kann nicht zum Speichern von Objekten in der Quarantäne verwendet werden.
25011	Der Name des Ordners für Quarantäne-Objekte enthält unzulässige Zeichen.
26251	Die DLL für Leistungsindikatoren konnte nicht geladen werden.
26252	Die DLL für Leistungsindikatoren konnte nicht geladen werden.
27300	Der Treiber kann nicht installiert werden.
27301	Der Treiber kann nicht gelöscht werden.
27302	Die Netzwerkkomponente kann nicht installiert werden. Der obere Grenzwert der unterstützten Anzahl der Geräte zur Filterung wurde erreicht.
27303	Die Antiviren-Datenbanken wurden nicht gefunden.

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

Dieser Abschnitt enthält allgemeine Informationen über die Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center. Er beschreibt ferner, wie man Kaspersky Embedded Systems Security über Kaspersky Security Center installiert und deinstalliert, sowie die Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen.

In diesem Abschnitt

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 Computern mit einheitlichen Einstellungen installiert.

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

Sie können eine Remote-Installationsaufgabe für Kaspersky Embedded Systems Security erstellen, die sich auf eine Auswahl von Computern bezieht, die nicht zur gleichen Administrationsgruppe gehören. Wenn Sie diese Aufgabe erstellen, müssen Sie die Liste der einzelnen Computer 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 Computer zur Gruppe der Administratoren gehören. Dies gilt in allen Fällen unter Ausnahme der folgenden:

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

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

- Alle Computer , 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 Computern 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 Computersätze, die Push-Installationsmethode (Deinstallationsmethode) nützen, muss das Benutzerkonto über die folgende Rechte auf dem Client-Computer 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

Detaillierte Informationen über die Erstellung des Installationspakets und die Aufgabe zur Remote Installation finden Sie im Implementierungshandbuch für Kaspersky Security Center.

Wenn Sie planen, Kaspersky Embedded Systems Security künftig über Kaspersky Security Center zu verwalten, vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Auf dem Computer, auf dem der Kaspersky Security Center-Administrationsserver installiert ist, ist auch das Verwaltungs-Plug-in installiert (Datei "\product\klcfginst.exe" aus dem Lieferumfang von Kaspersky Embedded Systems Security).
- Auf den geschützten Computern ist der Administrationsagent von Kaspersky Security Center installiert. Wenn der Administrationsagent von Kaspersky Security Center nicht auf geschützten Computern installiert ist, können Sie ihn im Rahmen der Remote-Installationsaufgabe zusammen mit Kaspersky Embedded Systems Security installieren.

Außerdem können Sie bestimmte Computer in einer Administrationsgruppe zusammenfassen, um die Schutzeinstellungen später mit Hilfe von Richtlinien und Gruppenaufgaben von Kaspersky Security Center zu verwalten.

► *Gehen Sie folgendermaßen vor, um Kaspersky Embedded Systems Security mithilfe einer Aufgabe zur Remote-Installation zu installieren:*

1. Starten Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in Kaspersky Security Center den Knoten **Erweitert**.
3. Erweitern Sie den untergeordneten Knoten **Remote-Installation**.
4. Klicken Sie im Detailbereich des untergeordneten Knotens **Installationspaket** auf die Schaltfläche **Installationspaket erstellen**.
5. Wählen Sie als Typ des Installationspakets **Installationspaket für ein Kaspersky Lab-Programm erstellen** aus.
6. Geben Sie den Namen des Installationspakets ein.
7. Geben Sie die Datei "ess.kud" aus dem Lieferumfang von Kaspersky Embedded Systems Security als Installationspaketdatei an.

   Das Fenster **Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie** wird geöffnet.
8. Wenn Sie mit den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie die Kontrollkästchen **Bedingungen dieses Endbenutzer-Lizenzvertrags** und Datenschutzrichtlinie, die den Umgang mit Daten beschreibt, um mit der Installation fortzufahren.

   Sie müssen den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie akzeptieren, um fortzufahren.
9. So ändern Sie den Umfang der zu installierenden Komponenten von Kaspersky Embedded Systems Security (siehe Abschnitt "Ändern der Programmkomponenten und Reparieren von Kaspersky Embedded Systems Security " auf Seite 59) und die standardmäßigen Installationseinstellungen (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 42) im Installationspaket:
   a. Erweitern Sie in Kaspersky Security Center den Knoten **Remote-Installation**.
   b. Öffnen Sie im Detailbereich des untergeordneten Knotens **Installationspakete** das Kontextmenü für das neu erstellte Installationspaket von Kaspersky Embedded Systems Security. Wählen Sie dort den Befehl **Eigenschaften**.
   c. Gehen Sie im Fenster **Eigenschaften: <Name des Installationspakets>** im Abschnitt **Einstellungen** wie folgt vor:
      a. Aktivieren Sie in der Einstellungsgruppe **Zu installierende Komponenten** die Kontrollkästchen neben den Namen der Komponenten von Kaspersky Embedded Systems Security, die Sie installieren möchten.
      b. Um einen Zielordner anzugeben, der nicht dem standardmäßigen Ordner entspricht, geben Sie im Feld **Zielordner** den Namen und Pfad des Ordners an.

         Der Pfad des Zielordners kann Umgebungsvariable enthalten. Wenn der angegebene Ordner auf dem Computer nicht existiert, wird er erstellt.

c. Passen Sie in der Optionsgruppe **Erweiterte Einstellungen für die Installation** folgende Einstellungen an:

- **Vor Installation Untersuchung des Computers auf Viren ausführen**.
- **Echtzeitschutz nach der Installation des Programms aktivieren**.
- **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**.

d. **Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen**.

d. Im Dialogfenster **Eigenschaften: <Name des Installationspakets>** auf **OK**.

10. Erstellen Sie im Knoten **Installationspakete** eine Aufgabe zur Remote-Installation von Kaspersky Embedded Systems Security installieren auf den ausgewählten Computern (Administrationsgruppe). Passen Sie die Aufgabeneinstellungen an.

    Detaillierte Informationen über die Erstellung und Konfiguration der Aufgabe zur Remote Installation finden Sie im *Hilfesystem von Kaspersky Security Center*.

11. Führen Sie die Aufgabe zur Remote-Installation von Kaspersky Embedded Systems Security aus.

Kaspersky Embedded Systems Security wird auf den in der Aufgabe angegebenen Computern installiert.

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 Computern zu aktualisieren. Sollte vor der Installation von Kaspersky Embedded Systems Security auf den Servern kein Virenschutzprogramm mit aktiviertem Echtzeitschutz installiert gewesen sein, wird außerdem empfohlen, eine Untersuchung wichtiger Bereiche der Computer durchzuführen.

Wenn Computer, 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. Für die Gruppe der Computer, auf denen Sie Kaspersky Embedded Systems Security installiert haben, eine Aufgabe zum Update der Programm-Datenbanken erstellen. Geben Sie den Kaspersky Security Center-Administrationsserver als Update-Quelle an.
2. Eine Gruppenaufgabe zur Untersuchung auf Befehl mit dem Status Untersuchung wichtiger Bereiche erstellen. Das Programm Kaspersky Security Center bewertet den Sicherheitszustand jedes Computers der Gruppe dann aufgrund der Ergebnisse dieser Gruppe, nicht nach den Ergebnissen der Systemaufgabe Untersuchung wichtiger Bereiche.
3. Erstellen Sie eine neue Richtlinie für die Computergruppe. Deaktivieren Sie in den Richtlinieneinstellungen im Abschnitt Programmeinstellungen den geplanten Start von Systemaufgaben zur Untersuchung auf Befehl und die Aufgaben zum Update der Programm-Datenbanken auf den Computern der Administrationsgruppe in den Einstellungen des Unterabschnitts Start von Systemaufgaben.

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

Installation der Programmkonsole über das Kaspersky Security Center

Detaillierte Informationen über die Erstellung des Installationspakets und der Aufgabe zur Remote-Installation finden Sie im Implementierungshandbuch für Kaspersky Security Center.

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

1. Öffnen Sie in der Verwaltungskonsole für Kaspersky Security Center den Knoten **Erweitert**.
2. Erweitern Sie den untergeordneten Knoten **Remote-Installation**.
3. Klicken Sie im Detailbereich des untergeordneten Knotens Installationspaket auf die Schaltfläche **Installationspaket erstellen**. Während Sie das neue Installationspaket erstellen:
   a. Wählen Sie im Fenster **Assistent für neues Paket** als Pakettyp Installationspaket für angegebene ausführbare Datei **erstellen** aus.
   b. Geben Sie den Namen des neuen Installationspakets ein.
   c. Wählen Sie die Datei "console\setup.exe" aus dem Ordner des Lieferumfangs von Kaspersky Embedded Systems Security aus und aktivieren Sie das Kontrollkästchen **Ganzen Ordner in das Installationspaket kopieren** aus.
   d. Falls erforderlich, ändern Sie im Feld **Starteinstellungen für ausführbare Datei (optional)** mithilfe der Einstellung ADDLOCAL die Auswahl der zu installierenden Komponenten und ändern Sie den Zielordner.

      Um beispielsweise im Ordner C:\KasperskyConsole nur die Programmkonsole zu installieren, nicht aber die Hilfedatei und Dokumentation, verwenden Sie folgende Befehlszeilenoptionen:

      ```
      /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1"
      ```
4. Erstellen Sie im untergeordneten Knoten **Installationspakete** eine Aufgabe zur Remote-Installation der Programmkonsole auf den ausgewählten Computern (Administrationsgruppe). Passen Sie die Aufgabeneinstellungen an.

   Detaillierte Informationen über die Erstellung und Konfiguration der Aufgabe zur Remote Installation finden Sie im Hilfesystem von Kaspersky Security Center.
5. Starten Sie die Aufgabe zur Remote-Installation.

Die Programmkonsole wird auf den in der Aufgabe angegebenen Computern installiert.

Deinstallation von Kaspersky Embedded Systems Security über Kaspersky Security Center

Wenn die Verwaltung von Kaspersky Embedded Systems Security auf Netzwerkcomputern 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 geschützten Computern deinstalliert, auf denen das eingegebene Kennwort mit dem festgelegten Wert übereinstimmt. Kaspersky Embedded Systems Security wird nicht von anderen Computern deinstalliert.

► *Um Kaspersky Embedded Systems Security zu deinstallieren, führen Sie in der Verwaltungskonsole von Kaspersky Security Center folgende Aktionen aus:*

1. Erstellen und starten Sie in der Verwaltungskonsole für Kaspersky Security Center eine Aufgabe zur Deinstallation von Programmen.
2. Wählen Sie in der Aufgabe die Deinstallationsmethode (auf die gleiche Weise, wie die Installationsmethode gewählt wurde; s. vorhergehender Abschnitt) und geben Sie das Benutzerkonto an, unter dem der Administrationsserver auf die Computer zugreifen soll. Sie können Kaspersky Embedded Systems Security nur mit den Standardinstallationseinstellungen deinstallieren (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 42).

Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory

In diesem Abschnitt wird die Installation und Deinstallation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory beschrieben. Er enthält ferner Informationen über die Aktionen, die nach der Installation von Kaspersky Embedded Systems Security über Gruppenrichtlinien ausgeführt werden müssen.

In diesem Abschnitt

Installation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory

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

Die Computer, 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 Computern, 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 dem Domain verfügen.

Um Kaspersky Embedded Systems Security zu installieren, verwenden Sie die Installationspakete `ess`_x86(x64).msi. Um die Programmkonsole zu installieren, verwenden Sie die Installationspakete `ess`tools.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 die msi-Datei, die der Bit-Version (32-Bit oder 64-Bit) des installierten Microsoft Windows-Betriebssystems entspricht, in einem freigegebenen Ordner auf dem Domain-Controller.
2. Speichern Sie die Schlüsseldatei (siehe Abschnitt "Über die Schlüsseldatei" auf Seite 84) im selben öffentlichen Ordner auf dem Domain-Controller.
3. Erstellen Sie im selben öffentlichen Verzeichnis auf dem Domain-Controller die Datei install_props.json mit dem nachfolgend angeführten Inhalt, mit dem Sie Ihre Annahme des Lizenzvertrags und der Datenschutzrichtlinie bestätigen.

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

4. Erstellen Sie auf dem Domain-Controller eine neue Richtlinie für die Gruppe, zu der die Computer 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 Computern 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 Computern wird empfohlen, sofort die Programm-Datenbanken zu aktualisieren und eine Untersuchung wichtiger Bereiche durchzuführen. Sie können diese Aktionen (siehe Abschnitt "Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen" auf Seite 56) 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

Wenn Sie eine Active Directory-Gruppenrichtlinie verwendet haben, um Kaspersky Embedded Systems Security (oder die Programmkonsole) auf der Gruppe von Computern 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 Computern 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 Computern nach deren Neustart und vor der Anmeldung bei Microsoft Windows deinstalliert.

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 und die Funktionen der Untersuchung auf Befehl von Kaspersky Embedded Systems Security zu überprüfen.

In diesem Abschnitt

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 Ihren Rechner beschädigen könnte, er wird jedoch von den meisten Antiviren-Anwendungen der Antiviren-Hersteller als Bedrohung erkannt.

Die Datei, die den Testvirus enthält, heißt eicar.com. Sie können Sie von der EICAR-Website http://www.eicar.org/anti_virus_test_file.htm herunterladen.

Vergewissern Sie sich vor dem Speichern der Datei in einem Ordner auf der Festplatte des Computers, dass 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 oder gefunden 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 verdächtige und möglicherweise infizierte Objekte erkannt werden. Öffnen Sie dazu die Datei mit einem Texteditor, fügen Sie am Anfang der Textzeile in der Datei eines der Präfixe hinzu, die in der Tabelle genannt werden, dann speichern Sie die Datei unter einem neuen Namen, beispielsweise 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 Echtzeitschutz für Dateien und die Aufgaben zur Untersuchung auf Befehl von Kaspersky Embedded Systems Security.

Tabelle 7. 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 oder gefunden** 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 oder gefunden zu und desinfiziert es. Wenn die Desinfektion gelingt, wird der gesamte Text in der Datei durch das Wort "CURE" ersetzt.

Echtzeitschutz 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 bösartigen Code enthalten. Um das zu prüfen, können Sie den EICAR-Testvirus verwenden (siehe Abschnitt "EICAR-Testvirus" auf Seite 77).

► *Um die Funktion Echtzeitschutz zu überprüfen, gehen Sie wie folgt vor:*

1. Laden Sie die Datei eicar.com von der EICAR-Website http://www.eicar.org/anti_virus_test_file.htm herunter. Speichern Sie sie in einem freigegebenen Ordner auf einem lokalen Datenträger eines Computers 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 funktioniert, vergewissern Sie sich, dass sowohl auf dem geschützten Computer als auch auf dem Computer, auf dem Sie die Datei eicar.com gespeichert haben, der Windows Messenger Dienst aktiviert ist.

3. Öffnen Sie die Programmkonsole.
4. Kopieren Sie auf folgende Weise die gespeicherte Datei "eicar.com" auf den lokalen Datenträger des geschützten Computers:
   - Um die Benachrichtigungsfunktion in einem Fenster für Terminaldienste zu testen, kopieren Sie die Datei "eicar.com" auf den Computer, nachdem Sie mithilfe des Dienstprogramms "Remote Desktop Connection" eine Verbindung zum Computer hergestellt haben.
   - Um die Benachrichtigungsfunktion über den Windows Messenger-Dienst zu testen, verwenden Sie die Netzwerkressourcen des Computers, um die Datei "eicar.com" von dem Computer zu kopieren, auf dem Sie sie gespeichert haben.

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

- Die Datei "eicar.com" wird vom geschützten Computer gelöscht.
- In der Programmkonsole wird dem Protokoll der Aufgabenausführung der Status *Kritisch* zugewiesen. Das Protokoll enthält eine neue Zeile mit Informationen über eine Bedrohung in der Datei eicar.com. (Um ein Protokoll der Aufgabenausführung anzuzeigen, erweitern Sie in der Struktur der Programmkonsole den Knoten **Echtzeitschutz für Computer**, wählen Sie die Aufgabe zum **Echtzeitschutz für Dateien** aus, und klicken Sie im Detailbereich des Knotens auf den Link Protokoll öffnen).
  - Auf dem Computer, 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 Computer>\eicar.com für den Computer <Netzwerkname des Servers> um <Uhrzeit für Ereigniseintritt> gesperrt. Grund: Bedrohung erkannt. Virus: EICAR-Test-File. Name des Objektbenutzers: <Benutzername>. Computername des Objektbenutzers: <Netzwerkname des Computers, von dem die Datei kopiert wurde>.`

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

► *Um die Funktion Untersuchung auf Befehl zu überprüfen, gehen Sie wie folgt vor:*

1. Laden Sie die Datei eicar.com von der EICAR-Website http://www.eicar.org/anti_virus_test_file.htm herunter. Speichern Sie sie in einem freigegebenen Ordner auf einem lokalen Datenträger eines Computers 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.
3. Führen Sie folgende Aktionen aus:
   a. Erweitern Sie in der Struktur der Programmkonsole den Knoten Untersuchung auf Befehl.
   b. Wählen Sie den untergeordneten Knoten Untersuchung wichtiger Bereiche aus.
   c. Öffnen Sie auf der Registerkarte Untersuchungsbereich - Einstellungen das Kontextmenü für den Knoten **Netzwerkumgebung** und wählen Sie **Netzwerkdatei hinzufügen**.

d. Tragen Sie den Netzwerkpfad zur Datei eicar.com auf dem Remote-Computer im UNC-Format (Universal Naming Convention) ein.

e. Aktivieren Sie das Kontrollkästchen, um den hinzugefügten Netzwerkpfad in den Untersuchungsbereich aufzunehmen.

f. Starten Sie die Aufgabe Untersuchung wichtiger Bereiche.

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

- Die Datei eicar.com wird von der Festplatte des Computers gelöscht.
- In der Programmkonsole wird dem Protokoll der Aufgabenausführung der Status *Kritisch* zugewiesen. Das Protokoll der Aufgabenausführung für die Untersuchung wichtiger Bereiche enthält eine neue Zeile mit Informationen über eine Bedrohung in der Datei eicar.com. (Um ein Protokoll der Aufgabenausführung aufzurufen, erweitern Sie in der Struktur der Programmkonsole den Knoten Untersuchung auf Befehl, wählen Sie die Aufgabe zur Untersuchung wichtiger Bereiche aus, und klicken Sie im Detailbereich auf den Link Protokoll der Aufgabenausführung öffnen.)

Programmoberfläche

Sie können Kaspersky Embedded Systems Security mithilfe des Verwaltungs-Plug-ins und der lokalen Programmkonsole steuern.

Aktionen in der Benutzeroberfläche der lokalen Programmkonsole werden im Abschnitt "Verwendung der Programmkonsole" (siehe Abschnitt "Verwendung der Konsole für Kaspersky Embedded Systems Security" auf Seite 145) beschrieben.

Die Benutzeroberfläche der Verwaltungskonsole von Kaspersky Security Center wird verwendet, um Aktionen mit dem Verwaltungs-Plug-in durchzuführen. Ausführliche Informationen zur Benutzeroberfläche von Kaspersky Security Center finden Sie in der *Hilfe zu Kaspersky Security Center*.

Lizenzverwaltung für das Programm

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzverwaltung für das Programm zusammenhängen.

In diesem Kapitel

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 können Sie wie folgt einsehen:

- Während der Installation von Kaspersky Embedded Systems Security
- Im Dokument license.txt. Dieses Dokument gehört zum Lieferumfang des Programms.

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, das Ihnen auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

- Nutzung des Programms in Übereinstimmung mit den Bedingungen des Endbenutzer-Lizenzvertrags
- Erhalt von technischem Support

Der Leistungsumfang und die Nutzungsdauer des Programms hängen von der zur Aktivierung des Programms verwendeten Lizenz ab.

Das Programm wird mithilfe einer Schlüsseldatei oder einem Aktivierungscode für eine gekaufte kommerzielle Lizenz aktiviert.

Eine kommerzielle Lizenz ist eine kostenpflichtige Lizenz, die beim Kauf eines Programms zur Verfügung gestellt wird.

Kaspersky Embedded Systems Security umfasst die folgenden kommerziellen Lizenzen:

- Standardlizenz für Kaspersky Embedded Systems Security.
- Erweiterte Lizenz für Kaspersky Embedded Systems Security Compliance Edition. Diese umfasst zwei weitere Komponenten der Systemdiagnose: "Überwachung der Datei-Integrität" und "Protokollanalyse".

Nach Ablauf der kommerziellen Lizenz funktioniert das Programm auch weiterhin, jedoch lediglich mit eingeschränktem Funktionsumfang (so können beispielsweise die Datenbanken von Kaspersky Embedded Systems Security nicht aktualisiert werden). Zur weiteren Nutzung von Kaspersky Embedded Systems Security mit allen Funktionen ist eine Verlängerung der kommerziellen Lizenz erforderlich.

Es wird empfohlen, eine Lizenz rechtzeitig vor dem Ablaufdatum zu verlängern. Nur so lässt sich maximale Sicherheit vor Computerbedrohungen gewährleisten

Stellen Sie sicher, dass der hinzugefügte Reserveschlüssel ein späteres Ablaufdatum besitzt als der aktive Schlüssel.

Über das Lizenzzertifikat

Ein *Lizenzzertifikat* ist ein Dokument, das Ihnen zusammen mit einer Schlüsseldatei bzw. einem Aktivierungscode übergeben wird (sofern zutreffend).

Ein Lizenzzertifikat enthält folgende Lizenzinformationen:

- Bestellnummer;
- Informationen über den Benutzer, dem diese Lizenz gewährt wurde
- Informationen über das Programm, das mit dieser Lizenz aktiviert werden kann
- Maximale Anzahl von Lizenzeinheiten (z. B. Geräte, auf denen das Programm unter dieser Lizenz verwendet werden kann)

- Datum für den Beginn der Lizenzgültigkeit
- Gültigkeitsdauer der Lizenz bzw. Laufzeit 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-Lab-Experten generiert.

Mithilfe einer Schlüsseldatei 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.

Bei Verstößen gegen die Bedingungen des Endbenutzer-Lizenzvertrags kann der Schlüssel von Kaspersky Lab blockiert werden. Wenn ein Schlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um das Programm zu nutzen.

Es gibt einen aktiven Schlüssel und einen Reserveschlüssel.

Aktiver Schlüssel – Schlüssel, der im Augenblick für die Programmausführung verwendet wird. Ein Schlüssel für eine kommerzielle Lizenz oder Testlizenz kann als aktiver Schlüssel hinzugefügt werden. Im Programm kann es nicht mehr als einen aktiven Schlüssel geben.

Reserveschlüssel – Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist. Der Reserveschlüssel wird automatisch aktiviert, wenn die Lizenz abläuft, die zum aktiven Schlüssel gehört. 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 Lab zur Verfügung gestellt wird. Mit der Schlüsseldatei wird ein Schlüssel hinzugefügt. Mit diesem Lizenzschlüssel wird das Programm aktiviert.

Die Schlüsseldatei wird an die E-Mail-Adresse geschickt, die Sie beim Kauf von Kaspersky Embedded Systems Security oder der Anforderung einer Testversion von Kaspersky Embedded Systems Security angegeben haben.

Um das Programm mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Kaspersky-Lab-Aktivierungsservern erforderlich.

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

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

- Wenden Sie sich an den Verkäufer der Lizenz.
- Rufen Sie eine Schlüsseldatei mithilfe Ihres verfügbaren Aktivierungscodes über die Website von Kaspersky Lab (https://keyfile.kaspersky.com/de/) ab.

Über den Aktivierungscode

Ein *Aktivierungscode* ist 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 die E-Mail-Adresse übermittelt, die Sie beim Kauf von Kaspersky Embedded Systems Security angegeben haben.

Sie müssen über einen Internetzugang verfügen, um sich mit den Aktivierungsservern von Kaspersky Lab zu verbinden und das Programm zu aktivieren.

Wenn Sie Ihren Aktivierungscode nach der Installation des Programms verloren haben, kann dieser wiederhergestellt werden. Der Aktivierungscode kann beispielsweise für die Registrierung eines Kaspersky CompanyAccount erforderlich sein. Um Ihren Aktivierungscode wiederherzustellen, wenden Sie sich an den Technischen Support von Kaspersky Lab.

Über die Bereitstellung von Daten

Im Endbenutzer-Lizenzvertrag für Kaspersky Embedded Systems Security, 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 Lab 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

Indem Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren, erklären Sie sich damit einverstanden, die folgenden Daten automatisch an Kaspersky Lab zu senden:

- Um den Mechanismus für den Erhalt 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 (Redirector-Service) - Informationen über das Programm und den Verknüpfungstyp, insbesondere: 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.

Die Bedingungen des Endbenutzer-Lizenzvertrags können Sie wie folgt einsehen:

- Während der Installation des Programms zeigt der Installationsassistent für Kaspersky Embedded Systems Security den vollständigen Text des Endbenutzer-Lizenzvertrags in einem Schritt an, bei dem zur Annahme der Bedingungen des Endbenutzer-Lizenzvertrags aufgefordert wird.
- Jederzeit in der TXT-Datei (license.txt), in der der vollständige Text des Endbenutzer-Lizenzvertrags enthalten ist. Diese Datei ist neben den Programminstallationsdateien Teil des Lieferumfangs von Kaspersky Embedded Systems Security.

Lokale Datenverarbeitung

Während der Ausführung der in diesem Handbuch beschriebenen Hauptfunktionen des Programms verarbeitet und speichert Kaspersky Embedded Systems Security lokal eine Folge von Datentypen auf dem geschützten Computer. Die vom Programm lokal verarbeiteten Daten werden nicht automatisch an Kaspersky Lab oder sonstige Dritthersteller-Systeme gesendet.

Von Kaspersky Embedded Systems Security werden die folgenden Daten lokal verarbeitet und gespeichert:

- Informationen über untersuchte Dateien und erkannte Objekte, z. B. Namen und Attribute von verarbeiteten Dateien und vollständige Pfade zu ihnen auf den untersuchten Medien, angewendete Aktionen auf untersuchte Dateien, Dateitypen, Konten von Benutzern, die Aktionen im geschützten Netzwerk oder auf dem geschützten Computer ausführen, Namen und Daten über untersuchte Geräte, Informationen über Prozesse, die auf dem System ausgeführt werden.
- Informationen über die Aktivität und Einstellungen des Betriebssystems, z. B. Windows-Firewall-Einstellungen, Windows-Ereignisprotokolleinträge, Namen von Benutzerkonten, Starts von ausführbaren Dateien, ihre Prüfsummen und Attribute.

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.

Mit Kaspersky Embedded Systems Security können Sie die Sicherheitsstufe für lokal verarbeitete Daten konfigurieren: Sie können die Benutzerrechte für den Zugriff auf Prozessdaten ändern, die Aufbewahrungsfristen für diese Daten ändern, die Funktionen zur Datenprotokollierung ganz oder teilweise deaktivieren und den Pfad und die Attribute des Ordners in dem die Daten protokolliert werden, ändern.

Detaillierte Informationen zur Konfiguration der Programmfunktionalität, die mit der Datenverarbeitung verbunden ist, und Standardeinstellungen von verarbeiteten Datenspeichern finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

Standardmäßig werden alle vom Programm während der Ausführung lokal verarbeiteten Daten nach dem Entfernen von Kaspersky Embedded Systems Security vom Computer entfernt.

Ausgenommen davon sind Dateien mit Diagnoseinformationen (Protokoll- und Dump-Dateien) und die Anwendungsereignisse im Windows-Ereignisprotokoll. Es wird empfohlen, diese Dateien manuell zu entfernen.

Lesen Sie detaillierte Informationen über die Arbeit mit Dateien, die Diagnosedaten des Programms enthalten, in den entsprechenden Abschnitten dieses Handbuchs.

Sie können Dateien aus dem Windows-Ereignisprotokoll, die Programmereignisse aus Kaspersky Embedded Systems Security enthalten, mithilfe der Standardbordmittel des Betriebssystems löschen.

Lokale Datenverarbeitung mithilfe von Hilfskomponenten des Programms

Das Installationspaket von Kaspersky Embedded Systems Security enthält Hilfskomponenten des Programms, die auf Ihrem Server oder Computer installiert werden können. Dies ist auch dann möglich, wenn Kaspersky Embedded Systems Security nicht installiert ist. Zu diesen Hilfskomponenten zählen folgende:

- Die Programmkonsole. Diese Komponente ist im Paket "Administrations-Tools" von Kaspersky Embedded Systems Security enthalten und wird von einem Microsoft Management Console-Snap-in dargestellt.
- 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 Computer 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: der Name des Computers mit installiertem Kaspersky Embedded Systems Security (IP-Adresse oder Domain-Name), mit dem sich die Programmkonsole das letzte Mal ferngesteuert verbunden hat; im Microsoft Management Console-Snap-in konfigurierte Anzeigeparameter; Daten zum letzten Ordner, in dem der Benutzer über die Programmkonsole Objekte ausgewählt hat (mithilfe des Systemdialogfelds, das durch Klicken auf die Schaltfläche **Durchsuchen** geöffnet wurde). Die Protokolldateien der Programmkonsole können auch die folgenden Daten enthalten: den Namen des Computers mit installiertem Programm Kaspersky Embedded Systems Security, zu dem die Remote-Verbindung hergestellt wurde, sowie den Namen des Benutzerkontos, unter dem die Remote-Verbindung hergestellt wurde.
- Von Kaspersky Embedded Systems Security verarbeitete Daten können vom Verwaltungs-Plug-in verarbeitet und temporär gespeichert werden. Dazu zählen z. B. konfigurierte Parameter der Programmaufgaben und -komponenten, Parameter der Kaspersky Security Center-Richtlinien sowie Daten, die über Netzwerklisten versendet werden.

Die von den Hilfskomponenten verarbeiteten Daten werden nicht automatisch an Kaspersky Lab oder sonstige Dritthersteller-Systeme gesendet.

Standardmäßig werden alle hierbei lokal von den Hilfskomponenten des Programms verarbeiteten Daten nach dem Entfernen dieser Komponenten gelöscht.

Die Ausnahme sind Protokolldateien der Hilfskomponenten des Programms. Es wird empfohlen, diese Dateien manuell zu löschen.

Lesen Sie detaillierte Informationen über die Arbeit mit Dateien, die Diagnosedaten der Hilfskomponenten des Programms enthalten, in den entsprechenden Abschnitten dieses Handbuchs.

Aktivieren des Programms mit einem Lizenzschlüssel

Sie können Kaspersky Embedded Systems Security aktivieren, indem Sie eine Schlüsseldatei anwenden.

Wenn bereits ein Schlüssel als aktiver Schlüssel zu Kaspersky Embedded Systems Security hinzugefügt wurde 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 zu Kaspersky Embedded Systems Security hinzugefügt wurde 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 zu Kaspersky Embedded Systems Security hinzugefügt wurde und Sie einen neuen Schlüssel als aktiven Schlüssel hinzufügen, wird der zuvor hinzugefügte aktive Schlüssel durch den neuen ersetzt; der Reserveschlüssel wird nicht entfernt.

► *Um Kaspersky Embedded Systems Security mithilfe einer Schlüsseldatei zu aktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
2. Betätigen Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** den Link **Schlüssel hinzufügen**.
3. Klicken Sie im folgenden Fenster auf die Schaltfläche **Durchsuchen** und wählen Sie eine Schlüsseldatei mit der Erweiterung key aus.

   Sie können einen Schlüssel auch als Reserveschlüssel hinzufügen. Um einen Schlüssel als Reserveschlüssel hinzuzufügen, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.

4. Klicken Sie auf **OK**.

Die ausgewählte Schlüsseldatei wird angewendet. Informationen über den hinzugefügten Schlüssel stehen im Knoten **Lizenzverwaltung** zur Verfügung.

Aktivieren des Programms mit einem Aktivierungscode

Um das Programm mithilfe eines Aktivierungscodes zu aktivieren, muss der Computer mit dem Internet verbunden sein.

Sie können Kaspersky Embedded Systems Security aktivieren, indem Sie einen Aktivierungscode verwenden.

Bei 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 an Aktivierungen überschritten wird, wird eine entsprechende Benachrichtigung angezeigt. Die Programmaktivierungsprozedur wird unterbrochen und Sie werden aufgefordert, den Technischen Support von Kaspersky Lab zu kontaktieren.

► *Um einen Schlüssel zur Aktivierung von Kaspersky Embedded Systems Security mithilfe eines Aktivierungscodes zu erhalten, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
2. Klicken Sie im Detailbereich 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 Reserveschlüssel verwenden**.
   - Wenn Sie die Lizenzinformationen einsehen möchten, klicken Sie auf die Schaltfläche **Lizenzinformationen anzeigen**. Diese werden daraufhin im Gruppenfeld **Lizenzinformationen** angezeigt.
4. Klicken Sie auf **OK**.

   Kaspersky Embedded Systems Security sendet Informationen über den angewendeten Aktivierungscode an den Aktivierungsserver.

Anzeigen von Informationen über die aktive Lizenz

Informationen zur Lizenzverwaltung anzeigen

Die Informationen zur aktuellen Lizenz werden im Detailbereich des Knotens **Kaspersky Embedded Systems Security** der Programmkonsole angezeigt. Ein Schlüssel kann die folgenden Status haben:

- **Schlüsselstatus wird überprüft** – Kaspersky Embedded Systems Security überprüft die angewendete Schlüsseldatei bzw. den Aktivierungscode und wartet auf die Antwort zum aktuellen Lizenzstatus.
- **Gültigkeitsdauer der Lizenz** – Kaspersky Embedded Systems Security bleibt bis zum angegebenen Zeitpunkt aktiviert. Der Schlüsselstatus ist in folgenden Fällen gelb hervorgehoben:
  - Die Restlaufzeit der Lizenz beträgt noch 14 Tage, und es wurde kein Schlüssel als Reserve hinzugefügt.
  - Der hinzugefügte Schlüssel befindet sich in der schwarzen Liste und seine Blockierung steht unmittelbar bevor
- **Die Lizenz ist abgelaufen!** – Kaspersky Embedded Systems Security ist nicht aktiviert, da die Lizenz abgelaufen ist. Der Status ist rot hervorgehoben.
- **Verstoß gegen den Endbenutzer-Lizenzvertrag** – Kaspersky Embedded Systems Security ist nicht aktiviert, da die Bedingungen des Endbenutzer-Lizenzvertrags verletzt wurden (siehe Abschnitt "Über den Endbenutzer-Lizenzvertrag" auf S. 82). Der Status ist rot hervorgehoben.
- **Der Schlüssel wurde auf die schwarze Liste gesetzt** – Der hinzugefügte Schlüssel ist blockiert und wurde durch Kaspersky Lab auf die schwarze Liste gesetzt, beispielsweise wenn der Schlüssel durch Unbefugte zur illegalen Programmaktivierung verwendet wurde. Der Status ist rot hervorgehoben.

Anzeigen von Informationen über die aktive Lizenz

► *Um Informationen über die aktive Lizenz anzuzeigen,*

Öffnen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.

Im Ergebnisbereich des Knotens **Lizenzverwaltung** werden allgemeine Informationen über die aktive Lizenz angezeigt (s. Tabelle unten).

Tabelle 8. Allgemeine Lizenzinformationen im Knoten Lizenzverwaltung

Feld	Beschreibung
Aktivierungscode	Der Aktivierungscode. Dieses Feld wird ausgefüllt, wenn Sie das Programm mithilfe eines Aktivierungscodes aktivieren.
Aktivierungsstatus	Informationen über den Aktivierungsstatus des Programms. Die Spalte **Aktivierung** des Detailbereichs des Knotens **Lizenzverwaltung** kann die folgenden Statusvarianten haben: • **Übernommen** – wenn Sie das Programm mithilfe eines Aktivierungscodes oder einer Schlüsseldatei aktiviert haben. **Aktivierung** – wenn Sie einen Aktivierungscode für die Aktivierung des Programms verwendet haben und der Aktivierungsprozess noch nicht abgeschlossen ist. Der Status ändert sich zu *Übernommen*, sobald die Aktivierung des Programms abgeschlossen ist und die Inhalte des Detailbereichs des Knotens aktualisiert wurden. • **Fehler beim Aktivieren** – wenn das Programm nicht aktiviert werden konnte. Die Ursache für das Fehlschlagen der Aktivierung finden Sie im Protokoll der Aufgabenausführung.
Schlüssel	Der Schlüssel, der zur Aktivierung des Programms verwendet wurde.
Lizenztyp	Lizenztyp: kommerziell oder Probe
Gültig bis	Gültigkeitsdauer der mit dem aktiven Schlüssel verknüpften Lizenz.
Status des Aktivierungscodes oder Schlüssels	Status des Aktivierungscodes oder des Schlüssels: aktiver oder Reserveschlüssel.

► *Um detaillierte Informationen über die aktuelle Lizenz anzuzeigen,*

wählen Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** im Kontextmenü der Zeile mit den Lizenzinformationen, die Sie anzeigen möchten, den Punkt **Eigenschaften** aus.

Im Fenster **Eigenschaften:<Status des Aktivierungscodes oder Schlüssels>** auf der Registerkarte **Allgemein** werden ausführliche Informationen über die aktive Lizenz angezeigt, auf der Registerkarte **Erweitert** werden Informationen über den Käufer und Kontaktinformationen von Kaspersky Lab oder dem Partner angezeigt, bei dem Sie Kaspersky Embedded Systems Security gekauft haben (siehe Tabelle unten).

Tabelle 9. Ausführliche Lizenzinformationen im Fenster Eigenschaften: <Status des Aktivierungscodes bzw. Schlüssels>

Feld	Beschreibung
Registerkarte Allgemein	
Schlüssel	Der Schlüssel, der zur Aktivierung des Programms verwendet wurde.
Schlüssel hinzugefügt am	Datum, an dem der Schlüssel zum Programm hinzugefügt wurde.
Lizenztyp	Lizenztyp: kommerziell oder Probe

Feld	Beschreibung
Läuft ab in (Tagen)	Anzahl der Tage bis zum Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Gültig bis	Gültigkeitsdauer der mit dem aktiven Schlüssel verknüpften Lizenz. Wenn Sie das Programm auf Basis eines unbefristeten Abonnements aktivieren, wird der Feldwert *Unbegrenzt* angezeigt. Wenn Kaspersky Embedded Systems Security die Gültigkeitsdauer der Lizenz nicht ermitteln kann, ist der Wert *Unbekannt*.
Programm	Name des Programms, das mit der Schlüsseldatei oder dem Aktivierungscode aktiviert wurde.
Nutzungsbeschränkung für Schlüssel	Beschränkungen für die Nutzung des Schlüssels (falls vorhanden).
Verfügbarkeit des Technischen Supports	Informationen darüber, ob Kaspersky Lab oder einer seiner Partner dem Kunden technischen Support gemäß den Lizenzbedingungen leistet.
Registerkarte Erweitert	
Lizenzinformationen	Aktuelle Lizenznummer.
Support-Informationen	Kontaktinformationen von Kaspersky Lab oder seinem Partner, der für den technischen Support verantwortlich ist. Dieses Feld kann leer sein, wenn kein technischer Support geleistet wird.
Informationen zum Benutzer	Informationen zum Eigentümer der Lizenz: ein Kundenname und der Name des Unternehmens, für das die Lizenz erworben wurde.

Funktionsbeschränkungen bei Ablauf der Lizenz

Wenn die aktive Lizenz abläuft, gelten folgende Beschränkungen für die Funktionskomponenten:

- Alle Aufgaben mit Ausnahme von Echtzeitschutz für Dateien, Untersuchung auf Befehl und Integritätsprüfung für Programme werden gestoppt
- Sie können mit Ausnahme von Echtzeitschutz für Dateien, Untersuchung auf Befehl und Integritätsprüfung für Programme keine Aufgaben starten. Diese Aufgaben werden mithilfe der alten Antiviren-Datenbanken weiter ausgeführt
- Die Funktionalität der Exploit-Prävention wird begrenzt:
  - Prozesse werden bis zu ihrem Neustart geschützt
  - Es können keine neuen Prozesse zum Schutzbereich hinzugefügt werden

Andere Funktionen (Datenverwaltung, Protokolle, Diagnoseinformationen) stehen weiterhin zur Verfügung.

Verlängern der Lizenz

Standardmäßig werden Sie 14 Tage vor dem Ablaufdatum der Lizenzgültigkeit von Kaspersky Embedded Systems Security über den baldigen Ablauf der Lizenz benachrichtigt. In diesem Fall wird der Status **Gültigkeitsdauer der Lizenz** im Detailbereich des Knotens **Kaspersky Embedded Systems Security** gelb hervorgehoben.

Sie können die Lizenz schon vor dem Ablaufdatum verlängern, indem Sie eine Schlüsseldatei oder einen Aktivierungscode als Reserve hinzufügen. So vermeiden Sie, dass der Computer nach Ablauf der Laufzeit der aktuellen Lizenz bis zur Aktivierung des Programms mit der neuen Lizenz ungeschützt ist.

► *Um die Lizenz zu verlängern, gehen Sie wie folgt vor:*

1. Kaufen Sie einen neuen Aktivierungscode oder eine Schlüsseldatei für das Programm.
2. Öffnen 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 eines Reserveschlüssels verlängern möchten:
     a. Klicken Sie auf den Link **Schlüssel hinzufügen**.
     b. Klicken Sie im erscheinenden Fenster auf die Schaltfläche **Durchsuchen** und wählen Sie die neue Schlüsseldatei mit der Erweiterung key aus.
     c. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel 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 Reserveschlüssel verwenden**.

   Für die Übernahme des Aktivierungscodes ist eine Internetverbindung erforderlich.
4. Klicken Sie auf **OK**.

Der Reserveschlüssel wird hinzugefügt, und nach Ablauf des aktiven Schlüssels für Kaspersky Embedded Systems Security automatisch aktiviert.

Schlüssel löschen

Sie können den hinzugefügten Schlüssel entfernen.

Wenn in Kaspersky Embedded Systems Security ein Reserveschlüssel hinzugefügt wurde und Sie den aktiven Schlüssel entfernen, wird der Reserveschlüssel automatisch zum aktiven Schlüssel.

Wenn Sie den Reserveschlüssel entfernen, können Sie ihn durch die erneute Anwendung der Schlüsseldatei wiederherstellen.

► *Um einen hinzugefügten Schlüssel zu entfernen, gehen Sie wie folgt vor:*

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.

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 Computer oder einer Gruppe von Computern installierte Programm verwaltet wird.

In diesem Kapitel

Verwalten von Kaspersky Embedded Systems Security über Kaspersky Security Center

Sie können mehrere Computer, auf denen Kaspersky Embedded Systems Security installiert ist und die Teil einer Administrationsgruppe sind, mithilfe des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security zentral verwalten. Ferner erlaubt Kaspersky Security Center ein separates Anpassen der Betriebseinstellungen für jeden in der Administrationsgruppe enthaltenen Computer.

Die *Administrationsgruppe* wird seitens Kaspersky Security Center manuell erstellt und beinhaltet mehrere Computer, 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 einen Computer sind nicht verfügbar, wenn die Arbeit von Kaspersky Embedded Systems Security auf diesem Computer durch die aktive Richtlinie von Kaspersky Security Center kontrolliert wird.

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 Computergruppen 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: <Computername>** von Kaspersky Security Center konfiguriert wurden.

  Mithilfe von Richtlinien können Sie allgemeine Programmeinstellungen, Einstellungen für Aufgaben zum Echtzeitschutz, Einstellungen für die Überwachung der Desktop-Aktivitäten, Einstellungen zum Start von Systemaufgaben nach Zeitplan und Einstellungen für die Verwendung von Profilen anpassen.

- **Mithilfe der Gruppenaufgaben von Kaspersky Security Center**. Die Gruppenaufgaben von Kaspersky Security Center ermöglichen die Konfiguration allgemeiner Einstellungen für Aufgaben mit einer begrenzten Ausführungsdauer für Computergruppen per Fernzugriff.

- Mithilfe von Gruppenaufgaben können Sie das Programm aktivieren sowie die Einstellungen der Aufgaben zur Untersuchung auf Befehl, der Update-Aufgaben und der Aufgaben zum automatischen 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 allgemeiner Einstellungen für Aufgaben mit begrenzter Ausführungsdauer und für Computer, die nicht einer der erstellten Administrationsgruppen zugeordnet sind, per Fernzugriff.

- **Mithilfe des Konfigurationsfensters für einen einzelnen Computer**. Im Fenster **Eigenschaften: <Computername>** können Sie die Aufgabeneinstellungen für einen einzelnen Computer, der einer Administrationsgruppe zugeordnet ist, per Fernzugriff konfigurieren. Sie können sowohl allgemeine Programmeinstellungen als auch Einstellungen für alle Aufgaben von Kaspersky Embedded Systems Security anpassen, wenn der ausgewählte Computer sich nicht unter der Verwaltung der aktiven Richtlinie von Kaspersky Security Center befindet.

Kaspersky Security Center ermöglicht die Anpassung der Programmeinstellungen, der erweiterten Optionen und erlaubt Ihnen mit Berichten und Benachrichtigungen zu arbeiten. Sie können diese Einstellungen sowohl für Gruppen von Computern als auch für einen einzelnen Computer anpassen.

Programmeinstellungen verwalten

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

In diesem Kapitel

Verwalten von Kaspersky Embedded Systems Security über Kaspersky Security Center

Sie können mehrere Computer, auf denen Kaspersky Embedded Systems Security installiert ist und die Teil einer Administrationsgruppe sind, mithilfe des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security zentral verwalten. Ferner erlaubt Kaspersky Security Center ein separates Anpassen der Betriebseinstellungen für jeden in der Administrationsgruppe enthaltenen Computer.

Die *Administrationsgruppe* wird seitens Kaspersky Security Center manuell erstellt und beinhaltet mehrere Computer, 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 einen Computer sind nicht verfügbar, wenn die Arbeit von Kaspersky Embedded Systems Security auf diesem Computer durch die aktive Richtlinie von Kaspersky Security Center kontrolliert wird.

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 Computergruppen 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: <Computername>** von Kaspersky Security Center konfiguriert wurden.

  Mithilfe von Richtlinien können Sie allgemeine Programmeinstellungen, Einstellungen für Aufgaben zum Echtzeitschutz, Einstellungen für die Überwachung der Desktop-Aktivitäten, Einstellungen zum Start von Systemaufgaben nach Zeitplan und Einstellungen für die Verwendung von Profilen anpassen.

- **Mithilfe der Gruppenaufgaben von Kaspersky Security Center**. Die Gruppenaufgaben von Kaspersky Security Center ermöglichen die Konfiguration allgemeiner Einstellungen für Aufgaben mit einer begrenzten Ausführungsdauer für Computergruppen per Fernzugriff.

- Mithilfe von Gruppenaufgaben können Sie das Programm aktivieren sowie die Einstellungen der Aufgaben zur Untersuchung auf Befehl, der Update-Aufgaben und der Aufgaben zum automatischen 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 allgemeiner Einstellungen für Aufgaben mit begrenzter Ausführungsdauer und für Computer, die nicht einer der erstellten Administrationsgruppen zugeordnet sind, per Fernzugriff.
- **Mithilfe des Konfigurationsfensters für einen einzelnen Computer**. Im Fenster **Eigenschaften: <Computername>** können Sie die Aufgabeneinstellungen für einen einzelnen Computer, der einer Administrationsgruppe zugeordnet ist, per Fernzugriff konfigurieren. Sie können sowohl allgemeine Programmeinstellungen als auch Einstellungen für alle Aufgaben von Kaspersky Embedded Systems Security anpassen, wenn der ausgewählte Computer sich nicht unter der Verwaltung der aktiven Richtlinie von Kaspersky Security Center befindet.

Kaspersky Security Center ermöglicht die Anpassung der Programmeinstellungen, der erweiterten Optionen und erlaubt Ihnen mit Berichten und Benachrichtigungen zu arbeiten. Sie können diese Einstellungen sowohl für Gruppen von Computern als auch für einen einzelnen Computer anpassen.

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Öffnen der allgemeinen Einstellungen über die Richtlinie

► *Um die Programmeinstellungen von Kaspersky Embedded Systems Security über die Richtlinie zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Richtlinien: <Name der Richtlinie>** den Abschnitt **Programmeinstellungen** aus.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt der Einstellung, die Sie konfigurieren möchten.

Öffnen der allgemeinen Einstellungen im Eigenschaftenfenster des Programms

► *Um das Eigenschaftenfenster von Kaspersky Embedded Systems Security für einen einzelnen Computer zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des geschützten Computers.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Computers aus.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
5. Wählen Sie im Abschnitt **Programme** die Option **Kaspersky Embedded Systems Security** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster mit **Programmeinstellungen für Kaspersky Embedded Systems Security** wird geöffnet.
7. Wählen Sie den Abschnitt **Programmeinstellungen** aus.

Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center

Sie können die allgemeinen Einstellungen von Kaspersky Embedded Systems Security für Computergruppen und für einen einzelnen Computer über Kaspersky Security Center konfigurieren.

In diesem Abschnitt

Skalierbarkeit und Schnittstelle in Kaspersky Security Center anpassen

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

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Skalierbarkeit und Oberfläche** auf die Schaltfläche **Einstellungen**.
5. Konfigurieren Sie im Fenster **Erweiterte Programmeinstellungen** auf der Registerkarte **Allgemein** die folgenden Einstellungen:
   - Passen Sie im Abschnitt **Skalierbarkeitseinstellungen** die Einstellungen an, durch die die Anzahl der von Kaspersky Embedded Systems Security verwendeten Arbeitsprozesse festgelegt wird:
     - **Skalierbarkeitseinstellungen automatisch ermitteln**

       Die Zahl der verwendeten Prozesse wird von Kaspersky Embedded Systems Security automatisch geregelt.

       Dieser Wert gilt als Standard.
     - **Anzahl der Arbeitsprozesse manuell angeben**

       Die Zahl der aktiven Arbeitsprozesse wird von Kaspersky Embedded Systems Security gemäß den angegebenen Werten geregelt.
       - **Maximale Anzahl aktiver Prozesse**

         Die maximale Anzahl der von Kaspersky Embedded Systems Security verwendeten Prozesse. Das Eingabefeld ist verfügbar, wenn die Variante **Anzahl der Arbeitsprozesse manuell angeben** ausgewählt wurde.
       - **Anzahl der Prozesse für den Echtzeitschutz.**

         Maximale Anzahl der Prozesse, die von den Komponenten der Aufgaben zum Echtzeitschutz verwendet werden. Das Eingabefeld ist verfügbar, wenn die Variante **Anzahl der Arbeitsprozesse manuell angeben** ausgewählt wurde.
       - **Anzahl der Prozesse für im Hintergrund ausgeführte Untersuchungen auf Befehl.**

         Die maximale Anzahl von Prozessen, die durch die Komponente der Untersuchung auf Befehl bei der Ausführung der Aufgaben zur Untersuchung auf Befehl im Hintergrundmodus verwendet werden. Das Eingabefeld ist verfügbar, wenn die Variante **Anzahl der Arbeitsprozesse manuell angeben** ausgewählt wurde.
   - Passen Sie im Block **Interaktion mit dem Benutzer** die Anzeige des Programmsymbols im Infobereich der Taskleiste an: Deaktivieren oder aktivieren Sie das Kontrollkästchen **Symbol im Infobereich der Taskleiste anzeigen**.
6. Wählen Sie auf der Registerkarte **Hierarchischer Speicher** die Option für den Zugriff auf den hierarchischen Speicher aus.
7. Klicken Sie auf **OK**.

Die vorgenommenen Programmeinstellungen werden gespeichert.

Sicherheitseinstellungen in Kaspersky Security Center anpassen

► *Um die Sicherheitsparameter manuell anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   > Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Sicherheit** auf die Schaltfläche **Einstellungen**.
5. Konfigurieren Sie im Fenster **Sicherheitseinstellungen** die folgenden Einstellungen:
   - Passen Sie im Abschnitt **Einstellungen für Zuverlässigkeit** die Wiederherstellungseinstellungen für die Aufgaben von Kaspersky Embedded Systems Security bei Störungen oder einer fehlerhaften Beendigung des Programms an.
     - **Wiederherstellen von Aufgaben ausführen**

       Dieses Kontrollkästchen aktiviert oder deaktiviert die Wiederherstellung der Aufgaben von Kaspersky Embedded Systems Security nach einer Störung bzw. einer fehlerhaften Beendigung des Programms.

       Ist das Kontrollkästchen aktiviert, stellt Kaspersky Embedded Systems Security die Aufgaben von Kaspersky Embedded Systems Security nach einer Störung oder einer fehlerhaften Beendigung automatisch wieder her.

       Ist das Kontrollkästchen deaktiviert, stellt Kaspersky Embedded Systems Security die Aufgaben von Kaspersky Embedded Systems Security nach einer Störung oder einer fehlerhaften Beendigung nicht wieder her.

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
     - **Maximale Anzahl der Wiederherstellungsversuche für Aufgaben zur Untersuchung auf Befehl**

       Die Anzahl versuchter Wiederherstellungen der Aufgaben zur Untersuchung auf Befehl nach einer Störung von Kaspersky Embedded Systems Security. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Wiederherstellen von Aufgaben ausführen** aktiviert ist.

- Legen Sie im Abschnitt **Aktionen beim Wechsel in den USV-Akkubetrieb** die von Kaspersky Embedded Systems Security beim Wechsel auf eine USV-Quelle erzeugte Belastungsbeschränkung auf den Computer fest:
  - **Aufgaben zur Untersuchung nach Zeitplan nicht starten**

    Dieses Kontrollkästchen aktiviert/deaktiviert beim Wechsel des Computers auf eine USV-Quelle das Starten der Aufgaben zur Untersuchung nach Zeitplan bis zur Wiederherstellung des Standardbetriebs.

    Ist dieses Kontrollkästchen aktiviert, startet Kaspersky Embedded Systems Security beim Wechsel auf eine USV-Quelle bis zur Wiederherstellung des Standardbetriebs keine Aufgaben zur Untersuchung nach Zeitplan.

    Ist das Kontrollkästchen deaktiviert, startet Kaspersky Embedded Systems Security die Aufgaben zur Untersuchung nach Zeitplan unabhängig vom Stromversorgungsmodus.

    Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
  - **Laufende Untersuchungsaufgaben anhalten**

    Dieses Kontrollkästchen aktiviert / deaktiviert das Beenden gestarteter Untersuchungsaufgaben beim Wechsel des Computers auf eine USV-Quelle.

    Ist dieses Kontrollkästchen aktiviert, hält Kaspersky Embedded Systems Security beim Wechsel des Computers auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben an.

    Ist dieses Kontrollkästchen deaktiviert, setzt Kaspersky Embedded Systems Security beim Wechsel des Computers auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben fort.

    Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
- Legen Sie im Abschnitt **Einstellungen für den Kennwortschutz** das Kennwort für den Schutz des Zugriffs auf die Funktionen von Kaspersky Embedded Systems Security fest.

6. Klicken Sie auf **OK**.

Die konfigurierten Sicherheitseinstellungen werden gespeichert.

Verbindungseinstellungen über Kaspersky Security Center anpassen

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

► *Zum Einrichten der Verbindungseinstellungen gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).

- Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

  Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Verbindungen** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Verbindungseinstellungen** wird geöffnet.

5. Konfigurieren Sie im Fenster **Verbindungseinstellungen** die folgenden Parameter:

   - Nehmen Sie im Abschnitt **Proxyserver-Einstellungen** die Einstellungen für die Verwendung eines Proxyservers vor:

     - **Keinen Proxyserver verwenden**

       Ist diese Einstellung ausgewählt, verwendet Kaspersky Embedded Systems Security keinen Proxyserver zur Verbindungsaufnahme mit den KSN-Diensten, sondern stellt die Verbindung direkt her.

     - **Einstellungen des angegebenen Proxyservers verwenden**

       Ist diese Einstellung ausgewählt, verwendet Kaspersky Embedded Systems Security für die Verbindungsaufnahme mit KSN die manuell eingegebenen Proxyserver-Einstellungen.

     - IP-Adresse oder symbolischer Name des Proxyservers und Portnummer.

     - **Für lokale Adressen keinen Proxyserver verwenden**.

       Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Nutzung eines Proxyservers für Anfragen an Computer aus dem Netzwerk, zu dem auch der Computer gehört, auf dem Kaspersky Embedded Systems Security installiert ist.

       Ist das Kontrollkästchen aktiviert, wird aus dem Netzwerk, zu dem der Computer mit installiertem Kaspersky Embedded Systems Security gehört, direkt auf Computer zugegriffen. Es wird kein Proxyserver verwendet.

       Wenn das Kontrollkästchen deaktiviert ist, wird für den Zugriff auf die lokalen Computer der Proxyserver verwendet.

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Legen Sie im Abschnitt **Einstellungen für die Authentifizierung auf dem Proxyserver** die Authentifizierungseinstellungen fest:

     - Wählen Sie in der Dropdown-Liste die Einstellungen für die Authentifizierung aus.

       - **Authentifizierung nicht verwenden** – es erfolgt keine Authentizitätsprüfung. Dieser Modus gilt als Standard.

       - **NTLM-Authentifizierung verwenden** – Authentizitätsprüfung mithilfe des von Microsoft entwickelten NTLM-Protokolls zur Netzwerkauthentifizierung.

- **NTLM-Authentifizierung mit Benutzername und Kennwort verwenden** – Authentizitätsprüfung mithilfe des von Microsoft entwickelten NTLM-Protokolls zur Netzwerkauthentifizierung sowie des Benutzernamens und Kennworts.
- **Benutzername und Kennwort verwenden** – Authentifizierung mithilfe des Benutzernamens und Kennworts.

- Geben Sie bei Bedarf Benutzername und Kennwort an.

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

6. Klicken Sie auf **OK**.

Die vorgenommenen Verbindungseinstellungen werden gespeichert.

Zeitplan für den Start von lokalen Systemaufgaben anpassen

Mithilfe von Richtlinien können Sie den Start von lokalen Systemaufgaben zur Untersuchung auf Befehl und zum Update nach dem lokal auf jedem Computer der Administrationsgruppe festgelegten folgenden Zeitplan erlauben oder verbieten:

- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie verboten ist, werden solche Aufgaben nicht auf dem lokalen Computer nach 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 von Quarantäne-Objekten, Untersuchung beim Hochfahren des Betriebssystems, Integritätsprüfung für Programme.
- Aufgaben zum Update: Update der Programm-Datenbanken, Update der Programm-Module und Update-Verteilung.

Wenn Sie einen geschützten Computer aus der Administrationsgruppe ausschließen, wird der Zeitplan der Systemaufgaben automatisch aktiviert.

► *Gehen Sie wie folgt vor, um den Start der Systemaufgaben von Kaspersky Embedded Systems Security nach Zeitplan in einer Richtlinie zu erlauben oder zu verbieten:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole den Knoten **Verwaltete Geräte**, klappen Sie die entsprechende Gruppe auf und öffnen Sie im Ergebnisfenster die Registerkarte **Richtlinien**.
2. Wählen Sie auf der Registerkarte **Richtlinie** im Kontextmenü der Richtlinie, mit deren Hilfe Sie den geplanten Start von Systemaufgaben für Kaspersky Embedded Systems Security auf der Computergruppe konfigurieren möchten, das Element **Eigenschaften**.
3. Öffnen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt Programmeinstellungen. Klicken Sie im Abschnitt Start von Systemaufgaben auf die Schaltfläche Einstellungen und gehen Sie wie folgt vor:
   - Aktivieren Sie die Kontrollkästchen Start von Aufgaben zur Untersuchung auf Befehl zulassen und Start von Aufgaben zum Update und zur Update-Verteilung zulassen, um den Start der angeführten Aufgaben nach Zeitplan zu erlauben.
   - Deaktivieren Sie die Kontrollkästchen Start von Aufgaben zur Untersuchung auf Befehl zulassen und Start von Aufgaben zum Update und zur Update-Verteilung zulassen, um den Start der angeführten Aufgaben nach Zeitplan zu verbieten.

   Das Aktivieren oder Deaktivieren der Kontrollkästchen beeinflusst nicht die Starteinstellungen der lokalen benutzerdefinierten Aufgaben des angegebenen Typs.
4. Vergewissern Sie sich, dass die Richtlinie, die Sie anpassen, aktiv ist und für die ausgewählte Gruppe von Computern übernommen wurde.
5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für den Start nach Zeitplan werden für die ausgewählten Aufgaben übernommen.

Quarantäne- und Backup-Einstellungen in Kaspersky Security Center anpassen

► *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 Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   > Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **Zusätzlich** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Speicher**.
5. Passen Sie im Fenster **Speicher** auf der Registerkarte **Backup** die folgenden Backup-Einstellungen an:
   - Um einen Backup-Ordner anzugeben, wählen Sie im Feld **Backup-Ordner** den entsprechenden Ordner auf einem Laufwerk des geschützten Computers aus oder geben Sie seinen vollständigen Pfad an.
   - Um die maximale Größe des Backups festzulegen, aktivieren Sie das Kontrollkästchen **Maximale Größe des Backups (MB)** und tragen Sie im Eingabefeld den entsprechenden Wert in MB ein.
   - Um einen Grenzwert für freien Speicherplatz im Backup festzulegen, definieren Sie den Wert der Einstellung **Maximale Größe des Backups (MB)**, aktivieren Sie das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz (MB)** und geben Sie den Mindestwert für den freien Speicher im Backup in MB an.
   - Um einen anderen Wiederherstellungsordner anzugeben, wählen Sie im Abschnitt **Einstellungen für die Wiederherstellung von Objekten** den entsprechenden Ordner auf einem lokalen Laufwerk des geschützten Computers aus oder geben Sie im Feld **Ordner für die Wiederherstellung von Objekten** den Namen und vollständigen Pfad des Ordners an.
6. Passen Sie im Fenster **Speicher** auf der Registerkarte **Quarantäne** die folgenden Quarantäne-Einstellungen an:
   - Wenn Sie den Quarantäneordner ändern möchten, geben Sie im Eingabefeld **Quarantäneordner** den vollständigen Ordnerpfad auf einem lokalen Laufwerk des geschützten Computers an.
   - Wenn Sie die maximale Größe der Quarantäne festlegen möchten, aktivieren Sie das Kontrollkästchen **Maximale Größe der Quarantäne (MB)** und tragen Sie im Eingabefeld den Wert in MB ein.
   - Wenn Sie die minimale Größe für den freien Speicherplatz in der Quarantäne festlegen möchten, aktivieren Sie die Kontrollkästchen **Maximale Größe der Quarantäne (MB)** und **Grenzwert für verfügbaren Speicherplatz (MB)** und tragen Sie im Eingabefeld den Grenzwert in Megabyte ein.
   - Wenn Sie den Ordner ändern möchten, in dem Objekte aus der Quarantäne wiederhergestellt werden, geben Sie im Eingabefeld **Ordner für die Wiederherstellung von Objekten** den vollständigen Pfad zum Ordner auf einem lokalen Laufwerk des geschützten Computers an.
7. Klicken Sie auf **OK**.

Die vorgenommenen Quarantäne und Backup-Einstellungen werden gespeichert.

Über die Konfiguration von Protokollen und Benachrichtigungen

In der Verwaltungskonsole von Kaspersky Security Center können Sie die Benachrichtigung an den Administrator und an die Benutzer für folgende Ereignisse anpassen, die mit der Arbeit von Kaspersky Embedded Systems Security und dem Status des Antiviren-Schutzes für den geschützten Computer zusammenhängen:

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerks, die auf den geschützten Computer zugreifen, sowie die Terminalbenutzer des Computers können Informationen über Ereignisse des Typs *Objekt gefunden* erhalten.

Sie können die Ereignisbenachrichtigungen für Kaspersky Embedded Systems Security entweder für einen Computer im Fenster **Eigenschaften: <Computername>**oder für eine Computergruppe im Fenster **Eigenschaften: <Name der Richtlinie>** der ausgewählten Administrationsgruppe anpassen.

Auf der Registerkarte **Ereignisbenachrichtigungen** oder im Fenster **Benachrichtigungen anpassen** können Sie die folgenden Benachrichtigungstypen anpassen:

- Auf der Registerkarte **Ereignisbenachrichtigungen** (Standard-Registerkarte des Programms Kaspersky Security Center) können Sie die Benachrichtigungen an den Administrator anpassen, die über Ereignisse der ausgewählten Typen erfolgen sollen. Ausführliche Informationen über Benachrichtigungsmethoden finden Sie im *Hilfesystem von Kaspersky Security Center*.
- Im Fenster **Benachrichtigungen anpassen** können Sie Benachrichtigungen sowohl für den Administrator als auch für Benutzer einstellen.

Die Benachrichtigungen über bestimmte Ereignistypen können Sie nur entweder auf der Registerkarte oder im Fenster konfigurieren, bei anderen Ereignistypen ist dies sowohl auf der Registerkarte als auch im Fenster möglich.

Wenn Sie die Benachrichtigungen über Ereignisse eines Typs mittels derselben Methode sowohl auf der Registerkarte **Ereignisbenachrichtigungen** als auch im Fenster **Benachrichtigungen anpassen** einstellen, erhält der Systemadministrator Benachrichtigungen über diese Ereignisse durch die angegebene Methode zweimal.

In diesem Abschnitt

Protokolleinstellungen anpassen

► *Um die Protokolle für Kaspersky Embedded Systems Security anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Block **Protokolle der Aufgabenausführung** auf die Schaltfläche **Einstellungen**.
5. Passen Sie im Fenster **Einstellungen für Protokolle** die folgenden Eigenschaften für Kaspersky Embedded Systems Security gemäß Ihren Anforderungen an:
   - Passen Sie die Genauigkeitsstufe der Ereignisse in Protokollen an. Gehen Sie hierzu wie folgt vor:
     a. Wählen Sie in der Liste **Komponente** die Komponente von Kaspersky Embedded Systems Security, deren Genauigkeitsstufe für Ereignisse Sie festlegen möchten.
     b. Um eine Genauigkeitsstufe in den Protokollen der Aufgabenausführung und im Systemaudit-Protokoll einer bestimmten Komponente anzugeben, wählen Sie die entsprechende Stufe in der Liste **Prioritätsstufe** aus.
   - Um den Standardordner für Protokolle zu ändern, geben Sie den Ordnerpfad an oder wählen Sie den Ordner mit Hilfe der Schaltfläche **Durchsuchen** aus.
   - Geben Sie an, wie viele Tage die Protokolle der Aufgabenausführung gespeichert bleiben sollen.
   - Geben Sie an, wie viele Tage die im Knoten **Systemaudit-Protokoll** angezeigten Informationen gespeichert werden sollen.
6. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für Protokolle werden gespeichert.

Sicherheitsprotokoll

Kaspersky Embedded Systems Security führt ein Sicherheits-Ereignisprotokoll über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Computer verbunden sind. In diesem Protokoll werden folgende Ereignisse registriert:

- Ereignisse der Komponente "Exploit-Prävention".
- Kritische Ereignisse der Komponente "Protokollanalyse"
- Kritische Ereignisse, die auf eine versuchte Verletzung der Sicherheit hindeuten (für die Aufgaben "Echtzeit-Computerschutz", "Untersuchung auf Befehl", "Überwachung der Datei-Integrität", "Kontrolle des Programmstarts" und "Gerätekontrolle").

Sie können das Sicherheitsprotokoll wie auch das Systemaudit-Protokoll leeren (siehe Abschnitt "Ereignisse aus dem Systemaudit-Protokoll löschen" auf Seite 216). Dabei registriert Kaspersky Embedded Systems Security ein Ereignis des Systemaudits über das Leeren des Sicherheitsprotokolls.

Anpassen der Einstellungen der SIEM-Integration

Um die Belastung für leistungsschwache Geräte zu reduzieren und die Gefahr eines Abfalls der Systemleistung infolge eines zu großen Umfangs der Programmprotokolle zu verringern, können Sie die Veröffentlichung der Audit-Ereignisse und der Ereignisse der Aufgabenausführung über das Protokoll syslog auf dem *syslog-Server* einrichten.

Ein syslog-Server ist ein externer Server für Ereignis-Management (SIEM), der eingehende Ereignisse sammelt und analysiert sowie andere Aktionen im Rahmen der Protokollverwaltung ausführt.

Sie können die SIEM-Integration in zwei Modi verwenden:

- Ereignisse auf dem syslog-Server duplizieren: In diesem Modus wird davon ausgegangen, dass 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 lokalen Computer gespeichert werden.

  Es wird empfohlen, diesen Modus zu verwenden, um die Belastung für den geschützten Computer auf ein Minimum zu reduzieren.

- Lokale Kopien der Ereignisse löschen: In diesem Modus wird davon ausgegangen, dass alle Ereignisse, die während der Programmausführung registriert und in SIEM veröffentlicht wurden, vom lokalen Computer gelöscht werden.

  > 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 empfangen und erfolgreich identifiziert werden können. Das Programm unterstützt die Konvertierung von Ereignissen in ein Format für strukturierte Daten und in das JSON-Format.

Um das Risiko eines misslungenen Versands von Ereignissen an SIEM zu verringern, können Sie die Verbindung zu einem syslog-Spiegelserver konfigurieren.

Der syslog-Spiegelserver ist ein zusätzlicher syslog-Server, zu dessen Verwendung das Programm automatisch übergeht, wenn keine Verbindung zum primären syslog-Server besteht oder wenn dieser nicht verwendet werden kann.

Standardmäßig wird die SIEM-Integration nicht verwendet. Sie können die SIEM-Integration aktivieren und deaktivieren und die entsprechenden Funktionen konfigurieren (s. Tabelle unten).

Tabelle 10. Einstellungen für die SIEM-Integration

Einstellung	Standardwert	Beschreibung
Ereignisse über das syslog-Protokoll an den externen syslog-Server senden	Wird nicht verwendet	Sie können die SIEM-Integration mithilfe dieses Kontrollkästchens aktivieren und deaktivieren.
Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen	Wird nicht verwendet	Sie können die Speicherung lokaler Kopien der Protokolle nach ihrem Versand an SIEM mithilfe dieses Kontrollkästchens konfigurieren.
Format der Ereignisse	Strukturierte Daten	Sie können eines von zwei Formaten wählen, in die das Programm die Ereignisse vor ihrem Versand an den syslog-Server konvertiert, damit sie von SIEM erfolgreich identifiziert werden können.
Verbindungsprotokoll	TCP	Sie können mithilfe der Dropdown-Liste die Verbindung mit dem primären syslog-Server über die Protokolle UPD oder TCP und mit dem zusätzlichen syslog-Server über das TCP-Protokoll anpassen.
Einstellungen der Verbindung mit dem primären syslog-Server	IP-Adresse: 127.0.0.1 Port: 514	Sie können in den entsprechenden Feldern die Werte für IP-Adresse und Port angeben, um die Verbindung mit dem primären syslog-Server anzupassen. Der Wert der IP-Adresse darf nur im Format IPv4 angegeben werden.
Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist	Wird nicht verwendet	Sie können mithilfe dieses Kontrollkästchens die Verwendung eines syslog-Spiegelservers aktivieren und deaktivieren.
Einstellungen der Verbindung mit dem zusätzlichen syslog-Server	IP-Adresse: 127.0.0.1 Port: 514	Sie können in den entsprechenden Feldern die Werte für IP-Adresse und Port angeben, um die Verbindung mit dem gespiegelten syslog-Server anzupassen. Der Wert der IP-Adresse darf nur im Format IPv4 angegeben werden.

► *Um die Einstellungen der SIEM-Integration zu konfigurieren, gehen Sie wie folgt vor:*

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Block **Protokolle der Aufgabenausführung** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen für Berichte und Benachrichtigungen** wird geöffnet.

5. Wählen Sie die Registerkarte **SIEM-Integration** aus.

6. Aktivieren Sie im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Ereignisse über das syslog-Protokoll an den externen syslog-Server senden**.

   Das Kontrollkästchen aktiviert/deaktiviert die Verwendung der Funktion zum Versand der zu veröffentlichenden Ereignisse an den externen syslog-Server.

   Wenn das Kontrollkästchen aktiviert ist, sendet das Programm die zu veröffentlichenden Ereignisse an SIEM gemäß der Konfiguration der SIEM-Integration.

   Wenn das Kontrollkästchen deaktiviert ist, nimmt das Programm keine SIEM-Integration vor. Sie können die Einstellungen der SIEM-Integration nicht anpassen, wenn das Kontrollkästchen deaktiviert ist.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

7. Aktivieren Sie bei Bedarf im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen**.

   Das Kontrollkästchen aktiviert/deaktiviert das Löschen der lokalen Kopien der Protokolle nach ihrem Versand an SIEM.

   Wenn das Kontrollkästchen aktiviert ist, löscht das Programm die lokalen Kopien der Ereignisse, sobald sie erfolgreich in SIEM veröffentlicht wurden. Es wird empfohlen, diesen Modus auf leistungsschwachen Computern zu verwenden.

   Wenn das Kontrollkästchen deaktiviert ist, sendet das Programm lediglich die Ereignisse an SIEM. Die Kopien der Protokolle werden weiterhin lokal gespeichert.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Der Status des Kontrollkästchens **Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen** beeinflusst nicht die Einstellungen zum Speichern der Ereignisse des Sicherheitsprotokolls: Das Programm löscht niemals automatisch die Ereignisse des Sicherheitsprotokolls.

8. Geben Sie im Abschnitt **Format der Ereignisse** das Format an, in das Sie die Ereignisse bei der Programmausführung für den Versand an SIEM konvertieren möchten.

   Standardmäßig konvertiert das Programm die Ereignisse in ein Format für strukturierte Daten.

9. Gehen Sie im Abschnitt **Verbindungseinstellungen** wie folgt vor:

   - Geben Sie das Protokoll für die Verbindung zu SIEM an.
   - Geben Sie die Einstellungen der Verbindung mit dem primären syslog-Server an.

     Die IP-Adresse darf nur im Format IPv4 angegeben werden.
   - Aktivieren Sie das Kontrollkästchen **Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist**, wenn Sie möchten, dass das Programm andere Verbindungseinstellungen verwendet, wenn der Versand der Ereignisse an den primären syslog-Server nicht verfügbar ist.
     - Geben Sie die folgenden Einstellungen für die Verbindung mit dem zusätzlichen syslog-Server an: **IP-Adresse** und **Port**.

       Die Felder **IP-Adresse** und **Port** des syslog-Spiegelservers können nicht bearbeitet werden, wenn das Kontrollkästchen **Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist** deaktiviert ist.

       Die IP-Adresse darf nur im Format IPv4 angegeben werden.

10. Klicken Sie auf **OK**.

Die angepassten Einstellungen der SIEM-Integration werden übernommen.

Benachrichtigungseinstellungen anpassen

► *Um die Benachrichtigungen für Kaspersky Embedded Systems Security anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Unterabschnitt **Ereignisbenachrichtigungen** auf die Schaltfläche **Einstellungen**.

5. Passen Sie im Fenster **Benachrichtigungen anpassen** die folgenden Eigenschaften für Kaspersky Embedded Systems Security gemäß Ihren Anforderungen an:

   - Wählen Sie in der Liste **Benachrichtigungen anpassen** den Benachrichtigungstyp aus, dessen Einstellungen Sie anpassen möchten.
   - Passen Sie im Abschnitt **Benachrichtigung für die Benutzer** die Methode für die Benachrichtigung der Benutzer an. Geben Sie bei Bedarf einen Benachrichtigungstext ein.
   - Passen Sie im Abschnitt **Benachrichtigung für die Administratoren** die Methode für die Benachrichtigung von Administratoren an. Geben Sie bei Bedarf einen Benachrichtigungstext ein. Passen Sie bei Bedarf die erweiterten Benachrichtigungseinstellungen über die Schaltfläche **Einstellungen** an.
   - Geben Sie im Abschnitt **Grenzwerte für Ereigniserstellung** die Zeitintervalle an, nach deren Ablauf Kaspersky Embedded Systems Security die Ereignisse *"Programm-Datenbanken sind veraltet", "Programm-Datenbanken sind stark veraltet"* und *"Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt"* protokolliert.

     - **Programm-Datenbanken sind veraltet (Tage)**

       Anzahl der Tage seit dem letzten Update der Programm-Datenbanken.

       Der Standardwert beträgt 7 Tage.

     - **Programm-Datenbanken sind stark veraltet (Tage)**

       Anzahl der Tage seit dem letzten Update der Programm-Datenbanken.

       Der Standardwert beträgt 14 Tage.

     - **Untersuchung wichtiger Bereiche des Computers wurde lange nicht durchgeführt (Tage)**

       Anzahl der Tagen seit der letzten erfolgreichen Aufgabe zur Untersuchung wichtiger Bereiche.

       Der Standardwert beträgt 30 Tage.

6. Klicken Sie auf **OK**.

Die festgelegten Benachrichtigungseinstellungen werden gespeichert.

Konfigurieren der Interaktion mit dem Administrationsserver

► *Um die Typen der Objekte auszuwählen, über die Kaspersky Embedded Systems Security Informationen an den Kaspersky Security Center-Administrationsserver übergeben soll, gehen Sie wie folgt vor:*

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   > Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** auf die Schaltfläche **Einstellungen** im Block **Interaktion mit Administrationsserver**.

   Das Fenster **Netzwerklisten des Administrationsservers** wird geöffnet.

5. Wählen Sie im Fenster **Netzwerklisten des Administrationsservers** die Objekttypen aus, über die Kaspersky Embedded Systems Security Informationen an den Kaspersky Security Center-Administrationsserver übergeben soll:

   - Quarantäneobjekte.
   - Objekte im Backup.

6. Klicken Sie auf **OK**.

   Kaspersky Embedded Systems Security wird Informationen über die ausgewählten Objekttypen an den Administrationsserver übertragen.

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 Computern.

Sie können in Kaspersky Security Center einheitliche Richtlinien erstellen, um den Schutz auf mehreren Computern zu verwalten, auf denen Kaspersky Embedded Systems Security installiert ist.

Eine Richtlinie übernimmt die in ihr eingetragenen Einstellungen, Funktionen und Aufgaben für Kaspersky Embedded Systems Security auf allen geschützten Computern 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 **Systemaudit-Protokoll** zur Verfügung.

In Kaspersky Security Center existiert eine einzige Methode zur Übernahme von Richtlinien auf lokalen Computern: *Änderung von Einstellungen verbieten*. Nach der Übernahme der Richtlinie übernimmt Kaspersky Embedded Systems Security die Einstellungswerte auf den lokalen Computern, neben denen Sie in den Richtlinieneigenschaften das Symbol 🔒 gesetzt haben, anstatt der vor Übernahme der Richtlinie lokal festgelegten Einstellungswerte. Einstellungswerte der aktiven Richtlinie, neben denen 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 einen einzelnen Computer aus dem Fenster **Eigenschaften: <Computername>**.

Die Einstellungen, die angepasst und mithilfe einer aktiven Richtlinie an den lokalen Computer übergeben wurden, werden nach der Deaktivierung der aktiven Richtlinie in den Einstellungen der lokalen Aufgaben gespeichert.

Wenn die Richtlinie Einstellungen für eine der Aufgaben zum Echtzeit-Computerschutz festlegt und diese Aufgabe ausgeführt wird, so werden die durch die Richtlinie definierten Einstellungen sofort nach der Übernahme der Richtlinie geändert. Wenn die Aufgabe nicht ausgeführt wird, werden die Parameter aus der Richtlinie beim nächsten Aufgabenstart übernommen.

In diesem Kapitel

Richtlinie erstellen

Das Erstellen einer neuen Richtlinie umfasst folgende Etappen:

1. Erstellung einer Richtlinie mit dem Assistenten für die Erstellung von Richtlinien. In den Fenstern des Assistenten können Sie die Parameter für den Echtzeit-Computerschutz anpassen.
2. Anpassung der Richtlinieneinstellungen. Im Fenster **Eigenschaften:<Name der Richtlinie>** der erstellten Richtlinie können Sie Folgendes anpassen: Einstellungen für den Echtzeit-Computerschutz, allgemeine Einstellungen für Kaspersky Embedded Systems Security, Einstellungen für Quarantäne und Backup-Einstellungen, Genauigkeitsstufe für Protokolle der Aufgabenausführung sowie Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Embedded Systems Security.

► *Gehen Sie folgendermaßen vor, um eine Richtlinie für eine Gruppe von Computern zu erstellen, auf denen Kaspersky Embedded Systems Security installiert ist:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie anschließend die Administrationsgruppe aus, für deren Computer Sie eine Richtlinie anlegen möchten.
2. Öffnen Sie im Ergebnisfenster der ausgewählten Administrationsgruppe die Registerkarte **Richtlinien** und klicken Sie dort auf den Link **Richtlinie erstellen**, um den Richtlinien-Assistenten zu öffnen.

   Das Fenster **Assistent für neue Richtlinie** wird geöffnet.
3. Wählen Sie im Fenster **Wählen Sie die Gruppe aus, für die Sie eine Richtlinie erstellen möchten** Kaspersky Embedded Systems Security aus und klicken Sie auf **Weiter**.
4. Geben Sie einen Gruppenrichtliniennamen in das Feld **Name** ein.

   Die Namen von Richtlinien dürfen keines der folgenden Symbole enthalten: " * < : > ? \ | .
5. Gehen Sie wie folgt vor, um die Richtlinienkonfiguration anzuwenden, die in der vorherigen Programmversion verwendet wurde:
   a. Aktivieren Sie das Kontrollkästchen **Einstellungen der Richtlinie für frühere Programmversionen verwenden**.
   b. Klicken Sie auf die Schaltfläche **Auswählen**.
   c. Wählen Sie die Richtlinie aus, die Sie übernehmen möchten.
   d. Klicken Sie auf **Weiter**.
6. Wählen Sie im Fenster **Vorgangsart auswählen** eine der folgenden Optionen aus:

- **Erstellen**, um eine neue Richtlinie mit den Standardeinstellungen zu erstellen.
- **Richtlinie importieren, die mit einer früheren Version von Kaspersky Embedded Systems Security** erstellt wurde, um die Richtlinie dieser Version als Vorlage zu verwenden.
- Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie die Konfigurationsdatei aus, in der Sie die vorhandene Richtlinie gespeichert haben.

7. Passen Sie im Fenster **Echtzeit-Computerschutz** bei Bedarf die Einstellungen der Aufgaben "Echtzeitschutz für Dateien", "Verwendung von KSN" sowie die Funktionalität der Exploit-Prävention an. Erlauben oder verbieten Sie die Übernahme konfigurierter Aufgaben in der Richtlinie in den lokalen Computernetzwerken:
   - Klicken Sie auf , um die Konfiguration der Einstellungen einer Aufgabe auf den Computern des Netzwerks zu erlauben und die Übernahme der in der Richtlinie konfigurierten Aufgabeneinstellungen zu verbieten.
   - Klicken Sie auf , um die Konfiguration der Einstellungen einer Aufgabe auf den Computern des Netzwerks zu verbieten und die Übernahme der in der Richtlinie konfigurierten Aufgabeneinstellungen zu erlauben.

   In neu erstellten Richtlinien gelten für die Parameter der Aufgaben zum Echtzeit-Computerschutz die Standardeinstellungen.
   - Wenn Sie die standardmäßig festgelegten Einstellungen der Aufgabe Echtzeitschutz für Dateien ändern möchten, klicken Sie im Unterabschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**. Passen Sie im erscheinenden Fenster die Aufgabeneinstellungen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.
   - Wenn Sie die Standardeinstellungen der Aufgabe Verwendung von KSN ändern möchten, klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Verwendung von KSN**. Passen Sie im erscheinenden Fenster die Aufgabeneinstellungen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.

     Um die Aufgabe zur Verwendung von KSN zu starten, müssen Sie die KSN-Erklärung im Fenster Datenverarbeitung akzeptieren (siehe Abschnitt "Datenverarbeitung über das Verwaltungs-Plug-in konfigurieren" auf Seite 297).
   - Wenn Sie die Standardeinstellungen der Komponente "Exploit-Prävention" ändern möchten, klicken Sie im Unterabschnitt **Exploit-Prävention** auf die Schaltfläche **Einstellungen**. Passen Sie im erscheinenden Fenster die Funktionen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.
8. Wählen Sie im Fenster **Gruppenrichtlinie für das Programme erstellen** eine der folgenden Statusvarianten für die Richtlinie 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 Sie nicht möchten, dass die Richtlinie sofort angewendet wird. Sie können diese Richtlinie später aktivieren.
   - Aktivieren Sie das Kontrollkästchen **Richtlinieneigenschaften sofort nach ihrer Erstellung öffnen**, um den **Assistenten für neue Richtlinien** automatisch zu schließen und die neu erstellte Richtlinie nach Klicken auf die Schaltfläche **Weiter** zu konfigurieren.

9. Klicken Sie auf **Fertig**.

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.

Abschnitte mit Richtlinieneinstellungen für Kaspersky Embedded Systems Security

Allgemein

Im Abschnitt **Allgemein** können Sie die folgenden Richtlinieneinstellungen konfigurieren:

- Richtlinienstatus festlegen.
- Vererbung der Einstellungen von übergeordneten Richtlinien auf untergeordnete Richtlinien konfigurieren

Konfiguration von Ereignissen

Im Abschnitt **Konfiguration von Ereignissen** können Sie die Einstellungen für die folgenden Ereigniskategorien konfigurieren:

- *Kritische Ereignisse*
- *Funktionsfehler*
- *Warnung*
- *Informatives Ereignis*

Über die Schaltfläche **Eigenschaften** können Sie die folgenden Einstellungen für die ausgewählten Ereignisse konfigurieren:

- Geben Sie den Speicherort und die Speicherdauer für Informationen über protokollierte Ereignisse an.
- Wählen Sie eine Methode für die Benachrichtigung über protokollierte Ereignisse aus.

Programmeinstellungen

Tabelle 11. Einstellungen des Abschnitts "Programmeinstellungen"

Abschnitt	Einstellungen
Skalierbarkeit und Oberfläche	Im Unterabschnitt **Skalierbarkeit und Oberfläche** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Auswahl der automatischen oder manuellen Konfiguration der Skalierbarkeitseinstellungen • Einstellungen für die Anzeige des Programmsymbols
Sicherheit	Im Unterabschnitt **Sicherheit** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Einstellungen der Aufgabenausführung anpassen • Aktionen des Programms beim Wechsel des Computers in den USV-Akkubetrieb angeben • Kennwortschutz der Programmfunktionen aktivieren und deaktivieren

Verbindungen	Im Unterabschnitt **Verbindungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Proxyserver-Einstellungen für die Verbindung mit den Update-Servern, den Aktivierungsservern und KSN konfigurieren: • Festlegung der Proxyserver-Einstellungen • Geben Sie die Einstellungen für die Authentifizierung auf dem Proxyserver an.
Start von Systemaufgaben	Im Unterabschnitt **Start von Systemaufgaben** können Sie über die Schaltfläche **Einstellungen** den Start der folgenden Systemaufgaben nach einem auf den lokalen Computern festgelegten Zeitplan erlauben oder verbieten: • Aufgabe zur Untersuchung auf Befehl • Update-Aufgabe und Aufgabe zur Update-Verteilung

Zusätzlich

Tabelle 12. Einstellungen des Abschnitts "Zusätzlich"

Abschnitt	Einstellungen
Vertrauenswürdige Zone	Im Unterabschnitt **Vertrauenswürdige Zone** können Sie über die Schaltfläche **Einstellungen** die folgenden Parameter für die Verwendung der vertrauenswürdigen Zone konfigurieren: • Erstellung einer Liste der Ausnahmen von der vertrauenswürdigen Zone • Aktivieren oder Deaktivieren der Untersuchung von Backup-Operationen • Erstellen Sie eine Liste der vertrauenswürdigen Prozesse.
Untersuchung von Wechseldatenträgern	Im Unterabschnitt **Untersuchung von Wechseldatenträgern** können Sie über die Schaltfläche **Einstellungen** die Untersuchungseinstellungen für USB-Wechseldatenträger anpassen.
Benutzerrechte für die Programmverwaltung	Im Unterabschnitt **Benutzerrechte für die Programmverwaltung** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Embedded Systems Security anpassen.
Benutzerrechte für die Verwaltung von Security Service	Im Unterabschnitt **Benutzerrechte für die Verwaltung von Security Service** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Security Service anpassen.
Speicher	Im Unterabschnitt **Speicher** können Sie über die Schaltfläche **Einstellungen** folgende Einstellungen für Quarantäne, Backup und blockierte Hosts anpassen: • Angabe des Ordnerpfads, in dem Sie die Quarantäne- oder Backup-Objekte ablegen möchten • Anpassung der maximalen Größe des Backups und der Quarantäne sowie Festlegung des Grenzwerts für verfügbaren Speicherplatz • Angabe des Ordnerpfads, in dem Sie die wiederhergestellten Quarantäne- oder Backup-Objekte ablegen möchten • Anpassen der Einstellungen für die Sperrung der Hosts

Echtzeit-Computerschutz

Tabelle 13. Einstellungen des Abschnitts "Echtzeit-Computerschutz"

Abschnitt	Einstellungen
Echtzeitschutz für Dateien	Im Unterabschnitt **Echtzeitschutz für Dateien** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Schutzmodus angeben • Verwendung der heuristischen Analyse anpassen • Verwendung der vertrauenswürdigen Zone anpassen • Schutzbereich angeben • Sicherheitsstufe für den ausgewählten Schutzbereich festlegen: Sie können die vorinstallierte Sicherheitsstufe auswählen oder die Sicherheitseinstellungen manuell anpassen. • Einstellungen für den Aufgabenstart festlegen
Verwendung von KSN	Im Unterabschnitt **Verwendung von KSN** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Aktionen für Objekte, die in KSN nicht vertrauenswürdig sind, angeben • Datentransfer und Verwendung von Kaspersky Security Center als KSN Proxyserver konfigurieren. Klicken Sie auf die Schaltfläche **Datenverarbeitung**, um die KSN-Erklärung und die KMP-Erklärung zu akzeptieren oder abzulehnen und die Einstellungen des abhängigen Datenaustausches zu konfigurieren.
Exploit-Prävention	Im Unterabschnitt **Exploit-Prävention** können Sie über die Schaltfläche **Einstellungen** die folgenden Parameter für die Aufgabenausführung konfigurieren: • Schutzmodus des Prozess-Arbeitsspeichers auswählen • Aktionen zur Minderung des Exploit-Risikos angeben • Liste der geschützten Prozesse ergänzen und bearbeiten

Überwachung der Desktop-Aktivitäten

Tabelle 14. Einstellungen des Abschnitts "Überwachung der Desktop-Aktivitäten"

Abschnitt	Einstellungen
Kontrolle des Programmstarts	Im Unterabschnitt **Kontrolle des Programmstarts** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Funktionsmodus der Aufgabe auswählen • Einstellungen für die Kontrolle wiederholter Programmstarts anpassen • Gültigkeitsbereich der Regeln für die Kontrolle des Programmstarts festlegen • Verwendung von KSN anpassen • Einstellungen für den Aufgabenstart festlegen

Gerätekontrolle	Im Unterabschnitt **Gerätekontrolle** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Funktionsmodus der Aufgabe auswählen • Einstellungen für den Aufgabenstart festlegen

Netzwerküberwachung

Tabelle 15. Einstellungen des Abschnitts "Netzwerküberwachung"

Abschnitt	Einstellungen
Firewall-Verwaltung	Im Unterabschnitt **Firewall-Verwaltung** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Firewall-Regeln anpassen • Einstellungen für den Aufgabenstart festlegen

System-Diagnose

Tabelle 16. Einstellungen des Abschnitts "System-Diagnose"

Abschnitt	Einstellungen
Überwachung der Datei-Integrität	Im Unterabschnitt **Überwachung der Datei-Integrität** können Sie die Überwachung von Dateiänderungen anpassen, die auf eine Sicherheitsverletzung auf einem geschützten Computer hindeuten.
Protokollanalyse	Im Abschnitt **Protokollanalyse** können Sie die Überwachung der Integrität eines geschützten Computers auf der Grundlage der Ergebnisse des Windows-Ereignisprotokolls anpassen.

Protokolle und Benachrichtigungen

Tabelle 17. Einstellungen des Abschnitts "Protokolle und Benachrichtigungen"

Abschnitt	Einstellungen
Protokolle der Aufgabenausführung	Im Unterabschnitt **Protokolle der Aufgabenausführung** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Prioritätsstufe protokollierter Ereignisse für die ausgewählten Programmkomponenten angeben • Speicherdauer für Protokolle der Aufgabenausführung festlegen • Konfiguration der SIEM-Integration in Kaspersky Security Center.

Ereignisbenachrichtigungen	Im Unterabschnitt **Ereignisbenachrichtigungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Legen Sie Einstellungen für die Benutzerbenachrichtigung für das Ereignis *Objekt gefunden*, das Ereignis *Nicht vertrauenswürdiger Massenspeicher gefunden und eingeschränkt* und das Ereignis *Computer wurde der Liste der nicht vertrauenswürdigen Computer hinzugefügt* fest. • Benachrichtigung des Administrators über ein beliebiges ausgewähltes Ereignis aus der Liste der Ereignisse im Abschnitt **Benachrichtigungen anpassen**
Interaktion mit Administrationsserver	Im Abschnitt **Interaktion mit Administrationsserver** können Sie über die Schaltfläche **Einstellungen** die Typen der Objekte auswählen, über die Kaspersky Embedded Systems Security Informationen an den Administrationsserver übergeben soll. Sie können die Übermittlung von Informationen über im Backup und in der Quarantäne gespeicherte Objekte an den Administrationsserver auch anpassen.

Ausführliche Informationen über die Aufgaben "Schutz für ins Netzwerk eingebundenen Speicher" finden Sie im *Implementierungshandbuch zum Schutz für ins Netzwerk eingebundene Speicher für Kaspersky Embedded Systems Security*.

Revisionsverlauf

Im Abschnitt **Revisionsverlauf** können Sie Revisionen verwalten: Sie können sie mit der aktuellen Revision oder einer anderen Richtlinie vergleichen, Beschreibungen für Revisionen hinzufügen, Revisionen in einer Datei speichern oder ein Rollback vornehmen.

Richtlinie anpassen

Im Fenster **Eigenschaften: <Name der Richtlinie>** einer vorhandenen Richtlinie können Sie folgende Einstellungen anpassen: allgemeine Einstellungen von Kaspersky Embedded Systems Security, Einstellungen für Quarantäne und Backup-Einstellungen, Einstellungen für die vertrauenswürdige Zone, Echtzeit-Computerschutz, Überwachung der Desktop-Aktivitäten, Genauigkeitsstufe für Protokolle der Aufgabenausführung, Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Embedded Systems Security, Zugriffsrechte für die Verwaltung des Programms und von Kaspersky Security Service, Einstellungen für die Übernahme von Richtlinienprofilen.

► *Gehen Sie wie folgt vor, um die Richtlinieneinstellungen zu konfigurieren:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Erweitern Sie die Administrationsgruppe, für die Sie die zugehörigen Richtlinieneinstellungen anpassen möchten, und öffnen Sie die Registerkarte **Richtlinien** im Detailbereich.

3. Wählen Sie eine Richtlinie, die Sie anpassen möchten, und öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>** auf eine der folgenden Arten:
   - Wählen Sie im Kontextmenü der Richtlinie die Option **Eigenschaften** aus.
   - Klicken Sie im rechten Ergebnisbereich der ausgewählten Richtlinie auf den Link **Richtlinie anpassen**.
   - Doppelklicken Sie auf die ausgewählte Richtlinie.
4. Aktivieren oder deaktivieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Richtlinienstatus** die Richtlinie. Wählen Sie dazu eine der folgenden Varianten:
   - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie auf allen Computern übernommen wird, die zur ausgewählten Administrationsgruppe gehören.
   - **Inaktive Richtlinie**, wenn Sie die Richtlinie später auf allen Computern der ausgewählten Administrationsgruppe aktivieren möchten.

   Die Einstellung **Out-Of-Office Richtlinie** ist bei der Verwendung von Kaspersky Embedded Systems Security nicht verfügbar.
5. In den Abschnitten **Konfiguration von Ereignissen**, **Programmeinstellungen**, **Zusätzlich**, **Protokolle und Benachrichtigungen** und **Revisionsverlauf** können Sie die allgemeinen Einstellungen der Programmausführung ändern (siehe Tabelle unten).
6. Konfigurieren Sie in den Abschnitten **Echtzeit-Computerschutz**, **Überwachung der Desktop-Aktivitäten**, **Netzwerküberwachung** und **System-Diagnose** die Einstellungen für die Ausführung der Aufgaben des Programms sowie die Einstellungen für deren Start (siehe Tabelle unten).

   Sie können die Ausführung einer beliebigen Aufgabe auf allen Computern, 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 Computern des Netzwerks für jede einzelne Programmkomponente festlegen.
7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden in der Richtlinie übernommen.

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.

In diesem Kapitel

Über die Erstellung von Aufgaben in Kaspersky Security Center

Sie können Gruppenaufgaben für Administrationsgruppen und für Zusammenstellungen von Computern erstellen. Sie können folgende Aufgabentypen erstellen:

- Programm aktivieren
- Update-Verteilung
- Update der Programm-Datenbanken
- Update der Programm-Module
- Rollback des Datenbanken-Updates
- Untersuchung auf Befehl
- Integritätsprüfung für Programme
- Automatisches 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 einen Computer: im Fenster **Eigenschaften: <Computername>** im Abschnitt **Aufgaben**.
- Für eine Administrationsgruppe: im Ergebnisbereich des Knotens der ausgewählten Computergruppe auf der Registerkarte **Aufgaben**.
- Für eine Auswahl an Computern: im Ergebnisbereich des Knotens **Geräteauswahl**

Mithilfe von Richtlinien können Sie Zeitpläne für lokale Systemaufgaben zum Update und zur Untersuchung auf Befehl (siehe Abschnitt "Zeitgesteuerten Start für lokale Systemaufgaben konfigurieren" auf Seite 103) auf allen geschützten Computern aus 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 Verwaltungskonsole von Kaspersky Security Center zu erstellen:*

1. Starten Sie den Assistenten für neue Aufgaben nach einer der folgenden Methoden:
   - Für das Erstellen einer lokalen Aufgabe:
     a. Erweitern Sie in der Struktur der Verwaltungskonsole den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, zu der der geschützte Computer gehört.
     b. Öffnen Sie im Detailbereich auf der Registerkarte **Geräte** das Kontextmenü des geschützten Computers und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im nächsten Fenster auf die Schaltfläche **Hinzufügen** im Abschnitt **Aufgaben**.
   - Für das Erstellen einer Gruppenaufgabe:
     a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
     b. Wählen Sie die Administrationsgruppe aus, für die Sie eine Aufgabe erstellen möchten.
     c. Öffnen Sie im Ergebnisbereich die Registerkarte **Aufgaben** und wählen Sie **Aufgabe erstellen**.
   - Um eine Aufgabe für eine benutzerdefinierte Auswahl von Computern zu erstellen, gehen Sie wie folgt vor:
     a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
     b. Wählen Sie die Administrationsgruppe aus, in der die Computer enthalten sind.
     c. Wählen Sie einen Computer oder eine benutzerdefinierte Gruppe von Computern aus.
     d. Wählen Sie in der Dropdown-Liste **Aktion ausführen** die Option **Aufgabe erstellen** aus.

   Darauf öffnet sich der Assistent für neue Aufgaben.
2. Wählen Sie im Fenster **Aufgabentyp** unter der Überschrift **Kaspersky Embedded Systems Security** den Typ der zu erstellenden Aufgabe aus.
3. Wenn Sie einen anderen Aufgabentyp als Rollback des Datenbanken-Updates. Integritätsprüfung für Programme oder Programmaktivierung ausgewählt haben, wird das Fenster **Einstellungen** geöffnet. Die Einstellungen können abhängig vom Aufgabentyp unterschiedlich sein:
   - Aufgabe zur Untersuchung auf Befehl erstellen (siehe Abschnitt "Erstellen einer Aufgabe zur Untersuchung auf Befehl" auf Seite 437).
   - Wenn Sie eine der Aufgaben zum Update erstellen, aktivieren Sie die gewünschten

Aufgabenparameter nach Ihren Bedürfnissen:

a. Wählen Sie im Fenster **Update-Quelle** eine Update-Quelle aus.

b. Klicken Sie auf **Verbindungseinstellungen**. Das Fenster **Verbindungseinstellungen** wird geöffnet.

c. Im Fenster **Verbindungseinstellungen**:

Geben Sie den Modus des FTP-Servers für die Verbindung mit einem geschützten Computer an.

Ändern Sie bei Bedarf die Wartezeit für die Verbindung mit der Update-Quelle.

Passen Sie die Einstellungen für den Zugang zum Proxy-Server während der Verbindung mit der Update-Quelle an.

Geben Sie den Standort des bzw. der geschützten Computer(s) an, um den Update-Download zu optimieren.

- Um eine Aufgabe zum Update der Programm-Module zu erstellen, passen Sie im Fenster **Einstellungen für das Update der Programm-Module anpassen** die entsprechenden Einstellungen für das Update der Programm-Module an:

a. Wählen Sie, ob kritische Updates der Programm-Module kopiert und installiert werden sollen, oder nur auf neue Updates geprüft werden soll, ohne Installation.

b. Wenn Sie **Wichtige Updates der Programm-Module verteilen und installieren** ausgewählt haben, kann zum Übernehmen der installierten Programm-Module ein Neustart des Computers erforderlich sein. Damit Kaspersky Embedded Systems Security den Computer nach Abschluss der Aufgabe automatisch neu startet, aktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**.

c. Wenn Sie Informationen über Upgrades der Module von Kaspersky Embedded Systems Security erhalten möchten, aktivieren Sie das Kontrollkästchen **Über verfügbare planmäßige Updates der Programm-Module informieren**.

Geplante Updatepakete werden von Kaspersky Lab nicht auf den Update-Servern veröffentlicht, um sie automatisch zu installieren. Sie können solche Updatepakete von der Kaspersky-Lab-Webseite downloaden. Sie können eine Benachrichtigung des Administrators über das Ereignis **Ein planmäßiges Update der Programm-Module ist verfügbar** einrichten. Darin ist die URL unserer Website enthalten, von der die geplanten Updates heruntergeladen werden können.

- Um die Aufgabe zur Update-Verteilung zu erstellen, geben Sie im Fenster **Einstellungen für die Update-Verteilung** die Zusammensetzung der Updates und den Zielordner an.
- Um die Aufgabe zur Aktivierung des Programms zu erstellen, gehen Sie wie folgt vor:

a. Geben Sie im Fenster **Aktivierungsparameter** die Schlüsseldatei an, mit der Sie das Programm aktivieren möchten.

b. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie eine Aufgabe zur Verlängerung der Lizenz erstellen möchten.

- Erstellen Sie die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" (siehe Abschnitt "Über die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts"" auf Seite 338)
- Erstellen Sie die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle (siehe Abschnitt "Regeln mithilfe der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen" auf Seite 378)

4. Passen Sie den Aufgabenzeitplan an (siehe Abschnitt "Einstellungen für den Zeitplan für den Aufgabenstart anpassen" auf Seite 139) (sie können einen Zeitplan für alle Aufgaben mit Ausnahme der Aufgabe zum Rollback des Datenbanken-Updates erstellen).
5. Klicken Sie auf **OK**.

6. Wenn die Aufgabe für eine Auswahl von Computern erstellt wird, wählen Sie das Netzwerk (die Gruppe) von Computern aus, für welche die Aufgabe ausgeführt werden soll.
7. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, mit dem Sie die Aufgabe ausführen möchten.
8. Geben Sie im Fenster **Aufgabenname festlegen** einen Aufgabennamen an (maximal 100 Zeichen), wobei folgende Zeichen unzulässig sind: **" * < > ? \ | :** .

   Es wird empfohlen, den Aufgabentyp im Namen anzugeben (z. B. "Untersuchung auf Befehl der freigegebenen Ordner").
9. Aktivieren Sie im Fenster **Erstellung der Aufgabe fertig stellen** das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe nach ihrer Erstellung gestartet wird. Klicken Sie auf **Fertig**.

Die erstellte Aufgabe erscheint in der Liste **Aufgaben**.

Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen

► *Um lokale Aufgaben oder allgemeine Programmeinstellungen für einen einzelnen Netzwerk-Computer zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur des Administrationsservers von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, zu der der geschützte Computer gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Geräte** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:

   - Doppelklicken Sie auf den Namen des geschützten Computers.
   - Öffnen Sie das Kontextmenü für den Namen des geschützten Computers und wählen Sie den Punkt **Eigenschaften**.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
4. Um die lokalen Aufgabeneinstellungen anzupassen, gehen Sie wie folgt vor:

   a. Wechseln Sie in den Abschnitt **Aufgaben**.

      - Wählen Sie in der Aufgabenliste die lokale Aufgabe aus, deren Einstellungen Sie anpassen möchten.
      - Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben.
      - Wählen Sie den Aufgabennamen aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
      - Wählen Sie den Punkt **Eigenschaften** im Kontextmenü der ausgewählten Aufgabe.

        Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.

5. Um die Programmeinstellungen anzupassen, gehen Sie wie folgt vor:
   a. Wechseln Sie zum Abschnitt **Programme**.
      - Wählen Sie in der Liste der installierten Programme das Programm aus, das Sie anpassen möchten.
      - Doppelklicken Sie in der Liste der installierten Programme auf den Programmnamen.
      - Wählen Sie den Programmnamen in der Liste der installierten Programme aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
      - Öffnen Sie in der Liste der installierten Programme das Kontextmenü für den Programmnamen und wählen Sie den Punkt **Eigenschaften**.

        Das Fenster **Einstellungen für <Programmname>** wird geöffnet.

      Wenn auf das Programm derzeit die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht über das Fenster **Einstellungen für <Programmname>** geändert werden.

Gruppenaufgaben in Kaspersky Security Center anpassen

► *Gehen Sie wie folgt vor, um eine Gruppenaufgabe für mehrere Computer zu konfigurieren:*

1. Erweitern Sie den Knoten **"Verwaltete Geräte"** in der Struktur der Verwaltungskonsole von Kaspersky Security Center 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. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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 betätigen Sie den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.
4. 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. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie eine Aufgabe zur Untersuchung auf Befehl konfigurieren:
     a. Legen Sie im Abschnitt **Untersuchungsbereich** den Untersuchungsbereich fest.
     b. Konfigurieren Sie im Abschnitt **Einstellungen** die Integration in andere Programmkomponenten sowie die Aufgabenpriorität.

- Wenn Sie eine der Update-Aufgaben konfigurieren, aktivieren Sie die gewünschten Aufgabenparameter nach Ihren Bedürfnissen:

  a. Passen Sie im Abschnitt **Einstellungen** die Einstellungen für die Update-Quelle an und optimieren Sie die Nutzung des Laufwerk-Subsystems.

  b. Klicken Sie auf die Schaltfläche **Verbindungseinstellungen**, um die Einstellungen für die Verbindung mit Update-Quellen anzupassen.

- Wenn Sie die Aufgabe "Update der Programm-Module" anpassen, wählen Sie im Abschnitt **Einstellungen für das Update der Programm-Module anpassen** die Aktion aus, die ausgeführt werden soll: wichtige Updates der Programm-Module kopieren und installieren oder nur auf Vorhandensein prüfen.

- Wenn Sie die Aufgabe Update-Verteilung konfigurieren, geben Sie im Abschnitt **Einstellungen für die Update-Verteilung** die Zusammensetzung der Updates und den Ordner der lokalen Update-Quelle an, in der die Updates gespeichert werden sollen.

- Wenn Sie die Aufgabe Programm aktivieren konfigurieren, verwenden Sie im Block **Aktivierungsparameter** die Schlüsseldatei, mit deren Hilfe Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie einen Aktivierungscode oder eine Schlüsseldatei zur Verlängerung der Lizenz hinzufügen möchten.

- Wenn Sie die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstarts für die Computer-Kontrolle anpassen, geben Sie im Abschnitt **Einstellungen** die Einstellungen an, auf deren Grundlage die Liste der Erlaubnisregeln erstellt werden soll.

6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
8. 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 zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
9. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Die konfigurierbaren Einstellungen von Gruppenaufgaben sind in der Tabelle unten beschrieben.

Tabelle 18. Einstellungen für Gruppenaufgaben in Kaspersky Embedded Systems Security

Aufgabentyp in Kaspersky Embedded Systems Security	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts	**Einstellungen**	Beim Anpassen der Einstellungen der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" können Sie: • Erlaubnisregeln auf Grundlage gestarteter Programme erstellen. • Erlaubnisregeln für Programme aus den bestimmten Ordnern erstellen.
	Einstellungen	Sie können Aktionen festlegen, die bei der Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen: • **Digitales Zertifikat verwenden** • **Header und Fingerabdruck des digitalen Zertifikats verwenden** • **Falls kein Zertifikat vorhanden, Folgendes verwenden** • **SHA256-Hash verwenden** • **Regeln für Benutzer oder Benutzergruppe erstellen** Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Erstellen von Regeln für die Gerätekontrolle	**Einstellungen**	• Betriebsmodus auswählen: Systemdaten über alle jemals angeschlossenen Massenspeicher berücksichtigen oder nur derzeit angeschlossene Massenspeicher berücksichtigen. • Passen Sie die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln an, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Programm aktivieren (siehe Abschnitt "Aufgabe Programm aktivieren" auf Seite 133)	**Aktivierungsparameter**	Sie können für die Programmaktivierung oder für die Verlängerung der Lizenz eine Schlüsseldatei hinzufügen.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Update-Verteilung (siehe Abschnitt "Update-Aufgaben" auf Seite 134)	**Update-Quelle**	Sie können den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung 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 Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.
	Fenster **Verbindungseinstellungen**	Im Fenster **Verbindungseinstellungen**, das aus dem Abschnitt **Update-Quelle** verlinkt ist, können Sie festlegen, ob eine Verbindung zu den Kaspersky Lab-Update-Servern oder anderen Servern über einen Proxyserver hergestellt werden soll.
	Einstellungen für die Update-Verteilung	Sie können die Zusammensetzung der zu kopierenden Updates festlegen. Geben Sie im Feld **Ordner für die lokale Speicherung kopierter Updates** den Ordnerpfad an, in dem Kaspersky Embedded Systems Security die kopierten Updates speichern soll.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Update der Programm-Datenbanken (siehe Abschnitt "Update-Aufgaben" auf Seite 134)	**Einstellungen**	Im Gruppenfeld **Update-Quelle** können Sie den Administrationsserver von Kaspersky Security Center oder die Kaspersky Lab-Update-Server als Update-Quelle für die Programmaktualisierung 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 Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind. Im Abschnitt Optimierung der Nutzung des Festplatten-Subsystems können Sie die Funktion zur Verringerung der Auslastung des Festplatten-Subsystems anpassen: • **Belastung des Festplatten-Subsystems verringern** • **Für die Optimierung genutztes Arbeitsspeichervolumen (MB)**
	Fenster **Verbindungseinstellungen**	Im Fenster **Verbindungseinstellungen**, das aus dem Abschnitt **Update-Quelle** verlinkt ist, können Sie festlegen, ob eine Verbindung zu den Kaspersky Lab-Update-Servern oder anderen Servern über einen Proxyserver hergestellt werden soll.
	Zeitplan	Sie können die Einstellungen für den Start einer geplanten Aufgabe anpassen.
Update der Programm-Module (siehe Abschnitt "Update-Aufgaben" auf Seite 134)	**Update-Quelle**	Sie können den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung 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 Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.
	Fenster **Verbindungseinstellungen**	Im Gruppenfeld **Einstellungen für die Verbindung mit Update-Quellen** können Sie festlegen, ob eine Verbindung zu den Kaspersky Lab-Update-Servern oder anderen Servern über einen Proxyserver hergestellt werden soll.

	Einstellungen für das Update der Programm-Module anpassen	Sie können die Aktionen angeben, die Kaspersky Embedded Systems Security bei Vorliegen kritischer Updates der Programm-Module und bei Vorliegen von Informationen über verfügbare planmäßige Updates ausführen soll, sowie auch das Verhalten von Kaspersky Embedded Systems Security nach Abschluss der Installation kritischer Updates anpassen.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Untersuchung auf Befehl anpassen (siehe Abschnitt "Erstellen einer Aufgabe zur Untersuchung auf Befehl" auf Seite 437)	**Untersuchungsbereich**	Sie können einen Untersuchungsbereich für die Aufgabe zur Untersuchung auf Befehl festlegen sowie zur Einstellung der Sicherheitsstufe wechseln.
	Fenster **Untersuchung auf Befehl anpassen**	Im Fenster **Untersuchung auf Befehl anpassen**, das aus dem Abschnitt **Untersuchungsbereich** verlinkt ist, können Sie eine der vorbestimmten Sicherheitsstufen auswählen oder die Sicherheitsstufe manuell anpassen.
	Einstellungen	Im Gruppenfeld **Heuristische Analyse** können Sie die Verwendung der heuristischen Analyse in der Aufgabe zur Untersuchung auf Befehl aktivieren oder deaktivieren und die Analysetiefe mithilfe eines Schiebereglers anpassen. Konfigurieren Sie im Gruppenfeld **Integration mit anderen Komponenten** die folgenden Einstellungen: • Verwendung der vertrauenswürdigen Zone in den Aufgaben zur Untersuchung auf Befehl. • Verwendung von KSN in den Aufgaben zur Untersuchung auf Befehl. • Priorität der Aufgabe zur Untersuchung auf Befehl angeben: Aufgabe im Hintergrundmodus ausführen (niedrige Priorität) oder Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Integritätsprüfung für Programme (auf Seite 136)	**Zeitplan**	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Für die Aufgaben zum Rollback des Datenbanken-Updates können Sie nur die durch Kaspersky Security Center geregelten Standard-Einstellungen in den Abschnitten **Benachrichtigung** und **Ausnahmen vom Gültigkeitsbereich** anpassen.

Eine ausführliche Anleitung zur Konfiguration der Einstellungen in diesen Abschnitten finden Sie im *Hilfesystem von Kaspersky Security Center*.

In diesem Abschnitt

Aufgabe Programm aktivieren

► *Um die Aufgabe Programm aktivieren anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **"Verwaltete Geräte"** in der Struktur der Verwaltungskonsole von Kaspersky Security Center 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. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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 betätigen Sie den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.
4. 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 Reserveschlüssel verwenden**, wenn Sie einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.
6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).

7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
8. 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 Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center*

9. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**.

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Update-Aufgaben

► *Um die Aufgabe Update-Verteilung, Update der Programm-Datenbanken oder Update der Programm-Module anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **"Verwaltete Geräte"** in der Struktur der Verwaltungskonsole von Kaspersky Security Center 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. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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 betätigen Sie den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.
4. 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. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eine der folgenden Aktionen aus:
   - Passen Sie im Abschnitt **Update-Quelle** die Einstellungen für die Update-Quelle an und optimieren Sie die Nutzung des Laufwerk-Subsystems.
     a. Im Abschnitt **Update-Quelle** können Sie den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung 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 Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

b. Im Abschnitt **Optimierung der Nutzung des Festplatten-Subsystems** der Aufgabe Update der Programm-Datenbanken können Sie die Funktion konfigurieren, welche die Auslastung des Festplatten-Subsystems verringert:

- **Belastung des Festplatten-Subsystems verringern**

  Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktion zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher.

  Ist das Kontrollkästchen aktiviert, so ist die Funktion aktiv.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

- **Für die Optimierung genutztes Arbeitsspeichervolumen (MB)**

  Größe des Arbeitsspeichers (in MB), den das Programm für die Speicherung der Update-Dateien verwendet. Standardmäßig ist ein Arbeitsspeichervolumen von 512 MB eingestellt. Das minimale Arbeitsspeichervolumen beträgt 400 MB.

c. Klicken Sie auf die Schaltfläche **Verbindungseinstellungen** und passen Sie im folgenden Fenster **Verbindungseinstellungen** die Verwendung des Proxyservers für die Verbindung zu Kaspersky-Lab-Update-Servern und anderen Servern an.

- Im Abschnitt **Einstellungen für das Update der Programm-Module anpassen** der Aufgabe zum Update der Programm-Module können Sie die Aktionen angeben, die Kaspersky Embedded Systems Security bei Vorliegen kritischer Updates der Programm-Module und bei Vorliegen von Informationen über verfügbare planmäßige Updates ausführen soll. Außerdem können Sie das Verhalten von Kaspersky Embedded Systems Security nach Abschluss der Installation wichtiger Updates konfigurieren.
- Geben Sie im Abschnitt **Einstellungen für die Update-Verteilung** der Aufgabe zur Update-Verteilung die Zusammensetzung der Updates und den Ordner der lokalen Update-Quelle an, in der die Updates gespeichert werden sollen.

6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.

   Ausführliche Informationen zum Anpassen der Einstellungen in diesen Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center*

8. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Für ein Rollback des Datenbanken-Updates können Sie nur Standardaufgabeneinstellungen anpassen, die von Kaspersky Security Center in den Blöcken **Benachrichtigungen** und **Ausnahmen vom Gültigkeitsbereich der Aufgabe** kontrolliert werden. Ausführliche Informationen zum Anpassen der Einstellungen in diesen Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center*

Integritätsprüfung für Programme

► *Um die Gruppenaufgabe zur Integritätsprüfung für Programme anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **"Verwaltete Geräte"** in der Struktur der Verwaltungskonsole von Kaspersky Security Center 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. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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 betätigen Sie den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.
4. 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. Wählen Sie im Abschnitt **Geräte** die Geräte aus, für die Sie die Aufgabe zur Integritätsprüfung für Programme anpassen möchten.
6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
8. 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 Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center*
9. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**.

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Anpassen der Einstellungen für die Crash-Diagnose in Kaspersky Security Center

Wenn bei der Arbeit von Kaspersky Embedded Systems Security ein Problem auftreten sollte (z. B. Kaspersky Embedded Systems Security stürzt ab) und Sie möchten das Problem diagnostizieren, können Sie die Erstellung von Protokolldateien und einer Dump-Datei für die Prozesse von Kaspersky Embedded Systems Security aktivieren und diese Dateien zur Analyse an den Technischen Support von Kaspersky Lab übermitteln.

Kaspersky Embedded Systems Security versendet Protokoll- oder Dump-Dateien nicht automatisch. Nur ein Benutzer mit entsprechenden Rechten kann Diagnosedaten versenden.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsrechte konfigurieren (siehe Abschnitt "Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security" auf Seite 239) und nur bestimmten Benutzern Zugriff auf Protokolle, Protokoll- und Dump-Dateien gewähren.

► *Um die Einstellungen für die Crash-Diagnose in Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 126).
2. Öffnen Sie den Abschnitt **Crash-Diagnose** und gehen Sie wie folgt vor:
   - Wenn Sie Debug-Informationen in eine Datei schreiben möchten, aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern**.
     - Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.
     - Passen Sie die Genauigkeitsstufe für die Debug-Informationen an.

       In dieser Dropdown-Liste können Sie die Genauigkeitsstufe für die Debug-Informationen auswählen, die Kaspersky Embedded Systems Security in der Protokolldatei speichert.

       Sie können eine der folgenden Genauigkeitsstufen auswählen:

       - **Kritische Ereignisse** – Kaspersky Embedded Systems Security speichert nur Informationen über kritische Ereignisse in der Protokolldatei.
       - **Fehler** – Kaspersky Embedded Systems Security speichert Informationen über kritische Ereignisse und Fehler in der Protokolldatei.
       - **Wichtige Ereignisse** – Kaspersky Embedded Systems Security speichert Informationen über kritische Ereignisse, Fehler und wichtige Ereignisse in der Protokolldatei.
       - **Informative Ereignisse** – Kaspersky Embedded Systems Security speichert Informationen über kritische Ereignisse, Fehler, wichtige Ereignisse und informative Ereignisse in der Protokolldatei.

- **Alle Debug-Informationen** – Kaspersky Embedded Systems Security speichert sämtliche Debug-Informationen in der Protokolldatei.

Die Genauigkeitsstufe, die für ein bestimmtes Problem festgelegt werden soll, wird vom Experten des Technischen Supports definiert.

Standardmäßig ist die Genauigkeitsstufe **Alle Debug-Informationen** eingestellt.

Die Dropdown-Liste ist verfügbar, wenn das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern** aktiviert ist.

- Geben Sie die maximale Größe der Protokolldateien an.
- Geben Sie die Komponenten für das Debuggen an. Komponentencodes müssen durch einen Strichpunkt getrennt werden. Bei den Codes muss die Groß- und Kleinschreibung beachtet werden (siehe Tabelle unten).

Tabelle 19. Subsystemcodes in Kaspersky Embedded Systems Security

Code des Subsystems	Name des Subsystems
*	Alle Komponenten.
gui	Subsystem der Benutzeroberfläche, Snap-In von Kaspersky Embedded Systems Security in der Microsoft Management Console.
ak_conn	Subsystem zur Integration des Administrationsagenten von Kaspersky Security Center.
bl	Steuerungsprozess, implementiert Steuerungsaufgaben von Kaspersky Embedded Systems Security
wp	Arbeitsprozess, der die Aufgaben zum Antiviren-Schutz realisiert
blgate	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security
ods	Subsystem für Untersuchung auf Befehl
oas	Subsystem für den Echtzeitschutz für Dateien
qb	Subsystem für Quarantäne und Backup-Speicher
scandll	Hilfsmodul für die Untersuchung auf Viren
core	Subsystem für die Antiviren-Basisfunktionalität
avscan	Subsystem für die Antiviren-Bearbeitung
avserv	Subsystem zur Steuerung des Antiviren-Kerns
prague	Subsystem für die Basisfunktionalität
updater	Subsystem für das Datenbanken-Update und das Update der Programm-Module
snmp	Subsystem für Unterstützung des SNMP-Protokolls
perfcount	Subsystem für Leistungsindikatoren

Die Einstellungen für die Protokollierung von Snap-ins für Kaspersky Embedded Systems Security (gui) und das Verwaltungs-Plug-in für Kaspersky Security Center (ak_conn) werden nach dem Neustart dieser Komponenten übernommen. Die Einstellungen für die Protokollierung des Subsystems zur SNMP-Unterstützung (snmp) werden nach dem Neustart des SNMP-Dienstes übernommen. Die Trace-Parameter für das Subsystem der Leistungsindikatoren (perfcount) werden nach einem Neustart aller Prozesse angewandt, die die Leistungsindikatoren verwenden. Die Einstellungen für die Protokollierung der übrigen Subsysteme von Kaspersky Embedded Systems Security werden sofort nach dem Speichern der Einstellungen für die Fehlerdiagnose wirksam.

Standardmäßig werden in Kaspersky Embedded Systems Security sämtliche Debug-Informationen für alle Komponenten von Kaspersky Embedded Systems Security protokolliert.

Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern** aktiviert ist.

- Wenn Sie eine Dump-Datei erstellen möchten, aktivieren Sie das Kontrollkästchen **Dump-Datei erstellen**.
  - Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Dump-Datei speichern soll.

3. Klicken Sie auf **OK**.

Die festgelegten Programmeinstellungen werden auf dem geschützten Computer übernommen.

Arbeit mit dem Aufgabenzeitplan

Sie können den Start der Aufgaben von Kaspersky Embedded Systems Security nach Zeitplan einrichten sowie die diesbezüglichen Einstellungen anpassen.

In diesem Abschnitt

Einstellungen des Zeitplans für den Aufgabenstart anpassen

In der Programmkonsole können Sie den Startzeitplan für lokale Systemaufgaben und benutzerdefinierte Aufgaben anpassen. Für den Start von Gruppenaufgaben kann der Zeitplan nicht angepasst werden.

► *Um die Zeitplan-Einstellungen für den Gruppenaufgabenstart anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Wählen Sie die Gruppe aus, zu der der geschützte Server gehört.
3. Wählen Sie im Ergebnisbereich die Registerkarte **Aufgaben** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie auf den Namen der Aufgabe.
   - Öffnen Sie das Kontextmenü für den Namen der Aufgabe und wählen Sie den Punkt "Eigenschaften".
5. Wählen Sie den Abschnitt **Zeitplan** aus.
6. Aktivieren Sie im Block **Zeitplan-Einstellungen** das Kontrollkästchen Aufgabe nach Zeitplan starten.

Die Felder mit den Zeitplan-Einstellungen der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe stehen nicht zur Verfügung, wenn der Start der Aufgabe durch eine Richtlinie von Kaspersky Security Center verboten ist.

7. Passen Sie die Zeitplaneinstellungen entsprechend Ihren Anforderungen an. Gehen Sie hierzu wie folgt vor:

   a. Wählen Sie in der Liste Startintervall einen der folgenden Werte aus:

      - Stündlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Stunden gestartet wird, wobei Sie die Anzahl der Stunden im Feld **Alle <Anzahl> Std.** eingeben müssen.
      - Täglich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Tagen gestartet wird, wobei Sie die Anzahl der Tage im Feld **Alle <Anzahl> Tage** eingeben müssen.
      - Wöchentlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl von Wochen gestartet wird, wobei Sie die Anzahl der Wochen im Feld **Alle <Anzahl> Wochen** eingeben müssen. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (Standardmäßig werden Aufgaben montags gestartet).
      - Bei Programmstart, wenn Sie möchten, dass die Aufgabe bei jedem Start von Kaspersky Embedded Systems Security ausgeführt wird.
      - Nach dem Update der Programm-Datenbanken, wenn Sie möchten, dass die Aufgabe nach jedem Update der Programm-Datenbanken gestartet wird.

   b. Legen Sie im Feld Startzeit die Uhrzeit des erstmaligen Aufgabenstarts fest.

   c. Tragen Sie im Feld Startdatum das Startdatum des Zeitplans ein.

   Nachdem Sie das Startintervall der Aufgabe, die Uhrzeit für den erstmaligen Aufgabenstart und das Datum, ab dem der Zeitplan gelten soll, angegeben haben, wird im oberen Bereich des Fensters im Feld Nächster Start der berechnete Zeitpunkt des nächsten Aufgabenstarts angezeigt. Aktualisierte Informationen über die Zeit, die bis zum nächsten Start verbleibt, werden jedes Mal angezeigt, wenn Sie das Fenster Aufgabeneinstellungen auf der Registerkarte Zeitplan öffnen.
   Der Wert Durch Richtlinie verboten im Feld Nächster Start wird angezeigt, wenn der Start von geplanten Systemaufgaben durch die Einstellungen der aktiven Richtlinie des Programms Kaspersky Security Center verboten ist (siehe Abschnitt "Zeitplan für den Start von lokalen Systemaufgaben anpassen" auf S. 103).

8. Passen Sie auf der Registerkarte Erweitert die folgenden Zeitplaneinstellungen gemäß Ihren Anforderungen an.

   - Im Abschnitt Einstellungen für das Anhalten der Aufgabe:

     a. Aktivieren Sie das Kontrollkästchen Dauer und geben Sie die erforderliche Anzahl an Stunden und Minuten in den Feldern rechts davon ein, um so die maximale Dauer der Aufgabenausführung vorzugeben.

     b. Aktivieren Sie das Kontrollkästchen Anhalten von und geben Sie die Anfangszeit und Endzeit des Zeitintervalls in den Feldern rechts davon ein, um einen Zeitraum innerhalb von 24 Stunden anzugeben, in dem die Aufgabenausführung angehalten wird.

- Im Abschnitt Erweiterte Einstellungen:
  a. Aktivieren Sie das Kontrollkästchen Zeitplan deaktivieren ab und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.
  b. Aktivieren Sie das Kontrollkästchen Übersprungene Aufgaben starten, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.
  c. Aktivieren Sie das Kontrollkästchen Aufgabenstart zufällig wählen innerhalb von und geben Sie einen Wert in Minuten ein.

9. Klicken Sie auf OK.
10. 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, gehen Sie wie im Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen (auf Seite 126) beschrieben vor.

Start nach Zeitplan aktivieren und deaktivieren

Sie können den Aufgabenstart nach Zeitplan sowohl vor als auch nach der Anpassung des Zeitplans aktivieren oder deaktivieren.

► *Um die den Zeitplan für den Aufgabenstart zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Aufgabennamen, für den Sie den Startzeitplan anpassen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
3. Führen Sie im folgenden Fenster auf der Registerkarte **Zeitplan** eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**, wenn Sie den Aufgabenstart nach Zeitplan aktivieren möchten
   - Deaktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**, wenn Sie den Aufgabenstart nach Zeitplan deaktivieren möchten

   > Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden nicht gelöscht und kommen bei der nächsten Aktivierung des Aufgabenstarts nach Zeitplan zur Anwendung.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden gespeichert.

Berichterstellung 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

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: *Läuft, Angehalten, Beendet, Fehlgeschlagen, Nicht installiert, Wird gestartet*.

Der Status *Nicht installiert* bezieht sich auf die Komponente, nicht auf das Programm selbst. Wenn das Programm nicht installiert ist, zeigt Kaspersky Security Center als Status N/A (Nicht verfügbar) an.

Sie können eine Komponentenauswahl erstellen und den Filter verwenden, um Netzwerkgeräte mit der 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 Verwaltungskonsole von Kaspersky Security Center 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** (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

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 Struktur der Verwaltungskonsole den Knoten **Administrationsserver <Computername>**.
2. Öffnen Sie die Registerkarte **Reports**.
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 Ausführung der Aufgabe zur Kontrolle des Programmstarts können zwei Arten von Berichten erstellt werden: ein Bericht über verbotene Programme (wenn die Aufgabe im Modus Aktiv gestartet wurde) sowie ein Bericht über verbotene Programme im Testmodus (wenn die Aufgabe im Modus Nur Statistik gestartet wurde). Diese Berichte enthalten Informationen über blockierte Programme auf den geschützten Computern im Netzwerk. Jeder Bericht wird für alle Administrationsgruppen erstellt und sammelt die Daten aller Kaspersky-Lab-Programme, die auf den geschützten Geräten installiert sind.

► *Um einen Bericht über verbotene Programme im Testmodus anzuzeigen, gehen Sie wie folgt vor:*

1. Starten Sie die Aufgabe zur Programmkontrolle im Modus "Nur Statistik" (siehe Abschnitt "Aufgabeneinstellungen für Kontrolle des Programmstarts konfigurieren" auf Seite 320).
2. Wählen Sie in der Struktur der Verwaltungskonsole den Knoten **Administrationsserver <Computername>**.
3. Öffnen Sie die Registerkarte **Reports**.
4. Doppelklicken Sie auf das Listenelement **Bericht über verbotene Programme im Testmodus**.

   Ein Bericht wird erstellt.
5. Passen Sie die folgenden Einstellungen für Anfragen an:
   - ein Schaubild mit den zehn Programmen, deren Start am häufigsten verboten 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. Starten Sie die Aufgabe zur Programmkontrolle im Modus "Aktiv" (siehe Abschnitt "Aufgabeneinstellungen für Kontrolle des Programmstarts konfigurieren" auf Seite 320).
2. Wählen Sie in der Struktur der Verwaltungskonsole den Knoten **Administrationsserver <Computername>**.
3. Öffnen Sie die Registerkarte **Reports**.
4. Doppelklicken Sie auf das Listenelement **Bericht über verbotene Programme**.

   Ein Bericht wird erstellt.

Dieser Bericht enthält die gleichen Datenblocks wie der Bericht über verbotene Programme im Testmodus.

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 oder einem anderen Computer installiert ist.

In diesem Kapitel

Einstellungen von Kaspersky Embedded Systems Security in der Programmkonsole

Die allgemeinen Einstellungen und die Einstellungen für die Crash-Diagnose von Kaspersky Embedded Systems Security legen die generellen Bedingungen für die Ausführung 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 zur Ablaufverfolgung; Anlegen einer Dump-Datei für Prozesse von Kaspersky Embedded Systems Security bei deren Absturz; andere allgemeine Einstellungen.

Die Programmeinstellungen sind in der Programmkonsole nicht verfügbar, wenn in der aktiven Richtlinie von Kaspersky Security Center ein Verbot von Änderungen der festgelegten Einstellungen definiert ist.

► *Um die Einstellungen von Kaspersky Embedded Systems Security anzupassen, gehen Sie wie folgt vor:*

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** aus.

   Das Fenster **Programmeinstellungen** wird geöffnet.
2. Legen Sie im nächsten Fenster die allgemeinen Einstellungen von Kaspersky Embedded Systems Security gemäß Ihren Anforderungen fest:
   - Auf der Registerkarte **Skalierbarkeit und Oberfläche** können Sie folgende Einstellungen anpassen:
     - Im Abschnitt **Skalierbarkeitseinstellungen**:
       - Maximale Anzahl der Arbeitsprozesse, die von Kaspersky Embedded Systems Security gestartet werden können

Tabelle 20. Maximale Anzahl aktiver Prozesse

<table>
<tr><th>Einstellung</th><th>Maximale Anzahl aktiver Prozesse</th></tr>
<tr><td>Beschreibung</td><td>Diese Einstellung bezieht sich auf die Gruppe Skalierbarkeitseinstellungen von Kaspersky Embedded Systems Security. Er bestimmt die maximale Anzahl der aktiven Prozesse, die das Programm gleichzeitig starten kann.
Eine Steigerung der Anzahl von parallel laufenden Prozessen erhöht die Geschwindigkeit bei der Überprüfung der Dateien und Stabilität von Kaspersky Embedded Systems Security. Allerdings kann ein erhöhter Wert dieses Parameters die Computerleistung beeinträchtigen und den Bedarf an Arbeitsspeicher erhöhen.
In der Verwaltungskonsole von Kaspersky Security Center können Sie den Parameter Maximale Anzahl aktiver Prozesse nur für Kaspersky Embedded Systems Security auf einem einzelnen Computer einstellen (im Dialogfenster Programmeinstellungen). Diese Einstellung kann in den Richtlinieneigenschaften für eine Computergruppe nicht geändert werden.</td></tr>
<tr><td>Mögliche Werte</td><td>1– 8</td></tr>
<tr><td>Standardwert</td><td>Das Programm führt die Skalierung in Abhängigkeit von der Anzahl der Prozessoren auf dem Computer automatisch aus:
<table>
<tr><th>Anzahl der Prozessoren</th><th>Maximale Anzahl aktiver Prozesse</th></tr>
<tr><td>1</td><td>1</td></tr>
<tr><td>1< Anzahl der Prozesse < 4</td><td>2</td></tr>
<tr><td>4 und mehr</td><td>4</td></tr>
</table>
</td></tr>
</table>

       - Anzahl der Prozesse für den Echtzeitschutz

Tabelle 21. Anzahl der Prozesse für den Echtzeitschutz

Einstellung	**Anzahl der Prozesse für den Echtzeitschutz**
Beschreibung	Diese Einstellung bezieht sich auf die Gruppe **Skalierbarkeitseinstellungen** von Kaspersky Embedded Systems Security. Mit dieser Einstellung können Sie eine feste Anzahl von Prozessen festlegen, in denen Kaspersky Embedded Systems Security die Aufgaben zum Echtzeitschutz ausführt. Ein höherer Wert dieses Parameters wird eine Erhöhung der Überprüfungsgeschwindigkeit in den Aufgaben des Echtzeitschutzes für Dateien bewirken. Je höher allerdings die Anzahl der von Kaspersky Embedded Systems Security benutzten Prozesse, umso größer wird der Einfluss auf die Gesamtleistung des geschützten Computers und auf die Arbeitsspeicherressourcen sein. In der Verwaltungskonsole von Kaspersky Security Center können Sie die Einstellung **Anzahl der Prozesse für den Echtzeitschutz** nur für Kaspersky Embedded Systems Security auf einem einzelnen Computer einstellen (im Fenster **Programmeinstellungen**). Diese Einstellung kann in den Richtlinieneigenschaften für eine Computergruppe nicht geändert werden.
Mögliche Werte	Mögliche Werte: 1-N, wobei N der Wert ist, der durch die Einstellung **Maximale Anzahl aktiver Prozesse** bestimmt wird. Wenn Sie für den Einstellungswert **Anzahl der Prozesse für den Echtzeitschutz** den gleichen Wert festlegen wie für die maximale Anzahl der aktiven Prozesse, senken Sie den Einfluss von Kaspersky Embedded Systems Security auf die Geschwindigkeit der Dateiübertragung zwischen Computern, während die Geschwindigkeit des Echtzeitschutzes weiter erhöht wird. Update-Aufgaben und Aufgaben zur Untersuchung auf Befehl mit der Basispriorität **Mittel (Normal)** werden trotzdem in bereits gestarteten Prozessen von Kaspersky Embedded Systems Security ausgeführt. Dabei verlangsamt sich die Ausführung von Aufgaben zur Untersuchung auf Befehl. Falls die Ausführung einer Aufgabe zum Absturz eines Prozesses führt, ist für seinen Neustart mehr Zeit erforderlich. Aufgaben zur Untersuchung auf Befehl mit der Basispriorität **Niedrig** werden immer in einem separaten Prozess bzw. separaten Prozessen ausgeführt.
Standardwert	Kaspersky Embedded Systems Security führt die Skalierung in Abhängigkeit von der Anzahl der Prozessoren auf dem Computer automatisch aus:

Anzahl der Prozessoren	**Anzahl der Prozesse für den Echtzeitschutz**
=1	1
>1	2

- Anzahl der aktiven Prozesse für im Hintergrund laufende Aufgaben zur Untersuchung auf Befehl

Tabelle 22. Anzahl der Prozesse für im Hintergrund ausgeführte Untersuchung auf Befehl

Einstellung	**Anzahl der Prozesse für im Hintergrund ausgeführte Untersuchung auf Befehl**
Beschreibung	Diese Einstellung bezieht sich auf die Gruppe **Skalierbarkeitseinstellungen** von Kaspersky Embedded Systems Security. Mit Hilfe dieser Einstellung können Sie die maximale Anzahl der Prozesse angeben, in denen das Programm die Aufgaben zur Untersuchung auf Befehl im Hintergrundmodus ausführen soll. Die Anzahl der Prozesse, die Sie durch diese Einstellung festlegen, zählt nicht zur Anzahl der aktiven Prozesse von Kaspersky Embedded Systems Security, die durch die Einstellung **Maximale Anzahl aktiver Prozesse** bestimmt wird. Beispielsweise, wenn Sie die folgenden Parameterwerte einstellen: • Maximale Anzahl aktiver Prozesse – 3. • Anzahl der Prozesse für Echtzeitschutz-Aufgaben – 3. • Anzahl der Prozesse für im Hintergrund ausgeführte Untersuchung auf Befehl – 1. und anschließend die Aufgabe zum Echtzeitschutz und eine Aufgabe zur Untersuchung auf Befehl im Hintergrundmodus starten, weist die Anzahl der aktiven Prozesse kavfswp.exe von Kaspersky Embedded Systems Security den Wert 4 auf. In einem aktiven Prozess mit niedriger Priorität können mehrere Aufgaben zur Untersuchung auf Befehl ausgeführt werden. Sie können die Anzahl der aktiven Prozesse beispielsweise erhöhen, wenn Sie gleichzeitig mehrere Aufgaben im Hintergrundmodus starten, damit jede Aufgabe einen einzelnen Prozess erhält. Die Zuweisung separater Aufgabenprozesse erhöht die Zuverlässigkeit und Geschwindigkeit der Aufgaben.
Mögliche Werte	1-4
Standardwert	1

- Wählen Sie im Abschnitt **Interaktion mit dem Benutzer** aus, ob das Taskleistensymbol nach jedem Start des Programms in der Taskleiste angezeigt werden soll (siehe Abschnitt "Taskleistensymbol im Infobereich" auf Seite 157).

- Auf der Registerkarte **Sicherheit und Zuverlässigkeit** können Sie folgende Einstellungen anpassen:
  - Geben Sie im Abschnitt **Einstellungen für Zuverlässigkeit** die Anzahl der Versuche zur Wiederherstellung von Aufgaben zur Untersuchung auf Befehl nach deren Absturz an.

Tabelle 23. Aufgaben wiederherstellen

Einstellung	Aufgaben wiederherstellen (**Wiederherstellen von Aufgaben ausführen**)
Beschreibung	Diese Einstellung bezieht sich auf die Gruppe **Einstellungen für Zuverlässigkeit** von Kaspersky Embedded Systems Security. Er umfasst die Wiederherstellung von Aufgaben, die mit einem Absturz abgeschlossen wurden, und legt die Anzahl der Wiederherstellungsversuche für Aufgaben zur Untersuchung auf Befehl zur Virensuche fest. Wenn eine Aufgabe abstürzt, versucht der Prozess kavfs.exe von Kaspersky Embedded Systems Security, den Prozess, in dem die Aufgabe zum Zeitpunkt des Absturzes ausgeführt wurde, neu zu starten. Wenn die Aufgabenwiederherstellung deaktiviert ist, stellt das Programm Aufgaben zum Echtzeitschutz und zur Untersuchung auf Befehl nicht wieder her. Wenn die Aufgabenwiederherstellung aktiviert ist, versucht das Programm, Aufgaben zum Echtzeitschutz wiederherzustellen, bis sie erfolgreich gestartet werden. Die Wiederherstellung von Aufgaben zur Untersuchung auf Befehl wird so oft versucht, wie durch diese Einstellung festgelegt ist.
Mögliche Werte	Aktiviert / deaktiviert. Anzahl der Versuche zur Wiederherstellung einer Aufgabe zur Untersuchung auf Befehl – 1-10.
Standardwert	Wiederherstellung von Aufgaben aktiviert. Anzahl der Versuche zur Wiederherstellung einer Aufgabe zur Untersuchung auf Befehl – 2.

- Legen Sie im Abschnitt **Aktionen beim Wechsel in den USV-Akkubetrieb** die Aktionen fest, die Kaspersky Embedded Systems Security nach dem Wechsel in den USV-Akkubetrieb ausführen soll:

Tabelle 24. Aktionen bei der Arbeit mit einer unterbrechungsfreien Stromversorgungsquelle

Einstellung	Aktionen beim Wechsel in den USV-Akkubetrieb:
Beschreibung	Diese Einstellung bestimmt die Aktionen, die Kaspersky Embedded Systems Security ausführt, wenn der Computer zur unterbrechungsfreien Stromversorgung gewechselt hat.
Mögliche Werte	Geplante Aufgaben zur Untersuchung auf Befehl starten oder nicht starten. Alle ausführbaren Aufgaben zur Untersuchung auf Befehl ausführen oder beenden.
Standardwert	Standardmäßig läuft Kaspersky Embedded Systems Security bei unterbrechungsfreier Stromversorgung des Computers in folgendem Modus: • Aufgaben zur Untersuchung auf Befehl, die nach Zeitplan laufen, werden nicht gestartet • Alle aktiven Aufgaben zur Untersuchung auf Befehl werden automatisch beendet

- Passen Sie im Abschnitt **Einstellungen für den Kennwortschutz** die Einstellungen für den Kennwortschutz der Programmfunktionen an (siehe Abschnitt "Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security" auf Seite 246) an.

- Auf der Registerkarte **Verbindungseinstellungen**:
  - Geben Sie im Abschnitt **Proxyserver-Einstellungen** die Einstellungen für die Verwendung eines Proxyservers an.
  - Geben Sie im Abschnitt **Einstellungen für die Authentifizierung auf dem Proxyserver** den Authentifizierungstyp und die notwendigen Daten für die Authentifizierung auf dem Proxyserver an.
  - Geben Sie im Abschnitt **Lizenzverwaltung** an, ob Kaspersky Security Center als Proxyserver für die Programmaktivierung verwendet wird.
- Auf der Registerkarte **Crash-Diagnose**:
  - Wenn Sie Debug-Informationen in eine Datei schreiben möchten, aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern**.
    - Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.
    - Passen Sie die Genauigkeitsstufe für die Debug-Informationen an.

      In dieser Dropdown-Liste können Sie die Genauigkeitsstufe für die Debug-Informationen auswählen, die Kaspersky Embedded Systems Security in der Protokolldatei speichert.

      Sie können eine der folgenden Genauigkeitsstufen auswählen:

      - **Kritische Ereignisse** – Kaspersky Embedded Systems Security speichert nur Informationen über kritische Ereignisse in der Protokolldatei.
      - **Fehler** – Kaspersky Embedded Systems Security speichert Informationen über kritische Ereignisse und Fehler in der Protokolldatei.
      - **Wichtige Ereignisse** – Kaspersky Embedded Systems Security speichert Informationen über kritische Ereignisse, Fehler und wichtige Ereignisse in der Protokolldatei.
      - **Informative Ereignisse** – Kaspersky Embedded Systems Security speichert Informationen über kritische Ereignisse, Fehler, wichtige Ereignisse und informative Ereignisse in der Protokolldatei.
      - **Alle Debug-Informationen** – Kaspersky Embedded Systems Security speichert sämtliche Debug-Informationen in der Protokolldatei.

      Die Genauigkeitsstufe, die für ein bestimmtes Problem festgelegt werden soll, wird vom Experten des Technischen Supports definiert.

      Standardmäßig ist die Genauigkeitsstufe **Alle Debug-Informationen** eingestellt.

      Die Dropdown-Liste ist verfügbar, wenn das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern** aktiviert ist.

    - Geben Sie die maximale Größe der Protokolldateien an.
    - Geben Sie die Komponenten für das Debuggen an.

      Eine Liste mit Codes für Komponenten von Kaspersky Embedded Systems Security, deren Debug-Informationen vom Programm in einer Protokolldatei gespeichert werden. Komponentencodes müssen durch einen Strichpunkt getrennt werden. Bei den Codes muss die Groß- und Kleinschreibung beachtet werden (siehe Tabelle unten).

Tabelle 25. Subsystemcodes in Kaspersky Embedded Systems Security

Code des Subsystems	Name des Subsystems
*	Alle Komponenten.
gui	Subsystem der Benutzeroberfläche, Snap-In von Kaspersky Embedded Systems Security in der Microsoft Management Console.
ak_conn	Subsystem zur Integration des Administrationsagenten von Kaspersky Security Center.
bl	Steuerungsprozess, implementiert Steuerungsaufgaben von Kaspersky Embedded Systems Security
wp	Arbeitsprozess, der die Aufgaben zum Antiviren-Schutz realisiert
blgate	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security
ods	Subsystem für Untersuchung auf Befehl
oas	Subsystem für den Echtzeitschutz für Dateien
qb	Subsystem für Quarantäne und Backup-Speicher
scandll	Hilfsmodul für die Untersuchung auf Viren
core	Subsystem für die Antiviren-Basisfunktionalität
avscan	Subsystem für die Antiviren-Bearbeitung
avserv	Subsystem zur Steuerung des Antiviren-Kerns
prague	Subsystem für die Basisfunktionalität
updater	Subsystem für das Datenbanken-Update und das Update der Programm-Module
snmp	Subsystem für Unterstützung des SNMP-Protokolls
perfcount	Subsystem für Leistungsindikatoren

Die Einstellungen für die Protokollierung von Snap-ins für Kaspersky Embedded Systems Security (gui) und das Verwaltungs-Plug-in von Kaspersky Embedded Systems Security für Kaspersky Security Center (ak_conn) werden nach dem Neustart dieser Komponenten übernommen. Die Einstellungen für die Protokollierung des Subsystems zur SNMP-Unterstützung (snmp) werden nach dem Neustart des SNMP-Dienstes übernommen. Die Trace-Parameter für das Subsystem der Leistungsindikatoren (perfcount) werden nach einem Neustart aller Prozesse angewandt, die die Leistungsindikatoren verwenden. Die Einstellungen für die Protokollierung der übrigen Subsysteme von Kaspersky Embedded Systems Security werden sofort nach dem Speichern der Einstellungen für die Fehlerdiagnose wirksam.

Standardmäßig werden in Kaspersky Embedded Systems Security sämtliche Debug-Informationen für alle Komponenten von Kaspersky Embedded Systems Security protokolliert.

Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern** aktiviert ist.

- Wenn Sie eine Dump-Datei erstellen möchten, aktivieren Sie das Kontrollkästchen **Bei Absturz Dump-Datei erstellen**.

Kaspersky Embedded Systems Security versendet Protokoll- oder Dump-Dateien nicht automatisch. Nur ein Benutzer mit entsprechenden Rechten kann Diagnosedaten versenden.

- Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Dump-Datei speichern soll.

Die Informationen in den Dump-Dateien des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsrechte konfigurieren (siehe Abschnitt "Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security" auf Seite 239) und nur bestimmten Benutzern Zugriff auf Protokolle, Protokoll- und Dump-Dateien gewähren.

1. Klicken Sie auf **OK**.

Die Einstellungen von Kaspersky Embedded Systems Security werden gespeichert.

Über die Konsole für Kaspersky Embedded Systems Security

Die Konsole für Kaspersky Embedded Systems Security ist ein isoliertes Snap-in, das in die Microsoft Management Console eingefügt wird.

Sie können das Programm über die Programmkonsole verwalten, die auf dem geschützten Computer oder auf einem anderen Computer im Unternehmensnetzwerk installiert ist.

Nachdem die Programmkonsole auf einem anderen Computer installiert wurde, ist eine erweiterte Konfiguration erforderlich.

Wenn die Programmkonsole und Kaspersky Embedded Systems Security auf verschiedenen Computern installiert sind, die zu verschiedenen Domänen gehören, kann es vorkommen, dass nicht alle Informationen über das Programm in der Programmkonsole verfügbar sind. Beispielsweise wird nach dem Start einer Aufgabe in der Programmkonsole der Status dieser Aufgabe in der Programmkonsole möglicherweise nicht mehr aktualisiert.

Beim Installieren der Programmkonsole speichert der Installationsassistent die Datei kavfs.msc im Installationsordner und fügt das Snap-in für Kaspersky Embedded Systems Security zur Liste der isolierten Microsoft Windows-Snap-ins hinzu.

Sie können die Programmkonsole über das **Startmenü** öffnen. Sie können die msc-Datei des Snap-ins von Kaspersky Embedded Systems Security starten oder als neues Element zur Struktur einer vorhandenen Microsoft Management Console hinzufügen.

In der 64-Bit-Version von Microsoft Windows können Sie das Snap-in von Kaspersky Embedded Systems Security nur in der 32-Bit-Version der Microsoft Management Console hinzufügen. Öffnen Sie dazu die Microsoft Management Console aus der Befehlszeile mit dem Befehl mmc.exe /32.

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 Computer zu verwalten, auf denen Kaspersky Embedded Systems Security installiert ist.

Benutzeroberfläche der Konsole für Kaspersky Embedded Systems Security

Die Konsole für Kaspersky Embedded Systems Security wird in der Struktur der Microsoft Management Console als Knoten angezeigt.

Nachdem eine Verbindung mit dem Programm Kaspersky Embedded Systems Security, das auf einem anderen Computer installiert ist, hergestellt wurde, werden der Name des Computers, auf dem das Programm installiert ist, sowie der Name des Benutzerkontos, mit dessen Rechten die Verbindung hergestellt wurde, zur Bezeichnung des Knotens hinzugefügt: **Kaspersky Embedded Systems Security <Computername> als <Computername>**. Nachdem die Verbindung mit Kaspersky Embedded Systems Security, das auf demselben Computer wie die Programmkonsole installiert ist, hergestellt wurde, ändert sich der Knotenname in **Kaspersky Embedded Systems Security**.

Standardmäßig enthält das Fenster der Programmkonsole folgende Elemente:

- Struktur der Programmkonsole
- Ergebnisfenster
- Werkzeugleiste

Die Programmkonsolenstruktur

Die Struktur der Programmkonsole enthält den Knoten **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**: Verwaltung des Echtzeitschutzes und der Einstellungen für die Verwendung von KSN-Diensten. Im Knoten **Echtzeit-Computerschutz** können die folgenden Aufgaben angepasst werden:
  - **Echtzeitschutz für Dateien**
  - **Verwendung von KSN**
- **Computer-Kontrolle**: Kontrolle der Starts der auf dem geschützten Computer installierten Programme und der Verbindungen zu externen Geräten. Im Knoten **Computer-Kontrolle** können die folgenden Aufgaben verwaltet werden:
  - **Kontrolle des Programmstarts**
  - **Gerätekontrolle**
  - **Firewall-Verwaltung**

- **Automatisches Erstellen von Regeln**: passt die automatische Erstellung von Gruppen- und Systemregeln für die Aufgaben "Kontrolle des Programmstarts" und "Gerätekontrolle" an.
  - **Automatisches 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 (siehe Abschnitt "Kategorien der Aufgaben von Kaspersky Embedded Systems Security" auf Seite 158) werden mithilfe von Kaspersky Security Center erstellt. Gruppenaufgaben können nicht über die Programmkonsole verwaltet werden.
- **System-Diagnose**: Anpassen der Steuerung von Dateioperationen und der Einstellungen für die Analyse des Windows-Ereignisprotokolls.
  - **Überwachung der Datei-Integrität**
  - **Protokollanalyse**
- **Untersuchung auf Befehl**: Verwalten der Aufgabe zur Virensuche. Jede Aufgabe hat ihr eigenes Steuerelement:
  - **Untersuchung beim Hochfahren des Betriebssystems**
  - **Untersuchung wichtiger Bereiche**
  - **Untersuchung von Quarantäne-Objekten**
  - **Integritätsprüfung für Programme**
  - Benutzerdefinierte Aufgaben **<Namen der Aufgaben>** (sofern vorhanden).

  Im Knoten werden Systemaufgaben (siehe Abschnitt "Kategorien der Aufgaben von Kaspersky Embedded Systems Security" auf Seite 158), bei der Installation erstellte Programme, hinzugefügte benutzerdefinierte Aufgaben sowie Gruppenaufgaben zur Untersuchung auf Befehl angezeigt, die mithilfe von Kaspersky Security Center erstellt und an den Computer übertragen wurden.
- **Update**: Verwaltet Datenbanken-Updates und Updates der Module für Kaspersky Embedded Systems Security und kopiert das Update in einen Ordner als lokale Update-Quelle. Der Knoten enthält untergeordnete Knoten für die Steuerung jeder Update-Aufgabe und für die Aufgabe "Rollback des Datenbanken-Updates":
  - **Update der Programm-Datenbanken**
  - **Update der Programm-Module**
  - **Update-Verteilung**
  - **Rollback des Datenbanken-Updates**

  Im Knoten werden alle benutzerdefinierten und Gruppen-Update-Aufgaben (siehe Abschnitt "Kategorien der Aufgaben von Kaspersky Embedded Systems Security" auf Seite 158) angezeigt, die mithilfe von Kaspersky Security Center erstellt und an den Computer übertragen wurden.
- **Speicher**: Verwaltung der Einstellungen für Quarantäne und Backup.
  - **Quarantäne**
  - **Backup**

- **Protokolle und Benachrichtigungen**: Verwaltung der lokalen Protokolle der Aufgabenausführung, des Sicherheitsprotokolls und des Systemaudit-Protokolls von Kaspersky Embedded Systems Security.
  - **Sicherheitsprotokoll**
  - **Systemaudit-Protokoll**
  - **Protokolle der Aufgabenausführung**
- **Lizenzverwaltung**: Hinzufügen und Löschen von Schlüsseln und Aktivierungscodes für Kaspersky Embedded Systems Security, Anzeige von Informationen über Lizenzen

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 Computers (siehe Abschnitt "Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen" auf Seite 171) und Informationen über Kaspersky Embedded Systems Security, den Schutzstatus seiner funktionellen Komponenten und die Gültigkeitsdauer der Lizenz angezeigt.

Kontextmenü des Knotens "Kaspersky Embedded Systems Security"

Mithilfe der Punkte im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** können Sie folgende Aktionen ausführen:

- **Verbindung mit anderem Computer herstellen**. Verbindung mit anderem Computer herstellen (siehe Abschnitt "Kaspersky Embedded Systems Security über die Programmkonsole auf einem anderen Computer verwalten" auf Seite 158), um Kaspersky Embedded Systems Security zu verwalten, das darauf installiert ist. Hierfür können Sie auch den Link in der rechten unteren Ecke im Detailbereich des Knotens **Kaspersky Embedded Systems Security** verwenden.
- **Dienst starten** / **Dienst beenden**. Programm oder eine ausgewählte Aufgabe starten oder beenden (siehe Abschnitt "Manuelles Starten / Anhalten / Fortsetzen / Beenden einer Aufgabe" auf Seite 160). Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden. Dies kann auch über das Kontextmenü der Aufgaben des Programms erfolgen.
- **Untersuchung von Wechseldatenträgern anpassen**. Untersuchung von Wechseldatenträgern anpassen (siehe Abschnitt "Über die Untersuchung von Wechseldatenträgern" auf Seite 431), die über den USB-Port an den geschützten Computer angeschlossen sind.
- **Exploit-Prävention: Allgemeine Schutzeinstellungen**. Den Modus der Exploit-Prävention anpassen und Aktionen zur Vorbeugung einrichten.
- **Exploit-Prävention: Einstellungen für den Schutz von Prozessen**. Prozesse zum Schutz hinzufügen und die Exploit-Präventionstechniken auswählen (siehe Abschnitt "Exploit-Präventionstechniken" auf Seite 495).
- **Einstellungen der vertrauenswürdigen Zone anpassen**. Einstellungen der vertrauenswürdigen Zone anzeigen und anpassen (siehe Abschnitt "Über die vertrauenswürdige Zone" auf Seite 471).
- **Benutzerrechte für die Programmverwaltung ändern**. Zugriffsrechte für Funktionen von Kaspersky Embedded Systems Security anzeigen und anpassen (siehe Abschnitt "Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security" auf Seite 239).
- **Benutzerrechte für die Verwaltung von Kaspersky Security Service ändern**. Benutzerrechte zur Verwaltung von Kaspersky Security Service anzeigen und anpassen (siehe Abschnitt "Konfigurieren der Zugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security und Kaspersky Security Service" auf Seite 244).

- **Einstellungen exportieren**. Programmeinstellungen in einer Konfigurationsdatei im XML-Format speichern (siehe Abschnitt "Einstellungen exportieren" auf Seite 165). Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Einstellungen importieren**. Programmeinstellungen aus Konfigurationsdatei im XML-Format importieren (siehe Abschnitt "Einstellungen importieren" auf Seite 166). Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Angaben zum Programm und zu verfügbaren Modul-Updates**. Siehe Informationen über Kaspersky Embedded Systems Security sowie über aktuelle verfügbare Updates der Programm-Module.
- **Aktualisieren**. Fensterinhalte der Programmkonsole aktualisieren. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Eigenschaften**. Einstellungen von Kaspersky Embedded Systems Security oder einer ausgewählten Aufgabe anzeigen und anpassen. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.

  Hierfür können Sie auch den Link **Eigenschaften des Programms** im Detailbereich des Knotens **Kaspersky Embedded Systems Security** oder die Schaltfläche in der Symbolleiste verwenden.

- **Hilfe**. Informationen über die Hilfe zu Kaspersky Embedded Systems Security anzeigen Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.

Symbolleiste und Kontextmenü der Aufgaben von Kaspersky Embedded Systems Security

Sie können die Aufgaben für Kaspersky Embedded Systems Security mithilfe der Punkte des Kontextmenüs für jede Aufgabe in der Programmkonsolenstruktur verwalten.

Mithilfe der Punkte im Kontextmenü der ausgewählten Aufgabe können Sie folgende Aktionen ausführen:

- **Starten** / **Beenden**. Aufgabe starten oder beenden (siehe Abschnitt "Manuelles Starten / Anhalten / Fortsetzen / Beenden einer Aufgabe" auf Seite 160). Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden.
- **Fortsetzen** / **Anhalten**. Aufgabe fortsetzen oder anhalten (siehe Abschnitt "Manuelles Starten / Anhalten / Fortsetzen / Beenden einer Aufgabe" auf Seite 160). 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 hinzufügen**. Neue benutzerdefinierte Aufgabe erstellen (siehe Abschnitt "Erstellen und Konfigurieren einer Aufgabe zur Untersuchung auf Befehl" auf Seite 453). Diese Aktion ist nur für Untersuchungen auf Befehl verfügbar.
- **Protokoll öffnen**. Protokoll der Aufgabenausführung anzeigen und verwalten (siehe Abschnitt "Über Protokolle der Aufgabenausführung" auf Seite 216). Diese Operation ist für alle Aufgaben verfügbar.
- **Aufgabe löschen**. Benutzerdefinierte Aufgabe löschen. Diese Aktion ist nur für Untersuchungen auf Befehl verfügbar.
- **Vorlagen für Einstellungen**. Vorlagen verwalten (siehe Abschnitt "Verwendung von Vorlagen für Sicherheitseinstellungen" auf Seite 167). Diese Aktion ist nur für Aufgaben zum Echtzeitschutz für Dateien und zur Untersuchung auf Befehl verfügbar.

Taskleistensymbol im Infobereich

Jedes Mal, wenn Kaspersky Embedded Systems Security nach dem Neustart des Computers automatisch gestartet wird, erscheint im Infobereich das Taskleistensymbol . Es wird standardmäßig angezeigt, wenn Sie bei der Installation des Programms die Komponente Taskleistensymbol installiert haben.

Das Aussehen des Taskleistensymbols zeigt den aktuellen Schutzstatus des Computers an. Es sind folgende zwei Status möglich:

- Aktiv (farbiges Symbol), wenn derzeit mindestens eine der folgenden Aufgaben ausgeführt wird: Echtzeitschutz für Dateien, Kontrolle des Programmstarts
- Inaktiv (schwarz-weißes Symbol), wenn derzeit keine der folgenden Aufgaben ausgeführt wird: Echtzeitschutz für Dateien, Kontrolle des Programmstarts

Sie können das Kontextmenü des Taskleistensymbols mit der rechten Maustaste öffnen.

Das Kontextmenü enthält mehrere Befehle, die zur Anzeige der Programmfenster dienen (s. Tabelle unten).

Tabelle 26. Befehle im Kontextmenü des Taskleistensymbols

Befehl	Beschreibung
Programmkonsole öffnen	Öffnet die Konsole für Kaspersky Embedded Systems Security (falls installiert).
Kompakte Server-Übersicht öffnen	Öffnen Sie 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 Programmsymbol wieder anzuzeigen,*

wählen Sie im **Startmenü** von Microsoft Windows **Alle Programme** > **Kaspersky Embedded Systems Security** > **Taskleistensymbol** aus.

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

In den allgemeinen Einstellungen von Kaspersky Embedded Systems Security können Sie festlegen, ob das Taskleistensymbol angezeigt werden soll oder nicht, wenn das Programm nach dem Neustart des Computers automatisch gestartet wird.

Kaspersky Embedded Systems Security für Windows Server über die Programmkonsole auf einem anderen Computer verwalten

Sie können Kaspersky Embedded Systems Security über eine auf einem Remote-Computer installierte Programmkonsole verwalten.

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, damit die Programmverwaltung mithilfe der Konsole für Kaspersky Embedded Systems Security auf einem Remote-Computer verfügbar ist:

- Die Benutzer der Programmkonsole auf einem Remote-Computer sind der Gruppe "ESS Administrators" auf dem geschützten Computer zugeordnet.
- Wenn auf dem geschützten Computer die Windows-Firewall aktiviert ist, sind Netzwerkverbindungen für den Prozess des Kaspersky Security Management Service (kavfsgt.exe) erlaubt.
- Während der Installation von Kaspersky Embedded Systems Security wurde im Fenster des Installationsassistenten das Kontrollkästchen **Remote-Zugriff erlauben** aktiviert.

Wenn Kaspersky Embedded Systems Security auf dem Remote-Computer kennwortgeschützt ist, müssen Sie ein Kennwort eingeben, um Zugriff auf die Programmverwaltung über die Programmkonsole zu erhalten.

Aufgaben von Kaspersky Embedded Systems Security verwalten

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.

In diesem Abschnitt

Aufgabenkategorien von Kaspersky Embedded Systems Security

Die Funktionen "Echtzeit-Computerschutz", "Computer-Kontrolle", "Untersuchung auf Befehl" und "Update" in Kaspersky Embedded Systems Security sind in Form von Aufgaben realisiert.

Aufgaben lassen sich über das Kontextmenü des Aufgabennamens in der Struktur der Programmkonsole, der Symbolleiste und der Symbolleiste für den Schnellzugriff verwalten. Informationen über den Aufgabenstatus werden im Ergebnisbereich 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 werden nur auf dem geschützten Computer ausgeführt, für die sie angelegt 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 Systemaufgaben ändern. Eine Ausnahme bilden die Aufgaben "Untersuchung von Quarantäne-Objekten" und "Rollback des Datenbanken-Updates". Sie können die Systemaufgaben nicht umbenennen oder löschen. Systemaufgaben und benutzerdefinierte Aufgaben zur Untersuchung auf Befehl können gleichzeitig gestartet werden.
- **Lokale benutzerdefinierte Aufgaben**. In der Programmkonsole können Sie Aufgaben zur Untersuchung auf Befehl erstellen. In Kaspersky Security Center können Sie Aufgaben für die Untersuchung auf Befehl, für das Update der Programm-Datenbanken, für das Rollback des Datenbanken-Updates und für die Update-Verteilung erstellen. Diese Aufgaben werden als "benutzerdefinierte Aufgaben" bezeichnet. Sie können die benutzerdefinierten Aufgaben umbenennen, konfigurieren und löschen. Es können gleichzeitig mehrere benutzerdefinierte Aufgaben gestartet werden.

Gruppenaufgaben

Gruppenaufgaben und Aufgaben für Zusammenstellungen von Computern, die über Kaspersky Security Center erstellt wurden, werden in der Programmkonsole angezeigt. Diese Aufgaben werden als Gruppenaufgaben bezeichnet. Sie können Gruppenaufgaben durch Kaspersky Security Center verwalten und konfigurieren. In der Programmkonsole können Sie nur den Status von Gruppenaufgaben sehen.

Speichern einer Aufgabe nach dem Ändern der Einstellungen

Die Einstellungen einer Aufgabe, die ausgeführt oder beendet (angehalten) wurde, können geändert werden. Die neuen Einstellungen werden unter folgenden Bedingungen wirksam:

- Wenn Sie die Einstellungen einer laufenden Aufgabe geändert haben, werden die neuen Einstellungen umgehend nach dem Speichern der Aufgabe wirksam.
- Wenn Sie die Einstellungen einer beendeten (angehaltenen) Aufgabe geändert haben, werden die neuen Einstellungen beim Starten der nächsten Aufgabe wirksam.

► *Um geänderte Aufgabeneinstellungen zu speichern, gehen Sie wie folgt vor:*

Wählen Sie im Kontextmenü der Aufgabe **Aufgabe speichern** aus.

Wird nach dem Ändern der Aufgabeneinstellungen ein anderer Knoten in der Struktur der Programmkonsole ausgewählt, ohne dass zuvor der Befehl **Aufgabe speichern** ausgewählt wurde, wird das Fenster zum Ändern der Einstellungen geöffnet.

► *Um geänderte Aufgabeneinstellungen beim Wechseln zu einem anderen Knoten der Programmkonsole zu speichern, gehen Sie wie folgt vor:*

Klicken Sie im Fenster zum Speichern der Einstellungen auf **Ja**.

Manuelles Starten / Anhalten / Fortsetzen / Beenden einer Aufgabe

Sie können nur die Aufgaben "Echtzeit-Computerschutz" und "Untersuchung auf Befehl" anhalten und fortsetzen.

► *Um eine Aufgabe zu starten / anzuhalten / fortzusetzen / abzubrechen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Kontextmenü der Aufgabe in der Programmkonsole.
2. Wählen Sie einen der folgenden Punkte aus: **Starten**, **Anhalten**, **Fortsetzen** oder **Beenden**.

Die Operation wird ausgeführt und im Systemaudit-Protokoll registriert (auf Seite 214).

Nach Fortsetzung der Aufgabe zur Untersuchung auf Befehl setzt Kaspersky Embedded Systems Security die Untersuchung bei dem Objekt fort, bei dem die Aufgabe angehalten wurde.

Arbeit mit dem Aufgabenzeitplan

Sie können den Start der Aufgaben von Kaspersky Embedded Systems Security nach Zeitplan einrichten sowie die diesbezüglichen Einstellungen anpassen.

In diesem Abschnitt

Einstellungen des Zeitplans für den Aufgabenstart anpassen

In der Programmkonsole können Sie den Startzeitplan für lokale Systemaufgaben und benutzerdefinierte Aufgaben anpassen. Für den Start von Gruppenaufgaben kann der Zeitplan nicht angepasst werden.

► *Um die Zeitplan-Einstellungen für den Aufgabenstart anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Kontextmenü des Namens der Aufgabe, deren Startzeitplan angepasst werden soll.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster Aufgabeneinstellungen wird geöffnet.
3. Aktivieren Sie im folgenden Fenster auf der Registerkarte Zeitplan das Kontrollkästchen Aufgabe nach Zeitplan starten.

4. Passen Sie die Zeitplaneinstellungen entsprechend Ihren Anforderungen an. Gehen Sie hierzu wie folgt vor:

   a. Wählen Sie unter Startintervall einen der folgenden Werte aus:

      - Stündlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Stunden gestartet wird, wobei Sie die Anzahl der Stunden im Feld Alle **<Anzahl>** Std. eingeben müssen.
      - Täglich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Tagen gestartet wird, wobei Sie die Anzahl der Tage im Feld Alle **<Anzahl>** Tage eingeben müssen.
      - Wöchentlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl von Wochen gestartet wird, wobei Sie die Anzahl der Wochen im Feld Alle **<Anzahl>** Wochen eingeben müssen. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (Standardmäßig werden Aufgaben montags gestartet).
      - Bei Programmstart, wenn Sie möchten, dass die Aufgabe bei jedem Start von Kaspersky Embedded Systems Security ausgeführt wird.
      - Nach dem Update der Programm-Datenbanken, wenn Sie möchten, dass die Aufgabe nach jedem Update der Programm-Datenbanken gestartet wird.

   b. Legen Sie im Feld Startzeit die Uhrzeit des erstmaligen Aufgabenstarts fest.

   c. Tragen Sie im Feld Startdatum das Startdatum des Zeitplans ein.

   Nachdem Sie das Startintervall der Aufgabe, die Uhrzeit für den erstmaligen Aufgabenstart und das Datum, ab dem der Zeitplan gelten soll, angegeben haben, wird im oberen Bereich des Fensters im Feld Nächster Start der berechnete Zeitpunkt des nächsten Aufgabenstarts angezeigt. Aktualisierte Informationen über die Zeit, die bis zum nächsten Start verbleibt, werden jedes Mal angezeigt, wenn Sie das Fenster Aufgabeneinstellungen auf der Registerkarte Zeitplan öffnen.
   Der Wert Durch Richtlinie verboten im Feld Nächster Start wird angezeigt, wenn der Start von Systemaufgaben nach Zeitplan durch die Einstellungen der geltenden Richtlinie von Kaspersky Security Center festgelegt wird.

5. Passen Sie auf der Registerkarte Erweitert die folgenden Zeitplaneinstellungen gemäß Ihren Anforderungen an.

   - Im Abschnitt Einstellungen für das Anhalten der Aufgabe:

     a. Aktivieren Sie das Kontrollkästchen Dauer und geben Sie die erforderliche Anzahl an Stunden und Minuten in den Feldern rechts davon ein, um so die maximale Dauer der Aufgabenausführung vorzugeben.

     b. Aktivieren Sie das Kontrollkästchen Anhalten von und geben Sie die Anfangszeit und Endzeit des Zeitintervalls in den Feldern rechts davon ein, um einen Zeitraum innerhalb von 24 Stunden anzugeben, in dem die Aufgabenausführung angehalten wird.

- Im Abschnitt Erweiterte Einstellungen:
  a. Aktivieren Sie das Kontrollkästchen Zeitplan deaktivieren ab und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.
  b. Aktivieren Sie das Kontrollkästchen Übersprungene Aufgaben starten, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.
  c. Aktivieren Sie das Kontrollkästchen Aufgabenstart zufällig wählen innerhalb von und geben Sie einen Wert in Minuten ein.

6. Klicken Sie auf **OK**.

Die Einstellungen im Zeitplan für den Start der ausgewählten Aufgabe werden gespeichert.

Start nach Zeitplan aktivieren und deaktivieren

Sie können den Aufgabenstart nach Zeitplan sowohl vor als auch nach der Anpassung des Zeitplans aktivieren oder deaktivieren.

► *Um die den Zeitplan für den Aufgabenstart zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Aufgabennamen, für den Sie den Startzeitplan anpassen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
3. Führen Sie im folgenden Fenster auf der Registerkarte "Zeitplan" eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**, wenn Sie den Aufgabenstart nach Zeitplan aktivieren möchten
   - Deaktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**, wenn Sie den Aufgabenstart nach Zeitplan deaktivieren möchten

   > Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden nicht gelöscht und kommen bei der nächsten Aktivierung des Aufgabenstarts nach Zeitplan zur Anwendung.
4. Klicken Sie auf **OK**.

Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden gespeichert.

Verwendung von Benutzerkonten für den Aufgabenstart

Sie können Aufgaben starten, indem Sie das Systemkonto verwenden oder ein anderes Benutzerkonto angeben.

In diesem Abschnitt

Über die Verwendung eines Benutzerkontos für den Aufgabenstart

Sie können für die folgenden funktionalen Komponenten von Kaspersky Embedded Systems Security das Benutzerkonto angeben, mit dessen Rechten Sie die ausgewählte Aufgabe starten möchten:

- Aufgaben "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" und "Erstellen von Regeln für die Gerätekontrolle"
- Aufgabe zur Untersuchung auf Befehl
- Update-Aufgaben

Die angegebenen Aufgaben werden standardmäßig mit den Rechten des Systemkontos ausgeführt.

In folgenden Fällen sollten Sie ein anderes Benutzerkonto mit ausreichenden Zugriffsrechten angeben:

- In der Update-Aufgabe, wenn Sie als Update-Quelle einen freigegebenen Ordner auf einem anderen Netzwerkcomputer angegeben haben
- In der Update-Aufgabe, wenn für Zugriff auf die Update-Quelle ein Proxyserver mit integrierter NTLM-Authentifizierung von Microsoft Windows verwendet wird
- In den Aufgaben zur Untersuchung auf Befehl, wenn das Systemkonto nicht über die Zugriffsrechte für die untersuchenden Objekte verfügt (beispielsweise für Dateien in freigegebenen Ordnern des Computers)
- In der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts", wenn die erstellten Regeln nach Abschluss der Aufgabe in eine Konfigurationsdatei importiert werden, die sich an einem Speicherort befindet, auf den das Systemkonto keinen Zugriff hat (beispielsweise in einem der freigegebenen Ordner auf dem Computer)

Sie können die Aufgaben zum Update, zur Untersuchung auf Befehl und zur automatischen Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts mit den Rechten des Systemkontos starten. Während der Ausführung dieser Aufgaben greift Kaspersky Embedded Systems Security auf die freigegebenen Ordner auf einem anderen Netzwerk-Computer zu, wenn dieser Computer in derselben Domäne wie der geschützte Computer 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 \ Computername>** auf den Computer zu.

Benutzerkonto für den Aufgabenstart festlegen

► *Um ein Benutzerkonto für den Aufgabenstart festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü der Aufgabe, für die Sie den Start mit den Rechten des Benutzerkontos anpassen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

3. Gehen Sie im folgenden Fenster auf der Registerkarte Mit folgenden Rechten starten wie folgt vor:
   a. Wählen Sie den Punkt Benutzername aus.
   b. Geben Sie den Namen und das Kennwort des Benutzers an, dessen Benutzerkonto Sie verwenden möchten.

      Der von Ihnen ausgewählte Benutzer muss auf dem geschützten Computer oder in derselben Domäne angemeldet sein.

   c. Bestätigen Sie das eingegebene Kennwort.
4. Klicken Sie auf **OK**.

Die geänderten Einstellungen für den Aufgabenstart mit Berechtigungen des Benutzerkontos werden gespeichert.

Import und Export von Einstellungen

Dieser Abschnitt enthält Informationen über den Export der Einstellungen von Kaspersky Embedded Systems Security bzw. der Einstellungen der verschiedenen Programmkomponenten in eine Konfigurationsdatei im XML-Format, sowie über den Import dieser Einstellungen aus der Konfigurationsdatei ins Programm.

In diesem Abschnitt

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
- Verwendung von KSN
- Gerätekontrolle
- Kontrolle des Programmstarts
- Erstellen von Regeln für die Gerätekontrolle
- Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts
- Benutzerdefinierte Aufgaben zur Untersuchung auf Befehl.

- Überwachung der Datei-Integrität
- Protokollanalyse
- Datenbanken-Update und Update der Programm-Module für Kaspersky Embedded Systems Security
- Quarantäne
- Backup
- Protokolle
- Benachrichtigungen an den Administrator und die Benutzer
- Vertrauenswürdige Zone
- Exploit-Prävention
- Kennwortschutz

Ferner können Sie die allgemeinen Einstellungen von Kaspersky Embedded Systems Security und die Berechtigungen des Benutzerkontos in der Datei speichern.

Die Einstellungen von Gruppenaufgaben können nicht exportiert werden.

Kaspersky Embedded Systems Security exportiert alle Kennwörter, die vom Programm verwendet werden, beispielsweise die Daten von Konten für den Start von Aufgaben oder für die Verbindungsaufnahme mit Proxyservern. Exportierte Kennwörter werden in der Konfigurationsdatei verschlüsselt gespeichert. Sie können Kennwörter nur dann mithilfe von Kaspersky Embedded Systems Security importieren, wenn dieses Programm auf demselben Computer 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 Computer installiert ist. Nach dem Import von Einstellungen auf einen anderen Computer müssen alle Kennwörter manuell angegeben werden.

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.

Einstellungen aus einer Konfigurationsdatei, die nur Einstellungen für bestimmte Komponenten von Kaspersky Embedded Systems Security enthält (z. B. aus einer Datei, die in Kaspersky Embedded Systems Security erstellt wurde, als nicht alle Komponenten installiert waren), können importiert werden. 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

► *Um Parameter in eine Konfigurationsdatei zu exportieren, gehen Sie wie folgt vor:*

1. Führen Sie in der Struktur der Programmkonsole eine der folgenden Aktionen aus:
   - Wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** die Option **Einstellungen exportieren**, um alle Einstellungen von Kaspersky Embedded Systems Security zu exportieren.

- Wählen Sie im Kontextmenü des Namens der Aufgabe, deren Einstellungen Sie exportieren möchten, den Punkt **Einstellungen exportieren** aus, um die Einstellungen einer einzelnen Komponente des Programms zu exportieren.
- Um Einstellungen der Komponente Vertrauenswürdige Zone zu exportieren:
  a. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
  b. Wählen Sie den Punkt **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

     Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
  c. Klicken Sie auf die Schaltfläche **Export**.

     Darauf öffnet sich das Begrüßungsfenster des Assistenten für den Export von Einstellungen.

2. Folgen Sie den Anweisungen in den Fenstern des **Assistenten**: Geben Sie einen Namen und einen Pfad für die Konfigurationsdatei an, in der die Einstellungen gespeichert werden sollen.

   Wenn Sie den Pfad angeben, können Sie Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariablen können jedoch nicht verwendet werden.

   > Wenn zum Zeitpunkt des Exports von Einstellungen eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert Kaspersky Embedded Systems Security die Werte der Einstellungen aus der Richtlinie.

3. Klicken Sie im Fenster **Export der Programmeinstellungen abgeschlossen** auf die Schaltfläche **Schließen**.

Der Assistent für den Export von Einstellungen wird geschlossen; der Export der Einstellungen wird abgeschlossen.

Einstellungen importieren

► *Um Parameter aus einer Konfigurationsdatei zu importieren, gehen Sie wie folgt vor:*

1. Führen Sie in der Struktur der Programmkonsole eine der folgenden Aktionen aus:
   - Wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** die Option **Einstellungen importieren**, um alle Einstellungen von Kaspersky Embedded Systems Security zu importieren.
   - Wählen Sie im Kontextmenü des Namens der Aufgabe, deren Einstellungen Sie importieren möchten, den Punkt **Einstellungen importieren** aus, um die Einstellungen einer einzelnen funktionalen Komponente zu importieren.
   - Um Einstellungen der Komponente Vertrauenswürdige Zone zu importieren:
     a. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
     b. Wählen Sie den Punkt **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

        Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
     c. Klicken Sie auf die Schaltfläche **Import**.

        Darauf öffnet sich das Begrüßungsfenster des Assistenten für den Import von Einstellungen.

2. Folgen Sie den Anweisungen in den Fenstern des Assistenten: Geben Sie die Konfigurationsdatei an, aus der die Parameter importiert werden sollen.

   Nachdem Sie allgemeine Einstellungen für Kaspersky Embedded Systems Security oder dessen funktionale Komponenten auf dem Computer importiert haben, können die vorherigen Werte nicht wiederhergestellt werden.

3. Klicken Sie im Fenster **Import der Programmeinstellungen abgeschlossen** auf die Schaltfläche **Schließen**.

   Der Assistent für den Import von Einstellungen wird geschlossen; die importierten Einstellungen werden gespeichert.

4. Klicken Sie in der Symbolleiste der Programmkonsole auf die Schaltfläche **Aktualisieren**.

Die importierten Einstellungen werden im Fenster der Programmkonsole angezeigt.

Kaspersky Embedded Systems Security importiert keine Kennwörter (Anmeldedaten für den Aufgabenstart oder für die Proxyserver-Verbindung) aus einer Datei, die auf einem anderen Computer angelegt wurde oder auf demselben Computer gespeichert wurde, nachdem Kaspersky Embedded Systems Security auf diesem neu installiert oder aktualisiert wurde. Die Kennwörter müssen nach dem Abschluss des Imports manuell angegeben werden.

Verwendung von Vorlagen für Sicherheitseinstellungen

Dieser Abschnitt enthält Informationen über die Arbeit mit Vorlagen für Sicherheitseinstellungen in den Schutz- und Untersuchungsaufgaben von Kaspersky Embedded Systems Security.

In diesem Abschnitt

Über Vorlagen für Sicherheitseinstellungen

Sie können die Sicherheitseinstellungen eines Knotens in der Struktur oder in der Liste der Dateiressourcen des Computers manuell konfigurieren und die Werte der angepassten Einstellungen in einer Vorlage speichern. Sie können diese Vorlage später bei der Konfiguration der Sicherheitseinstellungen anderer Knoten in den Schutz- und Untersuchungsaufgaben von Kaspersky Embedded Systems Security verwenden.

Die Verwendung von Vorlagen ist bei der Konfiguration der Sicherheitseinstellungen folgende Aufgaben von Kaspersky Embedded Systems Security verfügbar:

- Echtzeitschutz für Dateien
- Untersuchung beim Hochfahren des Betriebssystems
- Untersuchung wichtiger Bereiche
- Benutzerdefinierte Aufgaben zur Untersuchung auf Befehl.

Die Sicherheitseinstellungen aus einer Vorlage, die auf einen übergeordneten Knoten in der Struktur der Dateiressourcen des Computers angewandt wird, werden für alle untergeordneten Knoten übernommen. In folgenden Fällen wird die Vorlage eines übergeordneten Knotens nicht für die untergeordneten Knoten übernommen:

- Wenn die Sicherheitseinstellungen der untergeordneten Knoten gesondert konfiguriert wurden (siehe Abschnitt "Vorlage für Sicherheitseinstellungen anwenden" auf Seite 169).
- Wenn es sich bei den untergeordneten Knoten um virtuelle Knoten handelt. In diesem Fall muss die Vorlage für jeden virtuellen Knoten gesondert übernommen werden.

Vorlage für Sicherheitseinstellungen erstellen

► *Gehen Sie wie folgt vor, um die Sicherheitseinstellungen des Knotens manuell zu übernehmen und sie in einer Vorlage zu speichern:*

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, deren Vorlage für Einstellungen der Sicherheit Sie übernehmen möchten.
2. Klicken Sie im Ergebnisbereich der ausgewählten Aufgabe auf den Link **Schutzbereich anpassen** oder **Untersuchungsbereich anpassen**.
3. Wählen Sie in der Struktur bzw. Liste der freigegebenen Netzwerkordner des Computers die Vorlage aus, die Sie anzeigen möchten.
4. Klicken Sie auf der Registerkarte **Sicherheitsstufe** auf die Schaltfläche **Als Vorlage speichern**.

   Das Fenster **Eigenschaften der Vorlage** wird geöffnet.
5. Geben Sie im Feld **Vorlagenname** den Namen der Vorlage ein.
6. Tragen Sie im Feld **Beschreibung** beliebige Zusatzinformationen über die Vorlage ein.
7. Klicken Sie auf **OK**.

Die Vorlage mit dem Satz der Sicherheitseinstellungen wird gespeichert.

Sicherheitseinstellungen in einer Vorlage aufrufen

► *Um die Werte der Sicherheitsparameter in einer vorhandenen Vorlage anzuzeigen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, deren Vorlage mit den Sicherheitseinstellungen Sie ansehen möchten.
2. Wählen Sie im Kontextmenü der ausgewählten Aufgabe den Punkt **Vorlagen für Einstellungen** aus.

   Das Fenster **Vorlagen** wird geöffnet.

3. Wählen Sie im erscheinenden Fenster in der Vorlagenliste die Vorlage aus, die angezeigt werden soll.
4. Klicken Sie auf die Schaltfläche **Anzeigen**.

Das Fenster **<Vorlagenname>** wird geöffnet. Auf der Registerkarte **Allgemein** werden der Name der Vorlage und Zusatzinformationen über die Vorlage angezeigt. Die Registerkarte **Einstellungen** enthält eine Liste mit den Werten der Sicherheitsparameter, die in der Vorlage gespeichert sind.

Vorlage für Sicherheitseinstellungen anwenden

► *Gehen Sie wie folgt vor, um die Sicherheitseinstellungen aus der Vorlage für den ausgewählten Knoten zu übernehmen:*

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, deren Vorlage für Einstellungen der Sicherheit Sie übernehmen möchten.
2. Klicken Sie im Ergebnisbereich der ausgewählten Aufgabe auf den Link **Schutzbereich anpassen** oder **Untersuchungsbereich anpassen**.
3. Öffnen Sie in der Struktur oder Liste der freigegebenen Netzwerkordner des Computers das Kontextmenü des Knotens bzw. Elements, für das Sie die Vorlage übernehmen möchten.
4. Wählen Sie **Vorlage übernehmen** → **<Name der Vorlage>** aus.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Vorlage für Sicherheitseinstellungen wird für den ausgewählten Knoten in der Struktur der Dateiressourcen des Computers übernommen. Auf der Registerkarte **Sicherheitsstufe** des ausgewählten Knotens wird der Wert **Benutzerdefiniert** festgelegt.

Die Sicherheitseinstellungen aus einer Vorlage, die auf einen übergeordneten Knoten in der Struktur der Dateiressourcen des Computers angewandt wird, werden für alle untergeordneten Knoten übernommen.

Wenn der Schutzbereich bzw. Untersuchungsbereich der untergeordneten Knoten in der Struktur der Dateiressourcen des Computers gesondert konfiguriert wurde, werden die Sicherheitseinstellungen aus der Vorlage, die für den übergeordneten Knoten übernommen wurde, für diese untergeordneten Knoten nicht automatisch übernommen.

► *Gehen Sie wie folgt vor, um die Sicherheitseinstellungen aus der Vorlage für alle untergeordneten Knoten zu übernehmen:*

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, deren Vorlage für Einstellungen der Sicherheit Sie übernehmen möchten.
2. Klicken Sie im Ergebnisbereich der ausgewählten Aufgabe auf den Link **Schutzbereich anpassen** oder **Untersuchungsbereich anpassen**.
3. Wählen Sie in der Struktur oder Liste der freigegebenen Netzwerkordner des Computers einen übergeordneten Knoten aus, um die Vorlage für diesen Knoten und alle untergeordneten Knoten zu übernehmen.

4. Wählen Sie im Kontextmenü **Vorlage übernehmen → <Name der Vorlage>** aus.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Vorlage für Sicherheitseinstellungen wird für den übergeordneten und alle untergeordneten Knoten in der Struktur der Dateiressourcen des Computers übernommen. Auf der Registerkarte **Sicherheitsstufe** des ausgewählten Knotens wird der Wert **Benutzerdefiniert** festgelegt.

Vorlage für Sicherheitseinstellungen löschen

► *Um eine Vorlage für Sicherheitseinstellungen zu löschen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Programmkonsole die Aufgabe aus, für deren Konfiguration Sie die Vorlage für Sicherheitseinstellungen nicht mehr verwenden möchten.
2. Wählen Sie im Kontextmenü der ausgewählten Aufgabe den Punkt **Vorlagen für Einstellungen** aus.

   Sie können Vorlagen für Einstellungen für Aufgaben zur Untersuchung auf Befehl aus dem Ergebnisbereich des übergeordneten Knotens **Untersuchung auf Befehl** anzeigen.

   Das Fenster **Vorlagen** wird geöffnet.
3. Wählen Sie im erscheinenden Fenster in der Vorlagenliste die zu löschende Vorlage aus.
4. Klicken Sie auf die Schaltfläche **Löschen**.

   Ein Fenster zur Bestätigung des Löschvorgangs wird geöffnet.
5. Klicken Sie im folgenden Fenster auf **Ja**.

Die gewählte Vorlage wird gelöscht.

Wenn die Vorlage für Sicherheitseinstellungen zum Schutz oder zur Untersuchung von Knoten der Dateiressourcen des Computers übernommen wurde, werden die konfigurierten Sicherheitseinstellungen für diese Knoten nach dem Löschen der Vorlage gespeichert.

Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen

► *Um Informationen über den Schutzstatus des Computers in Kaspersky Embedded Systems Security anzuzeigen,*

wählen Sie in der Programmkonsolenstruktur den Knoten **Kaspersky Embedded Systems Security** aus.

Standardmäßig werden die Informationen im Ergebnisbereich der Programmkonsole automatisch aktualisiert:

- alle 10 Sekunden bei lokaler Verbindung
- alle 15 Sekunden bei Remote-Verbindung

Sie können die Informationen auch 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**.

Im Ergebnisbereich der Programmkonsole werden die folgenden Programminformationen angezeigt:

- Status der Verwendung von Kaspersky Security Network.
- Schutzstatus des Computers.
- Daten über das Datenbanken-Update und das Update der Programm-Module.
- Aktuelle Diagnoseinformationen.
- Daten über die Aufgaben zur Computer-Kontrolle.
- Lizenzinformationen.
- Status der Integration in Kaspersky Security Center: Daten des Computers, auf dem Kaspersky Security Center installiert und mit dem das Programm verknüpft ist; Daten über die Kontrolle der Programmaufgaben durch die aktive Richtlinie

Für die Darstellung des Schutzstatus werden verschiedene Farben verwendet:

- *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 **Verwendung von Kaspersky Security Network** zeigt den aktuellen Status der Aufgabe, z. B. *Wird ausgeführt*, *Beendet* oder *Nicht ausgeführt*, an. Der Indikator kann folgende Werte annehmen:

- Grün – die Aufgabe "Verwendung von KSN" wird ausgeführt und Dateianfragen zum Status werden an KSN gesendet.
- Gelb – eine der Erklärungen wurde akzeptiert, die Aufgabe wird jedoch nicht ausgeführt; oder die Aufgabe wird ausgeführt, es werden jedoch keine Dateianforderungen an KSN gesendet.

Computer**schutz**

Im Abschnitt **Computerschutz** (siehe Tabelle unten) werden Informationen über den aktuellen Schutzstatus des Computers angezeigt.

Tabelle 27. Informationen über den Schutzstatus des Computers

Abschnitt "Schutz"	Informationen
Statusanzeige für den Computerschutz	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der im Block ausführbaren Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Standard-Darstellung, die anzeigt, dass die Komponente "Echtzeitschutz für Dateien" installiert ist und die Aufgabe ausgeführt wird. • Gelb – die Komponente "Echtzeitschutz für Dateien" wurde nicht installiert und die Aufgabe zur Untersuchung wichtiger Bereiche wurde seit langer Zeit nicht ausgeführt. • Rot – die Aufgabe zum Echtzeitschutz für Dateien wird nicht ausgeführt.
Echtzeitschutz für Dateien	**Aufgabenstatus** – aktueller Status der Aufgabe (z. B. "*Läuft*" oder "*Beendet*"). **Gefunden** – Anzahl der Objekte, die von Kaspersky Embedded Systems Security gefunden wurden. Findet Kaspersky Embedded Systems Security beispielsweise in fünf Dateien ein und dieselbe Schadsoftware, dann wird der Wert in diesem Feld um den Wert eins erhöht. Ist die Anzahl der gefundenen Schadsoftware größer als 0, so wird der Wert rot dargestellt.
Untersuchung wichtiger Bereiche	**Letzte Untersuchung am** – Datum und Uhrzeit der letzten Untersuchung wichtiger Bereiche des Computers auf Viren und andere Bedrohungen der Computersicherheit. *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.
Exploit-Prävention	**Status** – aktueller Status der Exploit-Präventionstechniken, beispielsweise *Übernommen* oder *Nicht übernommen*. **Präventionsmodus** – einer von zwei verfügbaren Modi, der bei der Konfiguration des Schutzes des Prozess-Speichers ausgewählt wurde: • Bei Exploit beenden • Nur Statistik. **Geschützte Prozesse** – Gesamtanzahl der Prozesse, die zum Schutzbereich hinzugefügt wurden und gemäß dem gewählten Modus verarbeitet werden.

Abschnitt "Schutz"	Informationen
Objekte im Backup	*Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* – Ereignis, das auftritt, wenn sich der verfügbare Speicherplatz im Backup dem festgelegten Grenzwert nähert. Kaspersky Embedded Systems Security verschiebt Objekte weiterhin ins Backup. In diesem Fall wird der Wert im Feld **Belegter Speicherplatz** gelb dargestellt. *Die maximale Größe des Backups wurde überschritten* – Ereignis, das auftritt, wenn die Größe des Backups den festgelegten Grenzwert erreicht. Kaspersky Embedded Systems Security verschiebt Objekte weiterhin ins Backup. In diesem Fall wird der Wert im Feld **Belegter Speicherplatz** rot dargestellt. **Objekte im Backup** – Anzahl der Objekte, die sich momentan im Backup befinden. **Belegter Speicherplatz** – Volumen des verwendeten Speicherplatzes im Backup.

Update

Im Abschnitt **Update** (siehe Tabelle unten) werden Informationen über die Aktualität der Antiviren-Datenbanken und Programm-Module angezeigt.

Tabelle 28. Informationen über den Zustand der Datenbanken und Module von Kaspersky Embedded Systems Security

Abschnitt "Update"	Informationen
Statusindikator für Datenbanken und Programm-Module	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der Programm-Datenbanken und Programm-Module. Der Indikator kann folgende Werte annehmen: • Grün – Standarddarstellung, die anzeigt, dass die Programm-Datenbanken aktuell sind und dass das letzte Update der Programm-Datenbanken erfolgreich abgeschlossen wurde. • Gelb – die Datenbanken sind veraltet, oder die letzte Aufgabe zum Datenbanken-Update ist fehlgeschlagen. • Rot – das Ereignis *Programm-Datenbanken sind stark veraltet* oder *Programm-Datenbanken sind beschädigt* ist eingetreten.

Abschnitt "Update"	Informationen
Update der Programm-Datenbanken und **Update der Programm-Module**	**Status der Programm-Datenbanken** – Bewertung des Status des Updates der Programm-Datenbanken. Die Einstellung kann folgende Werte annehmen: • **Programm-Datenbanken sind aktuell** – die Programm-Datenbanken wurden vor höchstens 7 Tagen aktualisiert (Standard). • **Programm-Datenbanken sind veraltet** – die Programm-Datenbanken wurden zuletzt vor 7–14 Tagen aktualisiert (Standard). • **Programm-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 *Programm-Datenbanken sind veraltet* und *Programm-Datenbanken sind stark veraltet* ändern. **Veröffentlichungsdatum der Programm-Datenbanken** – Datum und Uhrzeit der Veröffentlichung des aktuellen Updates der Programm-Datenbanken. Datum und Uhrzeit werden in UTC angegeben. **Status der letzten gestarteten Aufgabe zum Update der Programm-Datenbanken** – Datum und Uhrzeit des letzten Datenbanken-Updates. Datum und Uhrzeit werden in der lokalen Zeit des geschützten Computers angegeben. Das Feld ist rot, wenn das Ereignis *Fehlgeschlagen* eingetreten ist. **Verfügbare Updates der Programm-Module** – Anzahl der zum Download und zur Installation verfügbaren Updates für die Module von Kaspersky Embedded Systems Security. **Installierte Updates der Programm-Module** – Anzahl der installierten Updates für Module von Kaspersky Embedded Systems Security.

Steuerelement

Im Abschnitt **Steuerelement** (s. Tabelle unten) werden Informationen über den Status der Aufgaben "Kontrolle des Programmstarts", "Gerätekontrolle" und "Firewall-Verwaltung" angezeigt.

Tabelle 29. Informationen über den Status der Computer-Kontrolle

Abschnitt "Steuerelement"	Informationen
Statusanzeige für die Computer-Kontrolle	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der im Block ausführbaren Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Standarddarstellung, die anzeigt, dass die Komponente "Kontrolle des Programmstarts" installiert wurde und die Aufgabe im Modus **Aktiv** ausgeführt wird • Gelb – Die Kontrolle des Programmstarts wird im Modus **Nur Statistik** ausgeführt. • Rot – Die Aufgabe zur Kontrolle des Programmstarts wird nicht ausgeführt oder ist fehlgeschlagen.

Abschnitt "Steuerelement"	Informationen
Kontrolle des Programmstarts	**Aufgabenstatus** – aktueller Status der Aufgabe (z. B. "*Läuft*" oder "*Beendet*"). **Modus** – einer von zwei verfügbaren Ausführungsmodi der Aufgabe "Kontrolle des Programmstarts": • Aktiv • Nur Statistik **Blockierte Programmstarts** – Anzahl der versuchten Programmstarts, die durch Kaspersky Embedded Systems Security während der Ausführung der Aufgabe zur Kontrolle des Programmstarts blockiert wurden. Ist die Anzahl der blockierten Versuche des Programmstarts größer als 0, so ist das Feld rot. **Durchschnittliche Bearbeitungsdauer (ms)** – Zeit, die Kaspersky Embedded Systems Security für die Verarbeitung eines versuchten Programmstarts auf dem geschützten Computer benötigt hat.
Gerätekontrolle	**Aufgabenstatus** – aktueller Status der Aufgabe (z. B. "*Läuft*" oder "*Beendet*"). **Modus** – einer von zwei verfügbaren Ausführungsmodi der Aufgabe "Gerätekontrolle": • **Aktiv** • **Nur Statistik** **Blockierte Geräte** – Anzahl der Verbindungsversuche von Massenspeichergeräten, die von Kaspersky Embedded Systems Security während der Aufgabe zur Gerätekontrolle blockiert wurden. Ist die Anzahl der blockierten Massenspeicher größer als 0, so ist das Feld rot.
Firewall-Verwaltung	**Aufgabenstatus** – aktueller Status der Aufgabe (z. B. "*Läuft*" oder "*Beendet*"). **Blockierte Verbindungsversuche** – Anzahl der Verbindungen mit dem geschützten Computer, die gemäß den festgelegten Firewall-Regeln nicht erlaubt wurden.

Diagnose

Im Abschnitt **Diagnose** (s. Tabelle unten) werden Informationen über den Status der Aufgaben "Überwachung der Datei-Integrität" und "Protokollanalyse" angezeigt.

Tabelle 30. Informationen über den Status der System-Diagnose

Abschnitt "Diagnose"	Informationen
Statusindikator der Diagnose	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der im Block ausführbaren Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Standarddarstellung, die anzeigt, dass eine oder beide Komponenten der System-Diagnose installiert sind und dass Aufgaben ausgeführt werden. • Gelb – beide Komponenten sind installiert, aber eine der Aufgaben zur System-Diagnose läuft nicht; das Ereignis *Nicht gestartet* ist eingetreten. • Rot – eine der Aufgaben ist fehlgeschlagen.

Überwachung der Datei-Integrität	**Aufgabenstatus** – aktueller Status der Aufgabe (z. B. "*Läuft*" oder "*Beendet*"). **Verbotene Dateioperationen** – Anzahl der Veränderungen an Dateien, die sich im Überwachungsbereich befinden. Diese Änderungen deuten eventuell auf eine Verletzung der Sicherheit auf dem geschützten Computer hin.
Protokollanalyse	**Aufgabenstatus** – aktueller Status der Aufgabe (z. B. "*Läuft*" oder "*Beendet*"). **Mögliche Verstöße**– Anzahl der registrierten Verstöße laut Angaben des Windows-Ereignisprotokolls. Diese Zahl wird auf Grundlage der festgelegten Aufgabenregeln oder mithilfe der heuristischen Analyse ermittelt.

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 (siehe Abschnitt "Einstellungen von Kaspersky Embedded Systems Security in der Programmkonsole" auf Seite 145).

Sie können eine Verbindung zu einem anderem Computer herstellen, indem Sie auf den Link **Verbindung mit anderem Computer herstellen** klicken (s. Abschnitt "Kaspersky Embedded Systems Security über die Programmkonsole auf einem anderen Computer verwalten" auf S. 158).

Kompaktes Diagnosefenster

In diesem Abschnitt wird beschrieben, wie Sie das kompakte Diagnosefenster zur Überprüfung des Computerstatus oder der aktuellen Aktivität nutzen und das Erstellen von Dump-Dateien und Protokolldateien anpassen.

In diesem Kapitel

Über das kompakte Diagnosefenster

Die Komponente "Kompaktes Diagnosefenster" ("Compact Diagnostic Interface", im Weiteren auch "CDI") wird gemeinsam mit der Komponente "Taskleistensymbol" unabhängig von der Programmkonsole installiert und deinstalliert und kann verwendet werden, wenn die Programmkonsole nicht auf dem geschützten Computer installiert ist. Das CDI wird aus dem über das Taskleistensymbol oder durch Ausführung von kavfsmui.exe aus dem Programmordner auf dem Computer gestartet.

Im CDI-Fenster können Sie folgenden Aktionen ausführen:

- Informationen über den allgemeinen Programmstatus überprüfen (siehe Abschnitt "Status von Kaspersky Embedded Systems Security mithilfe des kompakten Diagnosefensters überprüfen" auf Seite 178)
- Eingetretene Sicherheitsereignisse überprüfen (s. Abschnitt "Überprüfung der Sicherheitsereignis-Statistik" auf S. 179)
- Aktuelle Aktivitäten auf dem geschützten Computer überprüfen (s. Abschnitt "Aktuelle Programmaktivität überprüfen" auf S. 179)
- Das Erstellen von Dump-Dateien und Protokolldateien starten und stoppen (s. Abschnitt "Konfigurieren der Speicherung von Dump- und Protokolldateien" auf S. 180)
- Öffnen Sie die Programmkonsole.
- Das Fenster **Über das Programm** mit der Liste der installierten Updates und verfügbaren Patches öffnen

Das CDI ist auch verfügbar, wenn der Zugriff auf Kaspersky Embedded Systems Security kennwortgeschützt ist. Es ist kein Kennwort erforderlich.

Die CDI-Komponente kann nicht über Kaspersky Security Center angepasst werden.

Status von Kaspersky Embedded Systems Security mithilfe des kompakten Diagnosefensters überprüfen

► *Um das kompakte Diagnosefenster zu öffnen, führen Sie die folgenden Schritte aus:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompakte Server-Übersicht öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.

Überprüfen Sie den aktuellen Status des Schlüssels, den Echtzeit-Computerschutz und Updates auf der Registerkarte **Schutzstatus**. Die unterschiedlichen Farben informieren den Benutzer über den Schutzstatus (siehe nachfolgende Tabelle).

Tabelle 31. Schutzstatus des kompakten Diagnosefensters

Abschnitt	Status

Echtzeit-Computerschutz	Die Leiste ist *grün*, wenn eines der folgenden Szenarien zutrifft (eine beliebige Anzahl von Bedingungen ist erfüllt):
	• Empfohlene Konfiguration:
	  ◦ Die Aufgabe zum Echtzeitschutz für Dateien wurde mit den Standardeinstellungen gestartet.
	  ◦ Die Aufgabe zur Kontrolle des Programmstarts wurde im Modus **Aktiv** mit den Standardeinstellungen gestartet.
	• Annehmbare Konfiguration:
	  ◦ Die Aufgabe zum Echtzeitschutz für Dateien wurde vom Benutzer angepasst.
	  ◦ Die Einstellungen der Aufgabe zur Kontrolle des Programmstarts wurden geändert.

	Die Leiste ist *gelb*, wenn eine oder mehrere der folgenden Bedingungen zutreffen: • Die Aufgabe zum Echtzeitschutz für Dateien wurde angehalten (durch Benutzer oder Zeitplan). • Die Aufgabe zur Kontrolle des Programmstarts wurde im Modus **Nur Statistik** gestartet. • Die Exploit-Prävention und die Kontrolle des Programmstarts wurden im Modus **Nur Statistik** gestartet.
	Die Leiste ist *rot*, wenn beide der folgenden Bedingungen zutreffen: • Die Komponente "Echtzeitschutz für Dateien" ist nicht installiert oder die Aufgabe wurde beendet oder angehalten. • Die Komponente "Kontrolle des Programmstarts" ist nicht installiert oder die Aufgabe wurde im Modus **Nur Statistik** gestartet.
Lizenzverwaltung	Die Leiste ist *grün*, wenn die aktuelle Lizenz gültig ist.

	Die Leiste ist *gelb*, wenn eines der folgenden Ereignisse eingetreten ist: • **Untersuchung des Lizenzstatus läuft** • **Die Restlaufzeit der Lizenz beträgt noch 14 Tage, und es wurde kein Reserveschlüssel oder Aktivierungscode hinzugefügt** • **Der hinzugefügte Schlüssel befindet sich in der schwarzen Liste und seine Blockierung steht unmittelbar bevor**.
	Die Leiste ist *rot*, wenn eines der folgenden Ereignisse eingetreten ist: • **Das Programm wurde nicht aktiviert.** • **Die Lizenz ist abgelaufen!** • **Verstoß gegen den Endbenutzer-Lizenzvertrag.** • **Der Schlüssel wurde auf die schwarze Liste gesetzt.**
Update	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

Auf der Registerkarte **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.

► *Um eine Statistik zu überprüfen:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompakte Server-Übersicht öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.
3. Öffnen Sie die Registerkarte **Statistik**.
4. Überprüfen Sie die Sicherheitsvorfälle für die Schutzaufgaben.

Aktuelle Programmaktivität überprüfen

Auf dieser Registerkarte können Sie den Status der aktuellen Aufgaben und Programmprozesse überprüfen und erhalten sofort Benachrichtigungen über kritische Ereignisse, wenn sie auftreten.

Für die Darstellung der Programmaktivität werden verschiedene Farben verwendet:

- Im Abschnitt **Aufgaben**:
  - *Grün*. Keine Bedingungen für gelb oder rot erfüllt.
  - *Gelb*. Untersuchung wichtiger Bereiche liegt lange zurück.
  - *Rot*. Beliebige der folgenden Bedingungen treffen 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 "Verwendung von KSN" wurde gestartet.
  - *Gelb*. Die KSN-Erklärung wurde akzeptiert, aber die Aufgabe wurde nicht gestartet.

► *Um die aktuelle Programmaktivität auf dem Computer zu überprüfen, gehen Sie wie folgt vor:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompakte Server-Übersicht öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.
3. Öffnen Sie die Registerkarte **Aktuelle Programmaktivität**.
4. Überprüfen Sie die folgenden Informationen im Abschnitt **Aufgaben**:
   - **Untersuchung wichtiger Bereiche liegt lange zurück**

     Dieses Feld wird nur angezeigt, wenn das Programm die entsprechenden Warnungen über die Untersuchung wichtiger Bereiche zurückgibt.
   - **Wird jetzt ausgeführt**
   - **Ausführung fehlgeschlagen**
   - **Nächster Start durch Zeitplan definiert**
5. Überprüfen Sie die folgenden Informationen im Abschnitt **Kaspersky Security Network**:
   - **KSN ist aktiviert. Datei-Reputationsdienste sind aktiviert** oder **Schutz ist deaktiviert**.
   - **Die Programmstatistik wird an KSN gesendet**.

     Das Programm sendet während der Ausführung der Aufgaben zum Echtzeitschutz für Dateien und zur Untersuchung auf Befehl Informationen über Funde von Schadsoftware einschließlich Betrugssoftware sowie Debug-Informationen über Störungen während der Untersuchung.

     Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Statistiken zu Kaspersky Security Network senden** in den Aufgabeneinstellungen für die Verwendung von KSN aktiviert ist.
6. Überprüfen Sie die folgenden Informationen im Abschnitt **Integration in Kaspersky Security Center**:
   - Lokale Verwaltung ist erlaubt
   - Richtlinie wurde übernommen: <Kaspersky Security Center-Servername>.

Konfigurieren der Speicherung von Dump- und Protokolldateien

Sie können das Erstellen von Dump-Dateien und Protokolldateien über das kompakte Diagnosefenster (CDI) anpassen.

Sie können außerdem die Crash-Diagnose über die Programmkonsole einrichten (s. Abschnitt "Einstellungen von Kaspersky Embedded Systems Security in der Programmkonsole" auf Seite 145).

► *Um mit dem Erstellen von Dump-Dateien und Protokolldateien zu beginnen, führen Sie die folgenden Aktionen aus:*

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompakte Server-Übersicht öffnen**.

   Das Fenster **Kompakte Server-Übersicht** wird angezeigt.
3. Öffnen Sie die Registerkarte **Problembehandlung**.
4. Bei Bedarf können Sie folgende Protokollierungseinstellungen anpassen:
   a. Aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei in diesem Ordner speichern**.
   b. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner anzugeben, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.

      Die Protokollierung wird für alle Komponenten mit den Standardparametern aktiviert. Dabei werden die Genauigkeitsstufe für das **Debuggen** und die maximale Standardprotokollgröße von 50 MB verwendet.
5. Bei Bedarf können Sie folgende Einstellungen für Dump-Dateien anpassen:
   a. Aktivieren Sie das Kontrollkästchen **Bei Absturz Dump-Datei in diesem Ordner erstellen**.
   b. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner anzugeben, in dem Kaspersky Embedded Systems Security die Dump-Datei speichern soll.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.

   Eine neue Konfiguration wird übernommen.

Datenbanken und Programm-Module für Kaspersky Embedded Systems Security aktualisieren

Dieser Abschnitt enthält Informationen über die Aufgaben zum Datenbanken-Update und Update der Programm-Module von Kaspersky Embedded Systems Security, über die Update-Verteilung und das Rollback eines Datenbanken-Updates in Kaspersky Embedded Systems Security, sowie Anweisungen zum Anpassen der Aufgabeneinstellungen für Updates von Datenbanken und Programm-Module.

In diesem Kapitel

Über Update-Aufgaben

In Kaspersky Embedded Systems Security sind vier Systemaufgaben zum Update vorgesehen: Update der Programm-Datenbanken, Update der Programm-Module, Update-Verteilung und Rollback des Datenbanken-Updates.

Standardmäßig stellt Kaspersky Embedded Systems Security eine Verbindung zur Update-Quelle her (zu einem der Kaspersky-Lab-Update-Server). Sie können alle Update-Aufgaben konfigurieren (siehe Abschnitt "Einstellung von Update-Aufgaben" auf S. 187), mit Ausnahme der Aufgabe zum Rollback des Datenbanken-Updates. Nachdem Sie die Aufgabeneinstellungen geändert haben, übernimmt Kaspersky Embedded Systems Security die neuen Werte beim nächsten Aufgabenstart.

Update-Aufgaben können nicht angehalten und wieder fortgesetzt werden.

Update der Programm-Datenbanken

Kaspersky Embedded Systems Security kopiert die Datenbanken standardmäßig aus der Update-Quelle auf den geschützten Computer und verwendet in der laufenden Aufgabe zum Echtzeit-Computerschutz sofort die aktualisierten Datenbanken. Die Aufgaben zur Untersuchung auf Befehl verwenden beim nächsten Aufgabenstart die aktualisierten Programm-Datenbanken.

Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe zum Update der Programm-Datenbanken stündlich.

Update der Programm-Module

Standardmäßig überprüft Kaspersky Embedded Systems Security die Verfügbarkeit von Updates der Programm-Module an der Update-Quelle. Zur Übernahme der installierten Programm-Module müssen Sie den Computer und/oder Kaspersky Embedded Systems Security eventuell neu starten.

Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe Update der Programm-Module jeden Freitag um 16:00 Uhr (Zeit gemäß den regionalen Einstellungen des geschützten Computers). Während der Aufgabenausführung untersucht das Programm, ob wichtige und planmäßige Updates für die Module von Kaspersky Embedded Systems Security vorhanden sind, ohne diese zu kopieren.

Update-Verteilung

Kaspersky Embedded Systems Security lädt die Dateien für das Update der Programm-Datenbanken standardmäßig während der Aufgabenausführung herunter und speichert sie im angegebenen Netzwerkordner oder lokalen Ordner, ohne sie zu installieren.

In der Grundeinstellung wird die Aufgabe Update-Verteilung nicht ausgeführt.

Rollback des Datenbanken-Updates

Kaspersky Embedded Systems Security kehrt während der Ausführung der Aufgabe zu den Datenbanken mit den zuvor installierten Updates zurück.

Standardmäßig wird die Aufgabe Rollback des Datenbanken-Updates nicht ausgeführt.

Über das Update der Programm-Module von Kaspersky Embedded Systems Security

Kaspersky Lab stellt Updatepakete für die Module von Kaspersky Embedded Systems Security zur Verfügung. Es gibt *wichtige* (oder *kritische*) und geplante Updates. Wichtige Updatepakete beheben Schwachstellen und Fehler. Geplante Updates fügen neue Funktionen hinzu oder verbessern vorhandene.

Wichtige Updatepakete werden auf den Kaspersky Lab Update-Servern veröffentlicht. Sie können festlegen, dass sie mit Hilfe der Aufgabe Update der Programm-Module automatisch installiert werden. Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe Update der Programm-Module jeden Freitag um 16:00 Uhr (Zeit gemäß den regionalen Einstellungen des geschützten Computers).

Geplante Updatepakete werden von Kaspersky Lab nicht auf den Update-Servern veröffentlicht, um sie automatisiert zu installieren. Sie können solche Updatepakete von der Kaspersky-Lab-Webseite downloaden. Mit Hilfe der Aufgabe Update der Programm-Module können Sie sich über das Erscheinen von geplanten Updates für Kaspersky Embedded Systems Security informieren.

Sie können dringende Updates entweder auf jeden einzelnen geschützten Computer aus dem Internet herunterladen oder einen Computer als Verteiler einrichten. In diesem Fall werden Updates auf den Verteiler heruntergeladen, ohne sie zu installieren, und anschließend an die Netzwerkcomputer verteilt. Um Datenbank-Updates zu kopieren und zu speichern, ohne Sie zu installieren, verwenden Sie die Aufgabe Update-Verteilung.

Bevor Updates für die Module installiert werden, kann Kaspersky Embedded Systems Security Backup-Kopien der zuvor installierten Module anlegen. Wenn das Update der Programm-Module unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zu den zuvor installierten Programm-Modulen zurück. Außerdem können Sie manuell ein Rollback des Updates der Module zu den zuvor installierten Updates ausführen.

Während der Installation von heruntergeladenen Updates wird Kaspersky Security Service automatisch beendet und anschließend neu gestartet.

Über Updates der Programm-Datenbanken von Kaspersky Embedded Systems Security

Die auf einem geschützten Computer gespeicherten Datenbanken von Kaspersky Embedded Systems Security veralten schnell. Die Virenanalytiker von Kaspersky Lab entdecken täglich Hunderte neuer Bedrohungen, erstellen entsprechende Einträge und nehmen sie in die Updates der Programm-Datenbanken auf. Ein Datenbanken-Update besteht aus einer oder mehreren Dateien mit Einträgen, durch die sich Bedrohungen identifizieren lassen, die seit dem vorhergehenden Update erkannt wurden. Um das Infektionsrisiko für den Computer auf ein Minimum zu reduzieren, führen Sie regelmäßig ein Datenbanken-Update aus.

Standardmäßig tritt das Ereignis *Programm-Datenbanken sind veraltet* ein, wenn die Datenbanken von Kaspersky Embedded Systems Security seit der Erstellung der letzten installierten Datenbanken-Updates eine Woche lang nicht aktualisiert wurden. Erfolgt binnen zwei Wochen kein Update, erscheint die Meldung *Programm-Datenbanken sind stark veraltet*. Informationen über den aktuellen Staus der Datenbanken (s. Abschnitt "Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen" auf S. 171) werden im Detailbereich des Knotens **Kaspersky Embedded Systems Security** der Programmkonsolenstruktur angezeigt. Sie können die allgemeinen Parameter von Kaspersky Embedded Systems Security verwenden, um eine andere Anzahl von Tagen anzugeben, nach denen diese Ereignisse eintreten. Sie können ferner die Benachrichtigungen des Administrators über diese Ereignisse anpassen (siehe Abschnitt "Benachrichtigungen an Administrator und Benutzer anpassen" auf Seite 229).

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

Sie können die Updates auf jeden der geschützten Computer herunterladen oder einen Server als Verteiler einrichten, so dass die Updates auf ihn kopiert und anschließend an die Computer verteilt werden. Wenn Sie Kaspersky Security Center für die zentralisierte Verwaltung der Computer im Unternehmen verwenden, können Sie den Kaspersky Security Center-Administrationsserver als Verteiler für das Herunterladen von Updates einsetzen.

Sie können die Aufgabe für das Update der Programm-Datenbanken manuell oder nach Zeitplan starten (siehe Abschnitt "Einstellungen im Zeitplan für den Aufgabenstart anpassen" auf Seite 160). Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe zum Update der Programm-Datenbanken stündlich.

Wenn der Update-Download unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zu den Datenbanken mit 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 (siehe Abschnitt "Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security" auf Seite 194).

Schemata für das Datenbanken-Update und Update der Module von Antiviren-Anwendungen in einem Unternehmen

Die Auswahl der Update-Quelle in Update-Aufgaben ist davon abhängig, nach welchem Schema das Datenbanken-Update und Update der Programm-Module der Antiviren-Anwendungen in Ihrem Unternehmen aktualisiert werden.

Sie können die Datenbanken und Module von Kaspersky Embedded Systems Security auf den geschützten Computern nach folgenden Schemata aktualisieren:

- Download von Updates direkt aus dem Internet auf jeden der geschützten Computer (Schema 1).
- Download von Updates aus dem Internet auf einen zwischengeschalteten Computer und Verteilung des Updates von diesem Computer aus auf die anderen Computer.

Als Verteiler kann ein beliebiger Computer dienen, auf dem eine der folgenden Anwendungen installiert ist:

- Kaspersky Embedded Systems Security (Schema 2).
- Kaspersky Security Center-Administrationsserver (Schema 3).

Das Update über einen Computer, der als Verteiler funktioniert, erlaubt nicht nur die Einsparung von Internet-Datenverkehr, sondern bietet den Computern auch zusätzliche Sicherheit.

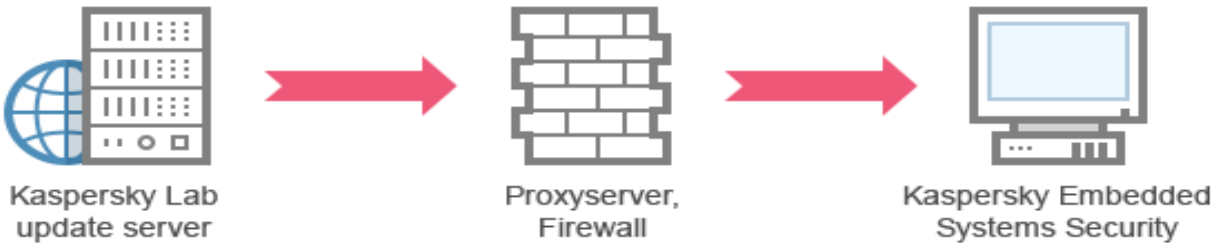
Im Folgenden werden die genannten Update-Schemata beschrieben.

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 Computer in den Einstellungen der Aufgaben zum Update der Programm-Datenbanken und Update der Programm-Module als Update-Quelle die Kaspersky-Lab-Update-Server an.

Als Update-Quelle können auch andere HTTP- oder FTP-Server gewählt werden, auf denen sich ein Ordner mit den Update-Dateien befindet.

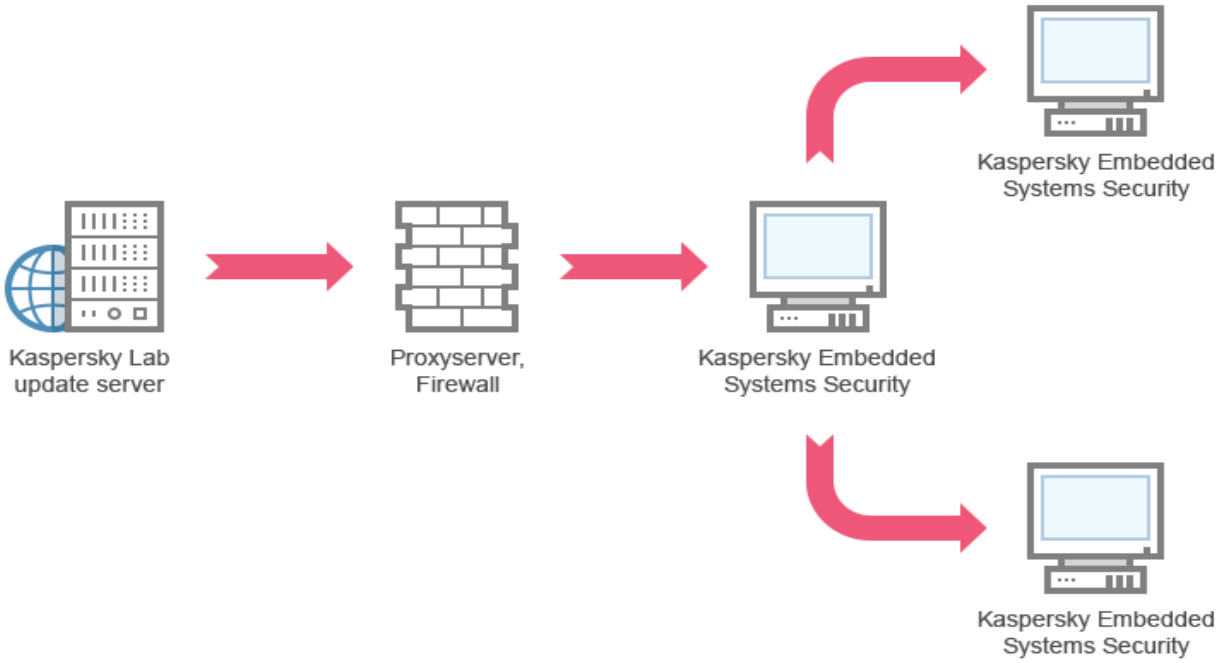


Schema 2. Aktualisieren von Datenbanken und Modulen über einen der geschützten Computer

► *Um die Updates für Kaspersky Embedded Systems Security über einen der geschützten Computer anzupassen, gehen Sie wie folgt vor:*

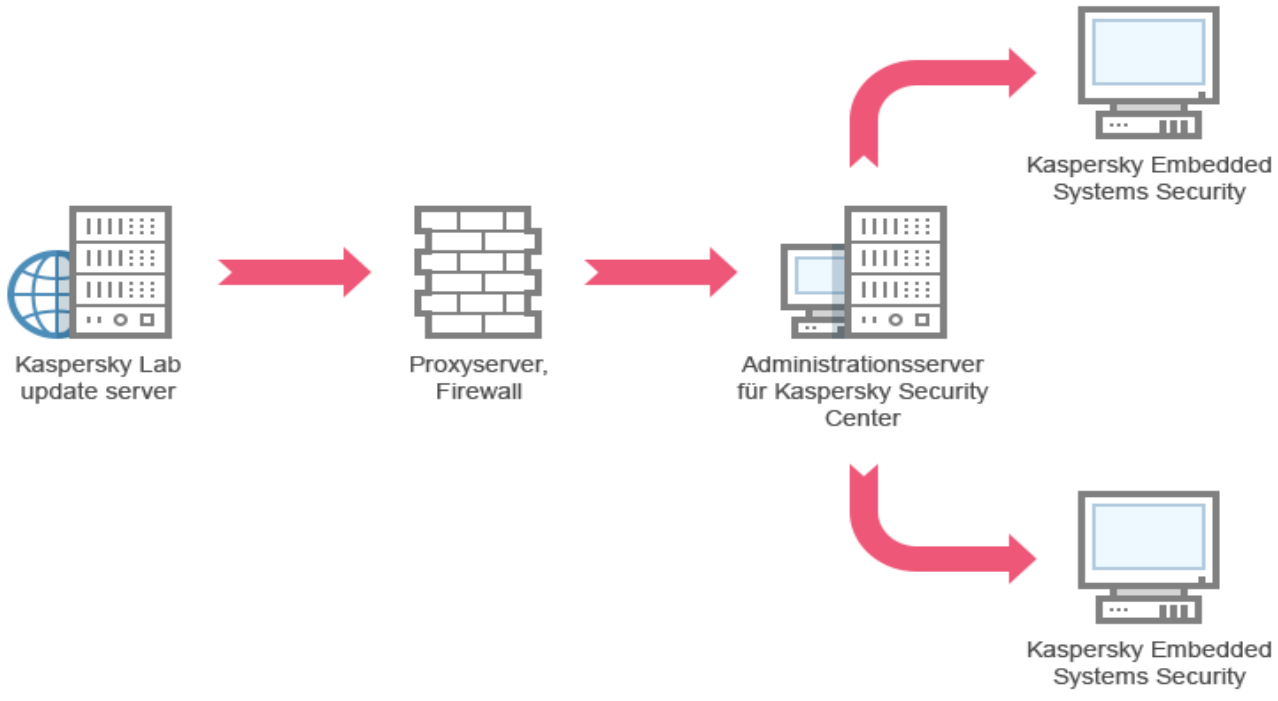
1. Kopieren Sie die Updates auf den ausgewählten geschützten Computer. Gehen Sie hierzu wie folgt vor:
   - Passen Sie auf dem als Verteiler ausgewählten Computer die Einstellungen der Aufgabe Update-Verteilung an:
     a. Geben Sie als Update-Quelle den Kaspersky Lab Update-Server an.
     b. Geben Sie als Ordner, in dem die Updates gespeichert werden sollen, einen freigegebenen Ordner an.
2. Verteilen Sie die Updates auf die übrigen geschützten Computer. Gehen Sie hierzu wie folgt vor:
   - Passen Sie auf jedem geschützten Computer die Aufgaben zum Update der Programm-Datenbanken und Update der Programm-Module an (siehe Abbildung unten).
     a. Geben Sie als Update-Quelle den Ordner auf dem Laufwerk des ausgewählten Rechners an, in den die Updates kopiert werden.

Kaspersky Embedded Systems Security erhält die Updates dann über einen der geschützten Computer.



Schema 3. Aktualisieren von Datenbanken und Modulen über den Kaspersky Security Center-Administrationsserver

Wenn Sie das Programm Kaspersky Security Center für die zentrale Verwaltung des Antiviren-Schutzes von Computern einsetzen, können Sie Updates über den Kaspersky Security Center-Administrationsserver downloaden (s. Abbildung unten).



► *Um den Erhalt von Updates für Kaspersky Embedded Systems Security über den Kaspersky*

Security Center-Administrationsserver anzupassen, gehen Sie wie folgt vor:

1. Laden Sie die Updates von einem Kaspersky Lab Update-Server auf den Administrationsserver von Kaspersky Security Center herunter. Gehen Sie hierzu wie folgt vor:
   - Passen Sie die globale Aufgabe Update-Download durch Administrationsserver für die angegebenen Zusammenstellungen von Computern an:
     a. Geben Sie als Update-Quelle die Kaspersky Lab Update-Server an.
2. Verteilen Sie die Updates auf die geschützten Computer. 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 Computer an:
     a. Wählen Sie im Aufgabenzeitplan die Startfrequenz **Nach Update-Download durch den Administrationsserver**.

        Der Administrationsserver startet die Aufgabe jedes Mal, wenn er Updates empfängt (Diese Variante gilt als empfohlen).

     Die Startfrequenz **Nach Update-Download durch den Administrationsserver** kann in der Programmkonsole nicht angegeben werden.

   - Erstellen Sie auf jedem der geschützten Computer die Aufgaben Update der Programm-Datenbanken und Update der Programm-Module:
     a. Geben Sie den Kaspersky Security Center-Administrationsserver als Update-Quelle an.
     b. Passen Sie den Zeitplan für die Aufgabe bei Bedarf an.

     Bei zu seltenen Updates der Antiviren-Datenbanken von Kaspersky Embedded Systems Security (einmal monatlich bis einmal jährlich) sinkt die Wahrscheinlichkeit, dass Bedrohungen entdeckt werden, während die Häufigkeit von Fehlalarmen der Programmkomponenten steigt.

Kaspersky Embedded Systems Security erhält die Updates dann über den Kaspersky Security Center-Administrationsserver.

Wenn Sie zur Update-Verteilung den Einsatz des Administrationsservers von Kaspersky Security Center planen, installieren Sie zuerst auf jedem geschützten Computer die Programmkomponente Administrationsagent, die zum Lieferumfang von Kaspersky Security Center gehört. Er gewährleistet die Interaktion zwischen dem Administrationsserver und Kaspersky Embedded Systems Security auf dem geschützten Computer. Ausführliche Informationen zum Administrationsagenten und seiner Konfiguration mithilfe von Kaspersky Security Center finden Sie in der *Hilfe für Kaspersky Security Center*.

Einstellung von Update-Aufgaben

Dieser Abschnitt enthält Anweisungen zum Anpassen der Update-Aufgaben von Kaspersky Embedded Systems Security.

In diesem Abschnitt

Anpassen der Einstellungen für die Arbeit mit Update-Quellen für Kaspersky Embedded Systems Security

Für jede Update-Aufgabe, mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates der Programmdatenbanken, können Sie eine oder mehrere Update-Quellen angeben, benutzerdefinierte Update-Quellen hinzufügen und die Verbindungseinstellungen für die angegebenen Update-Quellen konfigurieren.

Nach Anpassung der Einstellungen für die Update-Aufgaben werden die neuen Werte in den laufenden Update-Aufgaben nicht sofort übernommen. Die vorgenommenen Einstellungen treten erst beim nächsten Aufgabenstart in Kraft.

► *Um den Typ der Update-Quelle festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Update-Aufgabe entspricht, die Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Wählen Sie im Abschnitt **Update-Quelle** den Typ der Update-Quelle für Kaspersky Embedded Systems Security aus:

   - **Kaspersky Security Center-Administrationsserver**

     Kaspersky Embedded Systems Security verwendet als Update-Quelle den Kaspersky Security Center-Administrationsserver.

     Sie können diese Variante auswählen, wenn die Programme von Kaspersky Lab in Ihrem Netzwerk mithilfe des Remote-Verwaltungssystems von Kaspersky Security Center verwaltet werden und auf dem geschützten Computer der Administrationsagent installiert ist – eine Komponente von Kaspersky Security Center, die eine Kommunikation zwischen den Computern und dem Administrationsserver gewährleistet.

   - **Kaspersky-Lab-Update-Server**

     Kaspersky Embedded Systems Security verwendet als Update-Quelle die Internetseiten von Kaspersky Lab, auf denen Datenbanken-Updates und Updates der Programm-Module für alle Programme von Kaspersky Lab veröffentlicht werden.

     Diese Variante gilt als Standard.

- **Andere HTTP-, FTP-Server oder Netzwerkressourcen**

  Kaspersky Embedded Systems Security verwendet als Update-Quelle die vom Administrator angegebenen HTTP- oder FTP-Server oder Ordner im lokalen Netzwerkordner.

  Sie können eine Liste mit Quellen erstellen, die aktuelle Updates enthalten, indem Sie auf den Link **Andere HTTP-, FTP-Server oder Netzwerkressourcen** klicken.

5. Passen Sie bei Bedarf die erweiterten Einstellungen für die benutzerdefinierten Update-Quellen an:

   a. Betätigen Sie den Link **Andere HTTP-, FTP-Server oder Netzwerkressourcen**.

      i. Aktivieren oder deaktivieren Sie im erscheinenden Fenster **Update-Server** die Kontrollkästchen neben den benutzerdefinierten Update-Quellen, um deren Verwendung zu starten oder zu beenden.

      ii. Klicken Sie auf **OK**.

   b. Aktivieren oder deaktivieren Sie im Abschnitt **Update-Quelle** auf der Registerkarte **Allgemein** das Kontrollkästchen **Kaspersky-Lab-Update-Server verwenden, wenn vom Benutzer angegebene Server nicht verfügbar sind**.

      Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung der Kaspersky Lab-Update-Server als Update-Quelle, wenn die von Ihnen ausgewählten Update-Quellen nicht verfügbar sind.

      Ist das Kontrollkästchen aktiviert, so ist die Funktion aktiv.

      Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

      Sie können das Kontrollkästchen **Kaspersky-Lab-Update-Server verwenden, wenn vom Benutzer angegebene Server nicht verfügbar sind** aktivieren, wenn die Option **Andere HTTP-, FTP-Server oder Netzwerkressourcen** ausgewählt wurde.

6. Wählen Sie im Fenster **Aufgabeneinstellungen** die Registerkarte **Verbindungseinstellungen** aus, um die Einstellungen für die Verbindungsaufnahme mit der Update-Quelle zu konfigurieren:

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Lab-Update-Servern verwenden**.

     Das Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der Proxyserver-Einstellungen, wenn das Update von den Kaspersky-Lab-Servern erfolgt, oder das Kontrollkästchen **Kaspersky-Lab-Update-Server verwenden, wenn vom Benutzer angegebene Server nicht verfügbar sind** aktiviert ist.

     Wenn dieses Kontrollkästchen aktiviert ist, werden die Proxyserver-Einstellungen verwendet.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden die Proxyserver-Einstellungen nicht verwendet.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Proxyserver-Einstellungen für die Verbindung zu anderen Servern verwenden**.

     Das Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der Proxy-Server-Einstellungen, wenn als Update-Quelle die Option **Andere HTTP-, FTP-Server oder Netzwerkressourcen** ausgewählt wurde.

     Wenn dieses Kontrollkästchen aktiviert ist, werden die Proxyserver-Einstellungen verwendet.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

Informationen über das Konfigurieren der optionalen Proxyservereinstellungen und Authentifizierungseinstellungen für den Zugriff auf den Proxyserver finden Sie im Abschnitt Aufgabe zum Update der Datenbank von Kaspersky Embedded Systems Security starten und anpassen.

7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Update-Quelle für Kaspersky Embedded Systems Security werden gespeichert und beim nächsten Aufgabenstart verwendet.

Sie können die Liste der benutzerdefinierten Update-Quellen für Kaspersky Embedded Systems Security bearbeiten.

► *Gehen Sie wie folgt vor, um die Liste der benutzerdefinierten Update-Quellen für das Programm zu ändern:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Update-Aufgabe entspricht, die Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Betätigen Sie den Link **Andere HTTP-, FTP-Server oder Netzwerkressourcen**.

   Daraufhin wird das Fenster **Update-Server** geöffnet.
5. Führen Sie folgende Aktionen aus:

   - Geben Sie im Eingabefeld die Adresse des Ordners mit den Update-Dateien auf einem FTP- oder HTTP-Server an; geben Sie einen lokalen oder einen Netzwerkordner im UNC-Format (Universal Naming Convention) an, um eine neue benutzerdefinierte Update-Quelle hinzuzufügen. Drücken Sie die Taste **EINGABE**.

     Standardmäßig wird der hinzugefügte Ordner als Update-Quelle verwendet.
   - Um die Verwendung einer benutzerdefinierten Quelle zu deaktivieren, entfernen Sie in der Liste das Kontrollkästchen neben der Quelle.
   - Um die Verwendung einer benutzerdefinierten Quelle zu aktivieren, aktivieren Sie in der Liste das Kontrollkästchen neben der Quelle.
   - Um die Reihenfolge zu ändern, in der Kaspersky Embedded Systems Security auf benutzerdefinierte Update-Quellen zugreift, verschieben Sie die gewünschte Quelle mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Stelle der Liste, je nachdem, wann auf die Quelle zugegriffen werden soll.
   - Um den Pfad einer benutzerdefinierten Quelle zu ändern, markieren Sie die Quelle in der Liste und klicken auf die Schaltfläche **Ändern**. Nehmen Sie dann im Eingabefeld die erforderlichen Änderungen vor und klicken Sie die **EINGABE**-Taste.
   - Um eine benutzerdefinierte Quelle zu löschen, markieren Sie sie in der Liste und klicken Sie auf die Schaltfläche **Löschen**.

Ist nur eine einzige benutzerdefinierte Quelle in der Liste enthalten, können Sie diese nicht entfernen.

6. Klicken Sie auf **OK**.

Die Änderungen an der Liste der benutzerdefinierten Update-Quellen für das Programm werden gespeichert.

Optimierung der Nutzung des Festplatten-Subsystems bei der Ausführung der Aufgabe zum Update der Programm-Datenbanken

Bei Ausführung der Aufgabe zum Update der Programm-Datenbanken legt Kaspersky Embedded Systems Security die Update-Dateien auf einer lokalen Festplatte des Computers ab. Sie können die Belastung des Festplatten-Subsystems des Computers verringern, indem Sie die Update-Dateien während der Ausführung der Update-Aufgabe auf einer virtuellen Festplatte im Arbeitsspeicher ablegen.

Diese Funktion ist für das Betriebssystem Microsoft Windows 7 und höher verfügbar.

Bei Nutzung dieser Funktion kann während der Ausführung der Aufgabe Update der Programm-Datenbanken eine zusätzliche logische Festplatte im Betriebssystem erscheinen. Nach Abschluss der Aufgabe verschwindet diese logische Festplatte wieder aus dem Betriebssystem.

► *Gehen Sie wie folgt vor, um die Belastung des Festplatten-Subsystems bei der Ausführung der Aufgabe Update der Programm-Datenbanken zu verringern:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten **Update der Programm-Datenbanken** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Update der Programm-Datenbanken** auf den Link **Eigenschaften**.
4. Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
5. Nehmen Sie im Abschnitt "Optimierung der Nutzung des Festplatten-Subsystems" die folgenden Einstellungen vor:
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern**.

     Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktion zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher.

     Ist das Kontrollkästchen aktiviert, so ist die Funktion aktiv.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

- Geben Sie im Feld **Für die Optimierung zur Verfügung stehender Arbeitsspeicher** das Arbeitsspeichervolumen 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 512 MB eingestellt. Das minimale Arbeitsspeichervolumen beträgt 400 MB.

6. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und beim nächsten Aufgabenstart verwendet.

Einstellungen der Aufgabe zur Update-Verteilung anpassen

► *Um die Einstellungen der Aufgabe zur Update-Verteilung anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten **Update-Verteilung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Update-Verteilung** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Passen Sie auf den Registerkarten **Allgemein** und **Verbindungseinstellungen** die Einstellungen für die Arbeit mit den Update-Quellen an (siehe Abschnitt "Anpassen der Einstellungen für die Arbeit mit Update-Quellen für Kaspersky Embedded Systems Security" auf Seite 188).
5. Führen Sie auf der Registerkarte **Allgemein** im Abschnitt **Einstellungen für die Update-Verteilung** folgende Schritte aus:
   - Geben Sie die Bedingungen für die Update-Verteilung des Programms an:
     - **Updates der Programm-Datenbanken verteilen**.

       Kaspersky Embedded Systems Security lädt nur Updates der Programm-Datenbanken herunter.

       Diese Variante gilt als Standard.
     - **Wichtige Updates der Programm-Module verteilen**.

       Kaspersky Embedded Systems Security lädt nur wichtige Updates der Programm-Module von Kaspersky Embedded Systems Security herunter.
     - **Updates der Programm-Datenbanken und wichtige Updates der Programm-Module verteilen**.

       Kaspersky Embedded Systems Security lädt Updates der Programm-Datenbanken und wichtige Updates der Programm-Module für Kaspersky Embedded Systems Security herunter.
   - Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Kaspersky Embedded Systems Security die erhaltenen Updates kopieren soll.
6. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160).
7. Passen Sie auf der Registerkarte **Mit folgenden Rechten starten** die Aufgabe zum Start mithilfe von Benutzerrechten an (siehe Abschnitt "Festlegen eines Benutzerkontos für den Aufgabenstart" auf Seite 163).
8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und beim nächsten Aufgabenstart verwendet.

Einstellungen der Aufgabe zum Update der Programm-Module anpassen

► *Um die Einstellungen der Aufgabe zum Update der Programm-Module zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten **Update der Programm-Module** aus.
3. Klicken Sie im Ergebnisfenster des Knotens **Update der Programm-Module** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Passen Sie auf den Registerkarten **Allgemein** und **Verbindungseinstellungen** die Einstellungen für die Arbeit mit den Update-Quellen an (siehe Abschnitt "Anpassen der Einstellungen für die Arbeit mit Update-Quellen für Kaspersky Embedded Systems Security" auf Seite 188).
5. Konfigurieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Programm-Update-Einstellungen** die Einstellungen für das Update der Programm-Module:

   - **Nur auf wichtige Updates der Programm-Module überprüfen**

     Kaspersky Embedded Systems Security benachrichtigt über auf der Quelle vorhandene dringende Updates für Programm-Module ohne die Updates herunterzuladen. Eine Benachrichtigung erfolgt, wenn die Benachrichtigung über Ereignisse dieser Art aktiviert ist.

     Diese Variante gilt als Standard.

   - **Wichtige Updates der Programm-Module verteilen und installieren**

     Kaspersky Embedded Systems Security lädt kritische Updates für Programm-Module herunter und installiert sie.

   - **Neustart des Betriebssystems zulassen**

     Neustart des Computers nach einer Installation von Updates, die einen Neustart erfordern.

     Wenn dieses Kontrollkästchen aktiviert ist, startet Kaspersky Embedded Systems Security das Betriebssystem nach einer Installation von Updates, die einen Neustart erfordern, neu.

     Das Kontrollkästchen ist aktiv, wenn die Variante **Wichtige Updates der Programm-Module verteilen und installieren** ausgewählt ist.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - **Über verfügbare planmäßige Updates der Programm-Module informieren**

     Benachrichtigungen über alle auf der Quelle vorhandenen planmäßigen Updates für Programm-Module Kaspersky Embedded Systems Security erhalten. Das Programm benachrichtigt dann, wenn die Benachrichtigung über Ereignisse dieser Art aktiviert ist.

     Wenn dieses Kontrollkästchen aktiviert ist, benachrichtigt Kaspersky Embedded Systems Security über alle auf der Quelle vorhandenen planmäßigen Updates für Programm-Module.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160). Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe Update der Programm-Module jeden Freitag um 16:00 Uhr (Zeit gemäß den regionalen Einstellungen des geschützten Computers).
7. Passen Sie auf der Registerkarte **Mit folgenden Rechten starten** die Aufgabe zum Start mithilfe von Benutzerrechten an (siehe Abschnitt "Festlegen eines Benutzerkontos für den Aufgabenstart" auf Seite 163).
8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und beim nächsten Aufgabenstart verwendet.

Geplante Updatepakete werden von Kaspersky Lab nicht auf den Update-Servern veröffentlicht, um sie automatisch zu installieren. Sie können solche Updatepakete von der Kaspersky-Lab-Webseite downloaden. Sie können festlegen, dass der Administrator über das Ereignis *Ein planmäßiges Update der Programm-Module ist verfügbar* benachrichtigt wird. Die Benachrichtigung enthält die Adresse der Webseite, von der Sie geplante Updates herunterladen können.

Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security

Vor der Übernahme des Datenbanken-Updates 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 Update der Programm-Datenbanken Probleme auftreten, können Sie die Datenbanken mit den zuvor installierten Updates wiederherstellen. Starten Sie dazu die Aufgabe zum Rollback des Datenbanken-Updates.

► *Um die Aufgabe Rollback des Datenbanken-Updates zu starten,*

Klicken Sie auf den Link **Starten** im Ergebnisfenster des Knotens **Rollback des Datenbanken-Updates**.

Rollback des Updates für Programm-Module

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

Bevor Updates für Programm-Module installiert werden, legt Kaspersky Embedded Systems Security Backup-Kopien der bisher verwendeten Module an. Wenn die Aktualisierung von Modulen unterbrochen oder fehlerhaft abgeschlossen wurde, kehrt Kaspersky Embedded Systems Security automatisch zu den Modulen mit den zuletzt installierten Updates zurück.

Um ein Rollback der Programm-Module auszuführen, verwenden Sie die Verwaltungskomponente von Microsoft Windows **Programme ändern und löschen**.

Statistik zu Update-Aufgaben

Während eine Update-Aufgabe ausgeführt wird, können Sie in Echtzeit Informationen über das Volumen der Daten, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt empfangen wurden, sowie weitere Informationen zur Aufgabenausführung anzeigen.

Wenn die Aufgabe abgeschlossen oder beendet wurde, können Sie diese Informationen im Protokoll der Aufgabenausführung einsehen.

► *Um die Statistik der Update-Aufgabe anzuzeigen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe entspricht, deren Statistik Sie ansehen möchten.

Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Wenn Sie die Aufgabe zum Update der Programm-Datenbanken oder die Aufgabe zur Update-Verteilung anzeigen, wird im Block **Statistik** das Volumen der Daten anzeigt, die bis zum jetzigen Zeitpunkt von Kaspersky Embedded Systems Security empfangen wurden (**Empfangene Daten**).

Bei Anzeige der Aufgabe zum Update der Programm-Module werden die in der nachfolgenden Tabelle beschriebenen Informationen dargestellt.

Tabelle 32. Informationen über die Aufgabe Update der Programm-Module

Feld	Beschreibung
Empfangene Daten	Gesamtvolumen der empfangenen Daten.
Wichtige Updates sind verfügbar	Anzahl der kritischen Updates, die zur Installation bereitstehen.
Planmäßige Updates sind verfügbar	Anzahl der geplanten Updates, die zur Installation bereitstehen.
Fehler beim Übernehmen von Updates	Wenn dieser Wert ungleich Null ist, wurde das Update nicht übernommen. Den Namen des Updates, bei dessen Übernahme ein Fehler aufgetreten ist, finden Sie im Protokoll der Aufgabenausführung (siehe Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in Protokollen der Aufgabenausführung anzeigen" auf Seite 218).

Isolierung und Verschieben von Objekten ins Backup

Dieser Abschnitt enthält Informationen über das Verschieben von gefundenen schädlichen Objekten ins Backup, bevor diese desinfiziert oder gelöscht werden, sowie Information über die Isolation möglicherweise infizierter Objekte.

In diesem Kapitel

Isolierung möglicherweise infizierter Objekte. Quarantäne

Dieser Abschnitt enthält Informationen über die Isolierung von möglicherweise infizierten Objekten, also über die Verschiebung dieser Objekte in die Quarantäne sowie über die Anpassung der Quarantäneeinstellungen.

In diesem Abschnitt

Über die Isolierung möglicherweise infizierter Objekte

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.

Quarantäneobjekte anzeigen

Die unter Quarantäne stehenden Objekte können im Knoten **Quarantäne** der Programmkonsole angezeigt werden.

► *Um Objekte aus der Quarantäne anzusehen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.

2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.

   Die Informationen über die in der Quarantäne befindlichen Objekte werden im Ergebnisbereich des ausgewählten Knotens angezeigt.

► *Um ein bestimmtes Objekt in der Liste der Quarantäne-Objekte zu finden,*

sortieren Sie die Objekte (siehe Abschnitt "Quarantäneobjekte sortieren" auf Seite 197) oder filtern Sie die Objekte (siehe Abschnitt "Quarantäneobjekte filtern" auf Seite 197).

In diesem Abschnitt

Quarantäneobjekte sortieren

Die Objekte in der Liste mit den Quarantäneobjekten sind standardmäßig in umgekehrter chronologischer Reihenfolge nach dem Verschiebedatum angeordnet. Um ein bestimmtes Objekt zu finden, können Sie die Objekte nach dem Spalteninhalt und den Objektinformationen sortieren. Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne** schließen und erneut öffnen, oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und dann erneut aus dieser Datei öffnen.

► *Um die Objekte zu sortieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.
3. Klicken Sie im Ergebnisfenster des Knotens **Quarantäne** auf den Titel der Spalte, nach deren Inhalt die Objekte in der Liste sortiert werden sollen.

Die Listenobjekte werden nach dem ausgewählten Parameter sortiert.

Quarantäneobjekte filtern

Um ein Objekt in der Quarantäne zu suchen, können Sie die Objekte in der Liste filtern. Das heißt, es werden nur Objekte angezeigt, die den von Ihnen definierten Filterkriterien (Filtern) entsprechen. Das Filterergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne** verlassen und erneut öffnen, oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und sie erneut aus dieser Datei öffnen.

► *Um einen oder mehrere Filter einzustellen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.
3. Wählen Sie im Kontextmenü des Knotennamens den Punkt **Filter** aus.

   Das Fenster **Filtereinstellungen** wird geöffnet.

4. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

   a. Wählen Sie in der Liste **Feldname** ein Element aus, mit dem der Filterwert verglichen werden soll.

   b. Wählen Sie in der Liste **Operator** die Filterbedingungen aus. Die Filterbedingungen in der Liste können unterschiedlich sein, je nachdem, welchen Wert Sie in der Liste **Feldname** gewählt haben.

   c. Geben Sie im Feld **Feldwert** einen Wert für den Filter an oder wählen Sie ihn in der Liste aus.

   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt. Wiederholen Sie die Schritte a–d für jeden Filter, den Sie hinzufügen. Beachten Sie beim Arbeiten mit Filtern die folgenden Anweisungen:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.
   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.
   - Um einen Filter zu entfernen, markieren Sie ihn in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.
   - Um einen Filter zu ändern, wählen Sie den Filter in der Liste im Fenster **Filtereinstellungen** aus. Ändern Sie dann die benötigten Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

5. Nachdem alle Filter hinzugefügt wurden, klicken Sie auf **Übernehmen**.

Die erstellten Filter werden gespeichert.

► *Damit wieder alle Objekte in der Liste der Quarantäneobjekte angezeigt werden,*

wählen Sie im Kontextmenü des Knotens **Quarantäne** den Punkt **Löschen** aus.

Untersuchung von Quarantäne-Objekten

Kaspersky Embedded Systems Security führt in der Grundeinstellung nach jedem Update der Programm-Datenbanken die Systemaufgabe Untersuchung von Quarantäne-Objekten aus. Die Aufgabenparameter werden in folgender Tabelle genannt. Sie können die Einstellungen für die Aufgabe Untersuchung von Quarantäne-Objekten ändern.

Sie können einen Zeitplan für den Aufgabenstart einrichten (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160), die Aufgabe manuell starten sowie die Rechte des Benutzerkontos ändern (siehe Abschnitt "Festlegen eines Benutzerkontos für den Aufgabenstart" auf Seite 163), unter dem die Aufgabe gestartet werden soll.

Wenn die Quarantäne-Objekte nach einem Datenbanken-Update untersucht wurden, kann Kaspersky Embedded Systems Security bestimmte Objekte als nicht infiziert einstufen: Der Status dieser Objekte ändert sich in der Liste auf **Fehlalarm**. Kaspersky Embedded Systems Security kann andere Objekte als infiziert einstufen und für sie Aktionen ausführen, die in den Einstellungen der Aufgabe Untersuchung von Quarantäne-Objekten vorgegeben sind: Desinfizieren bzw. irreparable Objekte löschen.

Tabelle 33. Einstellungen der Aufgabe Untersuchung von Quarantäne-Objekten

Parameter der Aufgabe Untersuchung von Quarantäne-Objekten	Bedeutung
Untersuchungsbereich	Quarantäneordner
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, Werte stehen in der folgenden Tabelle.

Tabelle 34. Sicherheitsparameter der Aufgabe Untersuchung von Quarantäne-Objekten

Sicherheitsparameter	Bedeutung
Objekte untersuchen	Alle Objekte der Untersuchungsbereichs
Optimierung	Deaktiviert
Aktion für infizierte und andere gefundene Objekte	Desinfizieren, irreparable Objekte löschen
Aktion für infizierte Objekte	Überspringen
Objekte ausschließen	Nein
Nicht erkennen	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	Nicht festgelegt.
Objekte nicht scannen, wenn größer als (MB)	Nicht festgelegt.
Alternative NTFS-Ströme	Aktiviert
Laufwerksbootsektoren und MBR	Deaktiviert
iChecker-Technologie verwenden	Deaktiviert
iSwift-Technologie verwenden	Deaktiviert

Sicherheitsparameter	Bedeutung
Zusammengesetzte Objekte untersuchen	• Archive* • SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Der Parameter "Nur neue und veränderte Dateien untersuchen" ist deaktiviert.
Microsoft-Signatur bei Dateien prüfen	Wird nicht ausgeführt.
Heuristische Analyse verwenden	Die Analysestufe **Tief** ist eingestellt.
vertrauenswürdige Zone	Wird nicht verwendet

Wiederherstellen von Objekten aus der Quarantäne

Kaspersky Embedded Systems Security verschiebt Objekte, die möglicherweise infiziert sind, verschlüsselt in den Quarantäne-Ordner, damit der geschützte Computer vor schädlichen Wirkungen bewahrt wird.

Sie können jedes Objekt aus der Quarantäne wiederherstellen. Das kann in folgenden Fällen notwendig sein:

- Wenn nach der Untersuchung von Quarantäne-Objekten anhand der aktualisierten Datenbanken der Status des Objektes in **Fehlalarm** oder **Desinfiziert** geändert worden ist.
- Wenn Sie das Objekt als nicht gefährlich für den Computer einschätzen und es benutzen wollen. Damit Kaspersky Embedded Systems Security dieses Objekt bei künftigen Untersuchungen nicht isoliert, können Sie das Objekt von der Untersuchung in den Aufgaben "Echtzeitschutz für Dateien" und "Untersuchung auf Befehl" ausschließen. Geben Sie dazu das Objekt als Wert der Sicherheitseinstellung **Dateien ausschließen** (nach Dateiname) oder **Nicht erkennen** in diesen Aufgaben an oder fügen Sie es zur vertrauenswürdigen Zone hinzu (auf Seite 471).

Beim Wiederherstellen eines Objektes können Sie entscheiden, wo das wiederhergestellte Objekt gespeichert werden soll: Am ursprünglichen Ort (Standard), in einem speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Computer oder in einem benutzerdefinierten Ordner auf dem Computer, auf dem die Programmkonsole installiert ist, oder auf einem anderen Computer des Netzwerks.

Die Option **Wiederherstellungsordner** dient zum Speichern von wiederhergestellten Objekten auf dem geschützten Computer. Sie können für seine Untersuchung spezielle Sicherheitsparameter festlegen. Der Pfad dieses Ordners wird in den Quarantäneeinstellungen angegeben.

Das Wiederherstellen von Objekten aus der Quarantäne kann den Computer infizieren.

Sie können ein Objekt wiederherstellen, nachdem dessen Kopie im Quarantäne-Ordner gespeichert worden ist, damit Sie es weiter benutzen können, beispielsweise, um das Objekt nach einem Datenbanken-Update noch einmal zu untersuchen.

Wenn ein in die Quarantäne verschobenes Objekt zu einem zusammengesetzten Objekt gehört (z. B. zu einem Archiv), fügt es Kaspersky Embedded Systems Security bei der Wiederherstellung nicht mehr in das zusammengesetzte Objekt ein, sondern speichert es separat im festgelegten Ordner.

Sie können ein Objekt oder mehrere Objekte wiederherstellen.

► *Um eine Datei aus der Quarantäne wiederherzustellen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.
3. Führen Sie im Ergebnisfenster des Knotens **Quarantäne** 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 in der Liste die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der markierten Objekte, und wählen Sie den Punkt **Wiederherstellen** aus.

   Das Fenster **Objektwiederherstellung** wird geöffnet.
4. Geben Sie im Fenster **Objektwiederherstellung** 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.
5. Führen Sie eine der Aktionen durch:
   - Um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im Ursprungsordner wiederherstellen**.
   - Um ein Objekt in einem Ordner wiederherzustellen, den Sie in den Quarantäneeinstellungen als Ordner für wiederhergestellte Objekte angegeben haben, wählen Sie **Im Standard-Ordner wiederherstellen** aus.
   - Um ein Objekt in einem anderen Ordner auf dem Computer, auf dem die Programmkonsole installiert ist, oder in einem freigegebenen Ordner zu speichern, wählen Sie **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** aus und wählen Sie dann den gewünschten Ordner aus oder geben dessen Pfad ein.
6. Wenn Sie nach der Wiederherstellung eine Kopie des Objekts im Quarantäne-Ordner speichern möchten, deaktivieren Sie das Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Speicher löschen**.
7. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

   Alle ausgewählten Objekte werden am vorgegebenen Speicherort wiederhergestellt und gespeichert: Bei Auswahl der Variante **Im Ursprungsordner wiederherstellen** wird jedes Objekt an seinem ursprünglichen Speicherort gespeichert. Bei Auswahl der Variante **Im Standard-Ordner wiederherstellen** oder **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** werden alle Objekte im angegebenen Ordner gespeichert.

8. Klicken Sie auf **OK**.

   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 wiederhergestellte Objekt anstelle des vorhandenen Objektes zu speichern
      - **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie einen neuen Dateinamen für das Objekt und den vollständigen Pfad ein.
      - **Umbenennen und Suffix hinzufügen**, um das Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie im Eingabefeld das Suffix ein.

   b. Wenn Sie mehrere Dateien für die Wiederherstellung markiert haben und die gewählte Aktion **Ersetzen** oder **Umbenennen** angewendet und ein Suffix auf die übrigen markierten Objekte hinzugefügt werden soll, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**. (Wenn Sie den Wert **Umbenennen** eingestellt haben, steht das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden** nicht zur Verfügung.)

   c. Klicken Sie auf **OK**.

   Das Objekt wird wiederhergestellt. Informationen über den Wiederherstellungsvorgang werden im Systemaudit-Protokoll protokolliert.

   Wenn Sie im Fenster **Objektwiederherstellung** nicht die Variante **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, öffnet sich das Fenster **Objektwiederherstellung** noch einmal. Sie können dort den Speicherort angeben, an dem das folgende ausgewählte Objekt wiederhergestellt werden soll (s. Schritt 4 dieser Anleitung).

Verschieben von Objekten in die Quarantäne

Sie können manuell Dateien in die Quarantäne verschieben.

► *Um eine Datei in die Quarantäne zu verschieben, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Quarantäne**.
2. Wählen Sie den Punkt **Hinzufügen** aus.
3. Geben Sie im Fenster **Öffnen** die Datei an, die Sie in die Quarantäne verschieben möchten.
4. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security verschiebt die ausgewählte Datei in die Quarantäne.

Objekte aus der Quarantäne löschen

Gemäß den Einstellungen der Aufgabe zur Untersuchung von Quarantäne-Objekten löscht Kaspersky Embedded Systems Security Objekte, deren Status sich bei der Quarantäne-Untersuchung anhand aktualisierter Datenbanken auf *Infiziert oder gefunden* geändert hat und die Kaspersky Embedded Systems Security nicht desinfizieren konnte, automatisch aus dem Quarantäne-Ordner. Andere Objekte werden von Kaspersky Embedded Systems Security nicht aus der Quarantäne gelöscht.

Sie können ein oder mehrere Objekte manuell aus der Quarantäne entfernen.

► *Um ein oder mehrere Objekte aus der Quarantäne zu entfernen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.
3. Führen Sie eine der Aktionen durch:
   - Wählen Sie zum Entfernen eines Objekts im Kontextmenü des Objektnamens den Punkt **Löschen** aus
   - Um mehrere Objekte zu löschen, markieren Sie die entsprechenden Objekte mithilfe der Taste **Strg** oder **Umschalt** die entsprechenden Objekte. Öffnen Sie anschließend das Kontextmenü für eines der gewählten Objekte und wählen Sie den Punkt **Löschen** aus.
4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um die Operation zu bestätigen.

Die ausgewählten Objekte werden aus der Quarantäne gelöscht.

Möglicherweise infizierte Quarantäneobjekte zur Analyse an Kaspersky Lab einschicken

Wenn das Verhalten einer bestimmten Datei den Verdacht nahelegt, dass sie eine Bedrohung enthält, Kaspersky Embedded Systems Security die Datei aber als virenfrei einstuft, handelt es sich möglicherweise um eine neue, unbekannte Bedrohung, deren Beschreibung noch nicht in den Datenbanken verzeichnet ist. Sie können diese Datei zur Analyse in das Virenlabor von Kaspersky Lab einschicken. Die Viren-Analytiker von Kaspersky Lab untersuchen die Datei. Wenn sie eine neue Bedrohung darin finden, wird den Datenbanken ein entsprechender Eintrag und ein Desinfektionsalgorithmus hinzugefügt. Es ist möglich, dass Kaspersky Embedded Systems Security, wenn Sie das Objekt nach einem Datenbanken-Update erneut untersuchen, die Datei als infiziert einstuft und desinfizieren kann. Dadurch können Sie nicht nur das Objekt retten, sondern auch dabei helfen, eine Virenepidemie zu verhindern.

Nur Dateien aus der Quarantäne können zur Analyse eingeschickt werden. Die in der Quarantäne befindlichen Dateien werden in verschlüsselter Form gespeichert und beim Verschicken nicht von der auf dem Mail-Server installierten Antiviren-Anwendung gelöscht.

Nachdem die Gültigkeit der Lizenz abgelaufen ist, können keine Quarantäneobjekte an Kaspersky Lab geschickt werden.

► *Um eine Datei zur Analyse in das Virenlabor von Kaspersky Lab einzuschicken, gehen Sie wie folgt vor:*

1. Wenn sich die Datei nicht in der Quarantäne befindet, verschieben Sie sie zuerst in die **Quarantäne**.
2. Öffnen Sie im Knoten **Quarantäne** in der Liste der Quarantäneobjekte das Kontextmenü der Datei, die zur Analyse an Kaspersky Lab geschickt werden soll, und wählen Sie den Punkt **Objekt zur Analyse einschicken**.
3. Klicken Sie im erscheinenden Bestätigungsfenster auf **Ja**, wenn Sie das ausgewählte Objekt tatsächlich zur Untersuchung versenden möchten.
4. Wenn auf dem Computer, auf dem die Programmkonsole installiert ist, ein Mail-Client eingerichtet ist, wird eine neue E-Mail-Nachricht erstellt. Prüfen Sie die Nachricht und klicken Sie anschließend auf die Schaltfläche **Senden**.

   Das Feld **Empfänger** enthält die E-Mail-Adresse von Kaspersky Lab newvirus@kaspersky.com. Das Feld "Betreff" enthält den Text "Quarantäneobjekt".

Der Nachrichtenkörper enthält den Text "Datei wurde zur Analyse an Kaspersky Lab geschickt". Sie können der Nachricht zusätzliche Informationen über die Datei hinzufügen: z. B. warum Sie die Datei für möglicherweise infiziert oder gefährlich halten, wie sich die Datei verhält und wie sie das System beeinflusst.

Die Nachricht enthält als Anlage das Archiv <Objektname>.cab. Es enthält die Datei "<uuid>.klq" mit dem Objekt in verschlüsselter Form, die Datei "<uuid>.txt" mit Daten, die Kaspersky Embedded Systems Security über das Objekt abgerufen hat, sowie die Datei "Sysinfo.txt", die folgende Informationen über Kaspersky Embedded Systems Security und das auf dem Computer installierte Betriebssystem enthält:

- Name und Version des Betriebssystems.
- Name und Version von Kaspersky Embedded Systems Security.
- Veröffentlichungsdatum der zuletzt installierten Updates der Programm-Datenbanken.
- Aktiver Schlüssel.

Diese Informationen benötigen die Virenanalytiker von Kaspersky Lab zur schnellen und effektiven Analyse einer Datei. Wenn Sie diese Daten nicht weitergeben möchten, können Sie die Datei Sysinfo.txt aus dem Archiv entfernen.

Falls auf dem Computer, auf dem die Programmkonsole installiert ist, kein Mail-Client vorhanden ist, schlägt das Programm vor, das ausgewählte verschlüsselte Objekt in einer Datei zu speichern. Schicken Sie die Datei manuell an Kaspersky Lab.

► *Um ein verschlüsseltes Objekt in einer Datei zu speichern, gehen Sie wie folgt vor:*

1. Klicken Sie im nächsten Fenster zum Speichern des Objekts auf **OK**.
2. Wählen Sie den Ordner auf einem Laufwerk des geschützten Computers oder den Netzwerkordner, in den Sie die Datei mit dem Objekt speichern möchten.

Das Objekt wird in einer CAB-Datei gespeichert.

Anpassen der Quarantäne-Einstellungen

Sie können die Quarantäne-Einstellungen anpassen. Neue Quarantäne-Einstellungen werden unmittelbar nach dem Speichern übernommen.

► *Um die Quarantäneparameter anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Quarantäne**.
3. Wählen Sie den Menüpunkt **Eigenschaften**.

4. Passen Sie im Fenster **Eigenschaften der Quarantäne** die Quarantäne-Einstellungen entsprechend an:
   - Im Abschnitt **Quarantäne-Einstellungen**:
     - **Quarantäneordner**

       Pfad zum Quarantäne-Ordner im UNC-Format (Universal Naming Convention).

       Standardmäßig ist der folgende Pfad eingestellt: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Quarantine\.

     - **Maximale Größe der Quarantäne**

       Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktion, die die Gesamtgröße der Objekte verfolgt, die sich in der Quarantäne befinden. Bei einer Überschreitung des vorgegebenen Wertes (als Standard gelten 200 MB) protokolliert Kaspersky Embedded Systems Security das Ereignis *Maximale Größe der Quarantäne wurde überschritten* und benachrichtigt gemäß den Einstellungen für Benachrichtigungen über Ereignisse dieses Typs.

       Wenn dieses Kontrollkästchen aktiviert ist, verfolgt Kaspersky Embedded Systems Security die Gesamtgröße der Objekte, die sich in der Quarantäne befinden.

       Wenn dieses Kontrollkästchen deaktiviert ist, verfolgt Kaspersky Embedded Systems Security die Gesamtgröße der Objekte in der Quarantäne nicht.

       Das Kontrollkästchen ist standardmäßig deaktiviert.

     - **Grenzwert für verfügbaren Speicherplatz**

     Überschreitet der Umfang der in der Quarantäne befindlichen Objekte die maximale Größe der Quarantäne oder den Grenzwert für den verfügbaren Speicherplatz, so werden Sie von Kaspersky Embedded Systems Security hierüber benachrichtigt, wobei die Objekte jedoch trotzdem in die Quarantäne verschoben werden.

   - Im Abschnitt **Einstellungen für die Wiederherstellung von Objekten**:
     - **Ordner für die Wiederherstellung von Objekten**
5. Klicken Sie auf **OK**.

Die vorgenommenen Quarantäne-Einstellungen werden gespeichert.

Quarantäne-Statistik

In der Statistik für die Quarantäne können Sie Informationen über die Anzahl der Quarantäneobjekte erhalten.

► *Um eine Statistik für die Quarantäne anzuzeigen,*

wählen Sie im Kontextmenü des Knotens **Quarantäne** in der Struktur der Programmkonsole den Punkt **Statistik** aus.

Im Fenster **Statistik** werden Informationen über die aktuelle Anzahl der Quarantäneobjekte angezeigt (s. Tabelle unten):

Feld	Beschreibung
Möglicherweise infizierte Objekte	Anzahl der von Kaspersky Embedded Systems Security gefundenen Objekte, die als möglicherweise infiziert eingestuft wurden
Aktuelle Größe der Quarantäne	Gesamtvolumen der Daten im Quarantäne-Ordner.
Fehlalarme	Anzahl der Objekte, die den Status *Fehlalarm* erhielten, weil sie bei der Untersuchung von Quarantäne-Objekten unter Verwendung von aktualisierten Datenbanken nicht infiziert eingestuft wurden.
Desinfizierte Objekte	Anzahl der Objekte, denen nach der Untersuchung von Quarantäne-Objekten der Status *Desinfiziert* zugewiesen wurde.
Objekte insgesamt	Anzahl der Quarantäneobjekte.

Backup-Kopien von Objekten erstellen. Backup

Dieser Abschnitt enthält Informationen über das Verschieben von gefundenen schädlichen Objekten ins Backup, bevor diese desinfiziert oder gelöscht werden, sowie Anleitungen zur Anpassung der Backup-Einstellungen.

In diesem Abschnitt

Über das Verschieben von Objekten ins Backup vor der Desinfektion oder dem Löschen

Bevor Objekte desinfiziert oder gelöscht werden, speichert Kaspersky Embedded Systems Security verschlüsselte Kopien der als *Infiziert* eingestuften Objekte im *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 freie Festplattenplatz kann sich verringern.

Sie können Dateien aus dem Backup entweder im ursprünglichen Ordner oder in einem anderen Ordner auf dem geschützten Computer oder auf einem anderen Computer des lokalen Netzwerks wiederherstellen. Sie können eine Datei aus dem Backup beispielsweise wiederherstellen, wenn die infizierte Originaldatei wichtige Informationen enthielt, die Integrität der Datei aber bei der Desinfektion durch Kaspersky Embedded Systems Security verletzt wurde und dadurch der Zugriff auf die Informationen nicht mehr möglich ist.

Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des Computers führen.

Objekte im Backup anzeigen

Die Objekte im Backup-Ordner können nur über die Programmkonsole im Knoten **Backup** angezeigt werden. Sie können die Dateien nicht mit den Dateimanagern von Microsoft Windows anzeigen.

► *Um Objekte im Backup anzuzeigen,*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Backup** aus.

Die Informationen über die im Backup befindlichen Objekte werden im Ergebnisbereich des ausgewählten Knotens angezeigt.

► *Um ein bestimmtes Objekt in der Liste der Backup-Objekte zu finden,*

sortieren Sie die Objekte oder verwenden Sie einen Filter.

In diesem Abschnitt

Dateien im Backup sortieren

Standardmäßig werden die Dateien im Backup nach ihrem Speicherdatum in umgekehrter chronologischer Reihenfolge sortiert. Um eine bestimmte Datei zu suchen, können Sie die Dateien nach dem Inhalt einer beliebigen Spalte im Ergebnisfenster sortieren.

Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen und erneut öffnen, oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und sie erneut aus dieser Datei öffnen.

► *Um die Dateien im Backup zu sortieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Backup** aus.
3. Wählen Sie In der Dateiliste im **Backup** den Titel der Spalte aus, nach deren Inhalt Sie die Objekte sortieren möchten.

Die im Backup befindlichen Dateien werden nach dem ausgewählten Kriterium sortiert.

Dateien im Backup filtern

Um ein bestimmtes Objekt im Backup zu suchen, können Sie die Dateien filtern, das heißt, im Knoten **Backup** nur Dateien anzeigen, die den von Ihnen definierten Filterbedingungen (Filtern) entsprechen.

Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und sie wieder aus dieser Datei öffnen.

► *Um die Dateien im Backup zu filtern, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Knoten **Backup** und wählen Sie den Punkt **Filter** aus.

   Das Fenster **Filtereinstellungen** wird geöffnet.
2. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie in der Liste **Feldname** ein Feld aus, mit dessen Wert der von Ihnen angegebene Filterwert verglichen werden soll.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterbedingungen in der Liste können unterschiedlich sein, je nachdem, welchen Wert Sie im Feld **Feldname** gewählt haben.
   c. Geben Sie im Feld **Feldwert** einen Wert für den Filter an oder wählen Sie ihn aus.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt. Wiederholen Sie diese Schritte für alle Filter, die Sie hinzufügen. Beachten Sie beim Arbeiten mit Filtern die folgenden Anweisungen:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.
   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.
   - Um einen Filter zu entfernen, markieren Sie ihn in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.
   - Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Fensters **Filtereinstellungen**, ändern Sie die entsprechenden Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

   Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**. In der Liste werden nur die Dateien angezeigt, die den von Ihnen definierten Filtern entsprechen.

► *Damit wieder alle Dateien in der Liste der Backup-Dateien angezeigt werden,*

wählen Sie im Kontextmenü des Knotens **Backup** den Punkt **Filter entfernen** aus.

Dateien aus Backup wiederherstellen

Kaspersky Embedded Systems Security speichert Dateien im Backup im verschlüsselten Format, damit der geschützte Computer vor schädlichen Wirkungen bewahrt wird.

Sie können Dateien aus dem Backup wiederherstellen.

In den folgenden Fällen müssen Sie möglicherweise eine Datei wiederherstellen:

- Wenn die Ursprungsdatei, die sich als infiziert herausgestellt hat, wichtige Informationen enthalten hat und Kaspersky Embedded Systems Security bei der Reparatur dieser Datei deren Integrität nicht retten konnte und auf die Informationen deshalb nicht mehr zugegriffen werden kann
- Wenn Sie die Datei für den Computer als sicher einschätzen und sie benutzen möchten. Damit Kaspersky Embedded Systems Security diese Datei bei künftigen Untersuchungen nicht als infiziert oder möglicherweise infiziert einstuft, können Sie sie von der Untersuchung in der Aufgabe zum Echtzeitschutz für Dateien und in den Aufgaben zur Untersuchung auf Befehl ausschließen. Geben Sie dazu die Datei als Einstellung **Dateien ausschließen** oder als Einstellung **Nicht erkennen** für diese Aufgaben an.

  Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des Computers führen.

Beim Wiederherstellen einer Datei können Sie entscheiden, wo sie gespeichert werden soll: Am ursprünglichen Speicherplatz (Standard), in einen speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Computer oder in einen von benutzerdefinierten Ordner auf dem Computer, auf dem die Programmkonsole installiert ist, oder auf einem anderen Computer im Netzwerk.

Der **Wiederherstellungsordner** dient zum Speichern von wiederhergestellten Objekten auf dem geschützten Computer. Sie können für seine Untersuchung spezielle Sicherheitsparameter festlegen. Der Pfad dieses Ordners wird durch die Backup-Einstellungen angegeben (siehe Abschnitt "Anpassen der Backup-Einstellungen" auf Seite 211).

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.

► *Um Dateien aus dem Backup wiederherzustellen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Backup** aus.
3. 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 in der Liste die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der markierten Objekte, und wählen Sie den Punkt **Wiederherstellen** aus.

   Das Fenster **Objektwiederherstellung** wird geöffnet.
4. Geben Sie im Fenster **Objektwiederherstellung** 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.

5. Führen Sie eine der Aktionen durch:

   - Um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im Ursprungsordner wiederherstellen**.
   - Um ein Objekt in einem Ordner wiederherzustellen, den Sie in den Quarantäneeinstellungen als Ordner für wiederhergestellte Objekte angegeben haben, wählen Sie **Im Standard-Ordner wiederherstellen** aus.
   - Um ein Objekt in einem anderen Ordner auf dem Computer, auf dem die Programmkonsole installiert ist, oder in einem freigegebenen Ordner zu speichern, wählen Sie **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** aus und wählen Sie dann den gewünschten Ordner aus oder geben dessen Pfad ein.

6. 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 löschen** (standardmäßig deaktiviert).

7. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

   Alle ausgewählten Objekte werden am vorgegebenen Speicherort wiederhergestellt und gespeichert: Bei Auswahl der Variante **Im Ursprungsordner wiederherstellen** wird jedes Objekt an seinem ursprünglichen Speicherort gespeichert. Bei Auswahl der Variante **Im Standard-Ordner wiederherstellen** oder **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** werden alle Objekte im angegebenen Ordner gespeichert.

8. Klicken Sie auf **OK**.

   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 wiederhergestellte Objekt anstelle des vorhandenen Objektes zu speichern
      - **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie einen neuen Dateinamen für das Objekt und den vollständigen Pfad ein.
      - **Umbenennen und Suffix hinzufügen**, um das Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie im Eingabefeld das Suffix ein.

   b. Wenn Sie mehrere Dateien für die Wiederherstellung markiert haben und die gewählte Aktion **Ersetzen** oder **Umbenennen** angewendet und ein Suffix auf die übrigen markierten Objekte hinzugefügt werden soll, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**. (Wenn Sie den Wert **Umbenennen** eingestellt haben, steht das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden** nicht zur Verfügung.)

   c. Klicken Sie auf **OK**.

   Das Objekt wird wiederhergestellt. Informationen über den Wiederherstellungsvorgang werden im Systemaudit-Protokoll protokolliert.

Wenn Sie im Fenster **Objektwiederherstellung** nicht die Variante **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, öffnet sich das Fenster **Objektwiederherstellung** noch einmal. Sie können dort den Speicherort angeben, an dem das folgende ausgewählte Objekt wiederhergestellt werden soll (s. Schritt 4 dieser Anleitung).

Dateien aus Backup löschen

► *Um eine oder mehrere Dateien aus dem Backup zu entfernen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Backup** aus.
3. Führen Sie eine der Aktionen durch:
   - Wählen Sie zum Entfernen eines Objekts im Kontextmenü des Objektnamens den Punkt **Löschen** aus
   - Um mehrere Objekte zu löschen, markieren Sie die entsprechenden Objekte mithilfe der Taste **Strg** oder **Umschalt** die entsprechenden Objekte. Öffnen Sie anschließend das Kontextmenü für eines der gewählten Objekte und wählen Sie den Punkt **Löschen** aus.
4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um die Operation zu bestätigen.

Die ausgewählten Dateien werden aus dem Backup gelöscht.

Backup-Einstellungen anpassen

► *Um die Backup-Einstellungen anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Backup**.
3. Wählen Sie den Menüpunkt **Eigenschaften**.
4. Passen Sie im Fenster **Eigenschaften des Backups** die Backup-Einstellungen entsprechend an:

   Im Abschnitt **Backup-Einstellungen**:

   - **Backup-Ordner**

     Pfad zum Backup-Ordner im UNC-Format (Universal Naming Convention).

     Standardmäßig ist der folgende Pfad eingestellt: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Backup\.

   - **Maximale Größe des Backups (MB)**

     Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktion, die die Gesamtgröße der Objekte verfolgt, die sich im Backup-Ordner befinden. Bei einer Überschreitung des vorgegebenen Wertes (als Standard gelten 200 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 dieses Kontrollkästchen aktiviert ist, verfolgt Kaspersky Embedded Systems Security die Gesamtgröße der Objekte, die sich im Backup befinden.

     Wenn dieses Kontrollkästchen deaktiviert ist, verfolgt Kaspersky Embedded Systems Security die Gesamtgröße der Objekte im Backup nicht.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

- **Grenzwert für verfügbaren Speicherplatz (MB)**

  Das Kontrollkästchen aktiviert oder deaktiviert die Verfolgung der minimalen Größe des freien Speicherplatzes im Backup (als Standard gelten 50 MB). Ist die Größe des freien Speicherplatzes kleiner als die vorgegebene Größe, protokolliert Kaspersky Embedded Systems Security das Ereignis *Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* und benachrichtigt gemäß den Einstellungen für Benachrichtigungen 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 (MB)" ist aktiv, wenn das Kontrollkästchen "Maximale Größe des Backups (MB)" aktiviert ist.

  Das Kontrollkästchen ist in der Grundeinstellung 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.

Im Abschnitt **Einstellungen für die Wiederherstellung von Objekten**:

- **Ordner für die Wiederherstellung von Objekten**

  Pfad des Ordners, in den Objekte wiederhergestellt werden, im UNC-Format (Universal Naming Convention).

  Standardpfad: C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Restored\.

5. Klicken Sie auf **OK**.

Die vorgenommenen Backup-Einstellungen werden gespeichert.

Backup-Statistik

In der Statistik für das Backup können Sie Informationen über den aktuellen Status des Backups erhalten.

► *Um eine Statistik für das Backup anzuzeigen,*

öffnen Sie in der Programmkonsolenstruktur das Kontextmenü für den Knoten **Backup** und wählen Sie den Befehl **Statistik**. Das Fenster **Backup-Statistik** wird geöffnet.

Im Fenster **Backup-Statistik** werden Informationen über den aktuellen Status des Backups angezeigt (s. Tabelle unten).

Tabelle 35. Informationen über den aktuellen Backup-Status

Feld	Beschreibung
Aktuelle Größe des Backups	Datenvolumen im Backup-Ordner. Die Größe bezieht sich auf die verschlüsselten Dateien.
Objekte insgesamt	Aktuelle Anzahl der Objekte im Backup

Ereignisregistrierung. Protokolle in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen über die Arbeit mit den Protokollen von Kaspersky Embedded Systems Security: Systemaudit-Protokoll, Protokolle der Aufgabenausführung und Ereignisprotokoll.

In diesem Kapitel

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 der Verarbeitung von Objekten in den Aufgaben von Kaspersky Embedded Systems Security
- Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security, beispielsweise Programmstart, Erstellen oder Löschen von Aufgaben, Aufgabenstart, Ändern der Aufgabeneinstellungen.

Kaspersky Embedded Systems Security verwendet die folgenden Methoden zum Protokollieren von Ereignissen:

- **Protokolle der Aufgabenausführung**. Ein Protokoll der Aufgabenausführung enthält Informationen über die aktuellen Aufgabenparameter, den aktuellen Aufgabenstatus und Ereignisse, die während der Aufgabenausführung eingetreten sind.
- **Systemaudit-Protokoll**. Das Systemaudit-Protokoll enthält Informationen über Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security.
- **Ereignisprotokoll**. Das Ereignisprotokoll enthält Informationen über Ereignisse, die für die Crash-Diagnose von Kaspersky Embedded Systems Security erforderlich sind. Das Ereignisprotokoll ist in der Ereignisanzeige von Microsoft Windows verfügbar.
- **Sicherheitsprotokoll**. Das Sicherheitsprotokoll enthält Informationen über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Computer verbunden sind.

Wenn bei der Ausführung von Kaspersky Embedded Systems Security ein Problem auftreten sollte (z. B. Kaspersky Embedded Systems Security oder eine bestimmte Aufgabe stürzen ab) und Sie das Problem diagnostizieren möchten, können Sie eine Protokolldatei und eine Dump-Datei für die Prozesse von Kaspersky Embedded Systems Security anlegen und diese Dateien zur Analyse an den Technischen Support von Kaspersky Lab schicken.

Kaspersky Embedded Systems Security versendet Protokoll- oder Dump-Dateien nicht automatisch. Nur ein Benutzer mit entsprechenden Rechten kann Diagnosedaten versenden.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsrechte konfigurieren (siehe Abschnitt "Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security" auf Seite 239) und nur bestimmten Benutzern Zugriff auf Protokolle, Protokoll- und Dump-Dateien gewähren.

Systemaudit-Protokoll

Kaspersky Embedded Systems Security führt für Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security ein Systemaudit durch. Das Programm sammelt beispielsweise Informationen über den Programmstart, den Start und die Beendigung von Aufgaben in Kaspersky Embedded Systems Security, die Änderung von Aufgabeneinstellungen oder das Erstellen und Löschen von Aufgaben zur Untersuchung auf Befehl. Einträge zu diesen Ereignissen werden im Detailbereich angezeigt, wenn Sie in der Programmkonsole den Knoten Systemaudit-Protokoll auswählen.

Standardmäßig speichert Kaspersky Embedded Systems Security die Ereignisse des Systemaudit-Protokolls für unbegrenzte Zeit. Sie können die Aufbewahrungsdauer der Einträge im Systemaudit-Protokoll anpassen.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Embedded Systems Security die Log-Dateien des Systemaudit-Protokolls speichert.

In diesem Abschnitt

Ereignisse im Systemaudit-Protokoll sortieren

Standardmäßig werden die Ereignisse im Systemaudit-Protokoll in umgekehrter chronologischer Reihenfolge dargestellt.

Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte außer der Spalte **Ereignis** sortieren.

► *Um Ereignisse im Systemaudit-Protokoll zu sortieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Systemaudit-Protokoll**.
3. Klicken Sie im Ergebnisbereich auf den Titel der Spalte, nach deren Inhalt die Ereignisse in der Ereignisliste sortiert werden sollen.

Die Ergebnisse der Sortierung bleiben bis zur nächsten Anzeige des Systemaudit-Protokolls erhalten.

Ereignisse im Systemaudit-Protokoll filtern

Sie können im Systemaudit-Protokoll nur die Einträge jener Ereignisse anzeigen, die Ihren Filterkriterien (Filtern) entsprechen.

► *Um Ereignisse im Systemaudit-Protokoll zu filtern, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Systemaudit-Protokoll** und wählen Sie den Punkt **Filter**.

   Das Fenster **Filtereinstellungen** wird geöffnet.
3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie aus der Liste **Feldname** die Spalte, nach der die Filterung erfolgen soll.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.
   c. Wählen Sie in der Liste **Feldwert** den Filterwert.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.
4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:
   - Wenn Sie mehrere Filter durch logisches "UND" verknüpfen möchten, wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind**.
   - Wenn Sie mehrere Filter durch logisches "ODER" verknüpfen möchten, wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist**.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Filterkriterien für Ereignisse im Systemaudit-Protokoll zu speichern.

   In der Ereignisliste des Systemaudit-Protokolls werden nur Ereignisse angezeigt, die den Filterkriterien entsprechen. Die Filterergebnisse bleiben bis zur nächsten Anzeige des Systemaudit-Protokolls erhalten.

► *Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Systemaudit-Protokoll** und wählen Sie den Punkt **Filter entfernen**.

   In der Ereignisliste des Systemaudit-Protokolls werden alle Ereignisse angezeigt.

Ereignisse aus dem Systemaudit-Protokoll löschen

Standardmäßig speichert Kaspersky Embedded Systems Security die Ereignisse des Systemaudit-Protokolls für unbegrenzte Zeit. Sie können die Aufbewahrungsdauer der Einträge im Systemaudit-Protokoll anpassen.

Sie können manuell alle Ereignisse aus dem Systemaudit-Protokoll entfernen.

► *Um Ereignisse aus dem Systemaudit-Protokoll zu entfernen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des Knotens **Systemaudit-Protokoll** und wählen Sie den Punkt **Leeren**.
3. Führen Sie eine der Aktionen durch:
   - Wenn Sie den Inhalt des Systemaudit-Protokolls vor dem Löschen der Ereignisse aus dem Protokoll in einer csv-Datei oder txt-Datei speichern möchten, klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Ja**. Geben Sie im folgenden Fenster den Namen und den Speicherort der Datei an.
   - Wenn Sie den Inhalt des Protokolls nicht in einer Datei speichern möchten, klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Nein**.

Der Systemaudit-Protokoll wird gelöscht.

Protokolle der Aufgabenausführung

Dieser Abschnitt enthält Informationen zu den Protokollen der Aufgabenausführung in Kaspersky Embedded Systems Security sowie Anweisungen für deren Ausführung.

In diesem Abschnitt

Über Protokolle der Aufgabenausführung

Informationen über die Ausführung von Aufgaben in Kaspersky Embedded Systems Security werden im Ergebnisbereich angezeigt, wenn in der Programmkonsole der Knoten **Protokolle der Aufgabenausführung** ausgewählt ist.

Im Protokoll der Aufgabenausführung können Sie eine Statistik über die Aufgabenausführung, Informationen für alle Objekte, die seit den Start dem Aufgabenstart bis zum aktuellen Zeitpunkt vom Programm verarbeitet wurden sowie die Aufgabeneinstellungen anzeigen.

Standardmäßig werden Einträge in den Protokollen der Aufgabenausführung von Kaspersky Embedded Systems Security 30 Tage lang ab der Beendigung der Aufgabe aufbewahrt. Sie können die Aufbewahrungsdauer der Einträge in den Protokollen der Aufgabenausführung ändern.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Embedded Systems Security die Dateien der Protokolle der Aufgabenausführung speichert. Ferner können Sie die Ereignisse auswählen, über die Kaspersky Embedded Systems Security Einträge in den Protokollen der Aufgabenausführung speichert.

Ereignisliste in den Protokollen der Aufgabenausführung anzeigen

► *Um in den Protokollen der Aufgabenausführung eine Ereignisliste anzuzeigen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.

Die Ereignisliste, die in den Protokollen der Aufgabenausführung in Kaspersky Embedded Systems Security gespeichert ist, wird im Ergebnisbereich angezeigt.

Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte sortieren oder einen Filter anwenden.

Ereignisliste in den Protokollen der Aufgabenausführung sortieren

Standardmäßig werden die Ereignisse in den Protokollen der Aufgabenausführung in umgekehrter chronologischer Reihenfolge dargestellt. Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte sortieren.

► *Um die Ereignisse in den Protokollen der Aufgabenausführung zu sortieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Klicken Sie im Ergebnisbereich auf den Titel der Spalte, nach deren Inhalt die Ereignisse in den Protokollen der Aufgabenausführung in Kaspersky Embedded Systems Security sortiert werden sollen.

Die Ergebnisse der Sortierung bleiben bis zur nächsten Anzeige der Protokolle der Aufgabenausführung erhalten.

Ereignisliste in den Protokollen der Aufgabenausführung filtern

Sie können in der Ereignisliste der Protokolle der Aufgabenausführung nur die Einträge jener Ereignisse anzeigen, die Ihren Filterkriterien (Filtern) entsprechen.

► *Um die Ereignisse in den Protokollen der Aufgabenausführung zu filtern, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des Knotens **Protokolle der Aufgabenausführung** und wählen Sie den Punkt **Filter**.

   Das Fenster **Filtereinstellungen** wird geöffnet.
3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie aus der Liste **Feldname** die Spalte, nach der die Filterung erfolgen soll.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.
   c. Wählen Sie in der Liste **Feldwert** den Filterwert.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.
4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:
   - Wenn Sie mehrere Filter durch logisches "UND" verknüpfen möchten, wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind**.
   - Wenn Sie mehrere Filter durch logisches "ODER" verknüpfen möchten, wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist**.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Filterkriterien für Ereignisse in den Protokollen der Aufgabeausführung zu speichern.

In der Ereignisliste der Protokolle der Aufgabenausführung werden nur Ereignisse angezeigt, die den Filterkriterien entsprechen. Die Filterergebnisse der Sortierung bleiben bis zur nächsten Anzeige der Protokolle der Aufgabenausführung erhalten.

► *Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des Knotens **Protokolle der Aufgabenausführung** und wählen Sie den Punkt **Filter entfernen**.

In der Ereignisliste der Protokolle der Aufgabenausführung werden alle Ereignisse angezeigt.

Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in den Protokollen der Aufgabenausführung anzeigen

In den Protokollen der Aufgabenausführung können Sie detaillierte Informationen über alle Ereignisse, die in den Aufgaben seit ihrem Start bis zum aktuellen Zeitpunkt 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 Protokollen der Aufgabenausführung anzuzeigen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Öffnen Sie im Ergebnisfenster das Fenster **Protokolle** auf eine der folgenden Arten:
   - Doppelklicken Sie auf ein Ereignis, das in der Aufgabe aufgetreten ist, deren Protokoll Sie anzeigen möchten.
   - Öffnen Sie das Kontextmenü für das Ereignis, das in der Aufgabe aufgetreten ist, deren Protokoll Sie anzeigen möchten, und wählen Sie den Punkt **Protokoll anzeigen**.
4. Im folgenden Fenster werden folgende Informationen angezeigt:
   - Auf der Registerkarte **Statistik** werden Startzeit und Zeitpunkt der Beendigung der Aufgabe sowie deren Statistik angezeigt.
   - Auf der Registerkarte **Ereignisse** wird eine Liste der Ereignisse angezeigt, die bei der Ausführung der Aufgabe aufgetreten sind.
   - Auf der Registerkarte **Einstellungen** werden die Aufgabeneinstellungen angezeigt.
5. Klicken Sie erforderlichenfalls auf die Schaltfläche **Filter**, um die Ereignisse im Protokoll der Aufgabenausführung zu filtern.
6. Klicken Sie erforderlichenfalls auf die Schaltfläche **Export**, um Informationen aus dem Protokoll der Aufgabenausführung in eine csv-Datei oder eine txt-Datei zu exportieren.
7. Klicken Sie auf **Schließen**.

Das Fenster **Protokolle** wird geschlossen.

Informationen aus einem Protokoll der Aufgabenausführung exportieren

Sie können Informationen aus dem Protokoll der Aufgabenausführung in eine csv-Datei oder in eine txt-Datei exportieren.

► *Um Informationen aus dem Protokoll der Aufgabenausführung zu exportieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Öffnen Sie im Ergebnisfenster das Fenster **Protokolle** auf eine der folgenden Arten:
   - Doppelklicken Sie auf ein Ereignis, das in der Aufgabe aufgetreten ist, deren Protokoll Sie anzeigen möchten.
   - Öffnen Sie das Kontextmenü für das Ereignis, das in der Aufgabe aufgetreten ist, deren Protokoll Sie anzeigen möchten, und wählen Sie den Punkt **Protokoll anzeigen**.
4. Klicken Sie im unteren Bereich des Fensters **Protokolle** auf die Schaltfläche **Export**.

   Das Fenster **Speichern unter** wird angezeigt.

5. Geben Sie den Namen, den Speicherort, den Typ und die Codierung der Datei an, in die Sie die Information aus dem Protokoll der Aufgabenausführung exportieren möchten.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die vorgenommenen Einstellungen werden gespeichert.

Ereignisse aus den Protokollen der Aufgabenausführung löschen

Standardmäßig werden Einträge in den Protokollen der Aufgabenausführung von Kaspersky Embedded Systems Security 30 Tage lang ab der Beendigung der Aufgabe aufbewahrt. Sie können die Aufbewahrungsdauer der Einträge in den Protokollen der Aufgabenausführung ändern.

Sie können alle Ereignisse manuell aus den Protokollen der Ausführung der zum aktuellen Zeitpunkt abgeschlossenen Aufgaben entfernen.

Ereignisse aus Protokollen über Aufgaben, die zum aktuellen Zeitpunkt ausgeführt werden, sowie aus Protokollen, die von anderen Benutzern verwendet werden, können nicht entfernt werden.

► *Um die Ereignisse aus den Protokollen der Aufgabenausführung zu entfernen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Führen Sie eine der Aktionen durch:
   - Wenn Sie die Ereignisse aus allen Protokollen der Aufgabenausführung, die zum aktuellen Zeitpunkt abgeschlossen sind, entfernen möchten, öffnen Sie das Kontextmenü für den untergeordneten Knoten **Protokolle der Aufgabenausführung** und wählen Sie den Punkt **Leeren**.
   - Wenn Sie das Protokoll über die Ausführung einer einzelnen Aufgabe löschen möchten, öffnen Sie im Ergebnisbereich das Kontextmenü für das Ereignis, das in der Aufgabe aufgetreten ist, dessen Protokoll der Aufgabenausführung Sie löschen möchten, und wählen Sie den Punkt **Löschen**.
   - Um Protokolle über die Ausführung mehrerer Aufgaben zu löschen, gehen Sie wie folgt vor:
     a. Wählen Sie im Ergebnisbereich mithilfe der Tasten **Strg** oder **Umschalt** die Ereignisse aus, die in den Aufgaben aufgetreten sind, deren Ausführungsprotokolle Sie leeren möchten.
     b. Öffnen Sie das Kontextmenü eines beliebigen ausgewählten Ereignisses und wählen Sie den Punkt **Löschen**.
4. Klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Ja**, um das Löschen zu bestätigen.

Die ausgewählten Protokolle der Aufgabenausführung werden gelöscht. Das Löschen von Ereignissen aus den Protokollen der Aufgabenausführung wird im Systemaudit-Protokoll protokolliert.

Sicherheitsprotokoll

Kaspersky Embedded Systems Security führt ein Sicherheits-Ereignisprotokoll über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Computer verbunden sind. In diesem Protokoll werden folgende Ereignisse registriert:

- Ereignisse der Komponente "Exploit-Prävention".
- Kritische Ereignisse der Komponente "Protokollanalyse"
- Kritische Ereignisse, die auf eine versuchte Verletzung der Sicherheit hindeuten (für die Aufgaben "Echtzeit-Computerschutz", "Untersuchung auf Befehl", "Überwachung der Datei-Integrität", "Kontrolle des Programmstarts" und "Gerätekontrolle").

Sie können das Sicherheitsprotokoll wie auch das Systemaudit-Protokoll leeren (siehe Abschnitt "Ereignisse aus dem Systemaudit-Protokoll löschen" auf Seite 216). Dabei registriert Kaspersky Embedded Systems Security ein Ereignis des Systemaudits über das Leeren des Sicherheitsprotokolls.

Ereignisprotokoll von Kaspersky Embedded Systems Security in der Ereignisanzeige anzeigen

Mithilfe des Snap-ins "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 Protokoll registriert werden (informative, wichtige oder kritische Ereignisse). Am ausführlichsten ist die Stufe "Informative Ereignisse", bei der Ereignisse aller Ereigniskategorien aufgezeichnet werden. Dagegen werden auf der relativ oberflächlichen Stufe "Kritische Ereignisse" nur kritische Ereignisse registriert. In der Grundeinstellung gilt für alle Komponente außer für die Update-Komponente die Genauigkeitsstufe "Wichtige Ereignisse" (es werden nur wichtige und kritische Ereignisse registriert). Für die Update-Komponente gilt die Stufe "Informative Ereignisse".

► *Um das Ereignisprotokoll für Kaspersky Embedded Systems Security anzuzeigen, gehen Sie wie folgt vor:*

1. Klicken Sie auf die Schaltfläche **Start**, geben Sie in der Suchzeile den Befehl `mmc` ein und klicken Sie auf die Taste **EINGABE**.

   Es öffnet sich das Fenster Microsoft Management Console.

2. Wählen Sie **Datei** > **Snap-in hinzufügen oder löschen**.

   Das Fenster **Snap-in hinzufügen und löschen** wird geöffnet.

3. Wählen Sie aus der Liste der verfügbaren Snap-ins das Snap-in **Ereignisanzeige** aus und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Computer auswählen** wird geöffnet.

4. Geben Sie im Fenster **Computer auswählen** den Computer an, auf dem Kaspersky Embedded Systems Security installiert ist, und klicken Sie auf die Schaltfläche **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 in der Konsolenstruktur den Knoten **Ereignisanzeige** und wählen Sie den untergeordneten Knoten **Anwendungs- und Dienstprotokolle** > **Kaspersky Embedded Systems Security** aus.

Das Ereignisprotokoll für Kaspersky Embedded Systems Security wird geöffnet.

Protokolleinstellungen in der Konsole für Kaspersky Embedded Systems Security anpassen

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 das Systemaudit-Protokoll speichert
- Grenzwerte für Ereignisdarstellung von *Programm-Datenbanken sind veraltet*, *Programm-Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt*
- Ereignisse, die Kaspersky Embedded Systems Security in den Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisprotokoll von Kaspersky Embedded Systems Security in der Ereignisanzeige speichert.
- Einstellungen der Veröffentlichung der Audit-Ereignisse und der Ereignisse bei der Aufgabenausführung auf dem syslog-Server über das syslog-Protokoll

► *Um die Protokolle für Kaspersky Embedded Systems Security anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Knoten **Protokolle und Benachrichtigungen** und wählen Sie den Punkt **Eigenschaften** aus.

   Das Fenster **Einstellungen für Protokolle und Benachrichtigungen** wird geöffnet.
2. Passen Sie im Fenster **Einstellungen für Berichte und Benachrichtigungen** die Einstellungen für Protokolle nach Bedarf an. Gehen Sie hierzu wie folgt vor:
   - Wählen Sie auf der Registerkarte **Allgemein** erforderlichenfalls jene Ereignisse aus, die Kaspersky Embedded Systems Security in den Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisprotokoll von Kaspersky Embedded Systems Security in der Ereignisanzeige speichern soll. Gehen Sie hierzu wie folgt vor:
     - Wählen Sie in der Liste **Komponente** die Komponente von Kaspersky Embedded Systems Security, deren Genauigkeitsstufe für Ereignisse Sie festlegen möchten.

Für die Komponenten "Echtzeitschutz für Dateien", "Untersuchung auf Befehl" und "Update" ist eine Aufzeichnung von Ereignissen in den Protokollen der Aufgabenausführung und im Ereignisprotokoll vorgesehen. Für diese Komponenten enthält die Ereignisliste die Spalten **Protokoll der Aufgabenausführung** und **Windows-Ereignisprotokoll**. Für die Komponenten Quarantäne und Backup werden die Ereignisse im Systemaudit-Protokoll und im Ereignisprotokoll protokolliert. Für diese Komponenten enthält die Ereignisliste die Spalten **Systemaudit** und **Windows-Ereignisprotokoll**.

- Wählen Sie in der Liste **Prioritätsstufe** die Genauigkeitsstufe der Ereignisse in den Protokollen der Aufgabenausführung und im Systemaudit-Protokoll für die ausgewählte Funktionskomponente.

  In der unten stehenden Tabelle der Ereignisliste sind die Kontrollkästchen neben jenen Ereignissen aktiviert, die in den Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisprotokoll gemäß der ausgewählten Genauigkeitsstufe protokolliert werden.

- Wenn Sie den Eintrag einzelner Ereignisse für die ausgewählte Funktionskomponente manuell aktivieren möchten, gehen Sie wie folgt vor:

a. Wählen Sie in der Liste **Prioritätsstufe** die Option **Benutzerdefiniert** aus.

b. Aktivieren Sie in der Tabelle Ereignisliste die Kontrollkästchen neben jenen Ereignissen, für die Sie den Eintrag in das Protokoll der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisprotokoll aktivieren möchten.

- Passen Sie auf der Registerkarte **Erweitert** die Einstellungen der Speicherung von Protokollen und die Grenzwerte für Ereignisdarstellung über den Schutzstatus des Computers an:
  - Im Abschnitt **Protokoll speichern**:
    - **Ordner für Protokolle**

      Pfad zum Ordner mit Protokollen im UNC-Format (Universal Naming Convention).

      Standardpfad: C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports\.

      Wenn sich der Standardpfad ändert, wird ein Ordner mit dem entsprechenden Namen erstellt. Die neuen Protokolle werden in dem neuen Ordner gespeichert. Die alten Protokolle bleiben erhalten.

    - **Protokolle der Aufgabenausführung löschen, die älter sind als (Tage)**

      Das Kontrollkästchen aktiviert/deaktiviert die Funktion, die Protokolle über die Ergebnisse beendeter Aufgaben und Ereignisse sowie die in den Protokollen veröffentlichten ausgeführten Aufgaben nach Ablauf der vorgegebenen Frist (als Standard gelten 30 Tage) löscht.

      Wenn dieses Kontrollkästchen aktiviert ist, löscht Kaspersky Embedded Systems Security nach Ablauf der vorgegebenen Frist die Protokolle über die Ergebnisse beendeter Aufgaben und Ereignisse sowie die in den Protokollen veröffentlichten ausgeführten Aufgaben.

      Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Ereignisse aus dem Systemaudit-Protokoll löschen, die älter sind als (Tage)**

  Das Kontrollkästchen aktiviert/deaktiviert die Funktion, die im Systemaudit-Protokoll eingetragene Ereignisse nach Ablauf der vorgegebenen Frist (als Standard gelten 60 Tage) löscht.

  Wenn dieses Kontrollkästchen aktiviert ist, löscht Kaspersky Embedded Systems Security nach Ablauf der vorgegebenen Frist die im Systemaudit-Protokoll eingetragenen Ereignisse.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

- Im Abschnitt **Grenzwerte für Ereigniserstellung**:
  - Anzahl der Tage, nach deren Ablauf die Ereignisse *Programm-Datenbanken sind veraltet*, *Programm-Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt* eintreten sollen

Tabelle 36. Grenzwerte für Ereignisdarstellung

Einstellung	Grenzwerte für Ereignisdarstellung
Beschreibung	Sie können Grenzwerte für die Ereignisauslösung folgender Ereignisse einstellen: *Programm-Datenbanken sind veraltet* und *Programm-Datenbanken sind stark veraltet*. Dieses Ereignis tritt auf, wenn die Datenbanken von Kaspersky Embedded Systems Security nicht innerhalb der von der Einstellung vorgegebenen Anzahl von Tagen seit dem Veröffentlichungsdatum des letzten installierten Datenbanken-Update aktualisiert werden. Sie können eine Benachrichtigung für Administrator einstellen, wenn das Ereignis entsteht. *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt*. Dieses Ereignis tritt ein, wenn innerhalb einer angegebenen Anzahl an Tagen keine der mit dem Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten** markierten Aufgaben ausgeführt wurde.
Mögliche Werte	Anzahl der Tage von 1 bis 365.
Standardwert	Die Programm-Datenbanken sind veraltet – 7 Tage. Die Programm-Datenbanken sind stark veraltet – 14 Tage. Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt – 30 Tage.

- Passen Sie auf der Registerkarte **SIEM-Integration** die Einstellungen der Veröffentlichung von Audit-Ereignissen und Ereignissen bei der Aufgabenausführung auf dem syslog-Server an (siehe Abschnitt "Anpassen der Einstellungen der SIEM-Integration" auf Seite 225).

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

In diesem Abschnitt

Über die SIEM-Integration

Um die Belastung für leistungsschwache Geräte zu reduzieren und die Gefahr eines Abfalls der Systemleistung infolge eines zu großen Umfangs der Programmprotokolle zu verringern, können Sie die Veröffentlichung der Audit-Ereignisse und der Ereignisse der Aufgabenausführung über das Protokoll syslog auf dem *syslog-Server* einrichten.

Ein syslog-Server ist ein externer Server für Ereignis-Management (SIEM), der eingehende Ereignisse sammelt und analysiert sowie andere Aktionen im Rahmen der Protokollverwaltung ausführt.

Sie können die SIEM-Integration in zwei Modi verwenden:

- Ereignisse auf dem syslog-Server duplizieren: In diesem Modus wird davon ausgegangen, dass 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 lokalen Computer gespeichert werden.

  Es wird empfohlen, diesen Modus zu verwenden, um die Belastung für den geschützten Computer auf ein Minimum zu reduzieren.

- Lokale Kopien der Ereignisse löschen: In diesem Modus wird davon ausgegangen, dass alle Ereignisse, die während der Programmausführung registriert und in SIEM veröffentlicht wurden, vom lokalen Computer gelöscht werden.

  > 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 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-Systems zu orientieren.

Einstellungen für Zuverlässigkeit

Sie können das Risiko eines misslungenen Versands von Ereignissen an SIEM verringern, indem Sie die Verbindung zu einem syslog-Spiegelserver konfigurieren.

Der syslog-Spiegelserver ist ein zusätzlicher syslog-Server, zu dessen Verwendung das Programm automatisch übergeht, wenn keine Verbindung zum primären syslog-Server besteht oder wenn dieser nicht verwendet werden kann.

Kaspersky Embedded Systems Security benachrichtigt Sie mithilfe der Ereignisse des Systemaudits auch über misslungene Versuche der Verbindung zu SIEM und über Fehler beim Versand der Ereignisse an SIEM.

Anpassen der Einstellungen der SIEM-Integration

Standardmäßig wird die SIEM-Integration nicht verwendet. Sie können die SIEM-Integration aktivieren und deaktivieren und die entsprechenden Funktionen konfigurieren (s. Tabelle unten).

Tabelle 37. Einstellungen für die SIEM-Integration

Einstellung	Standardwert	Beschreibung
Ereignisse über das syslog-Protokoll an den externen syslog-Server senden	Wird nicht verwendet	Sie können die SIEM-Integration mithilfe dieses Kontrollkästchens aktivieren und deaktivieren.
Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen	Wird nicht verwendet	Sie können die Speicherung lokaler Kopien der Protokolle nach ihrem Versand an SIEM mithilfe dieses Kontrollkästchens konfigurieren.
Format der Ereignisse	Strukturierte Daten	Sie können eines von zwei Formaten wählen, in die das Programm die Ereignisse vor ihrem Versand an den syslog-Server konvertiert, damit sie von SIEM erfolgreich identifiziert werden können.
Verbindungsprotokoll	TCP	Sie können mithilfe der Dropdown-Liste die Verbindung mit dem primären und dem zusätzlichen syslog-Server über die Protokolle UPD oder TCP anpassen.
Einstellungen der Verbindung mit dem primären syslog-Server	IP-Adresse: 127.0.0.1 Port: 514	Sie können in den entsprechenden Feldern die Werte für IP-Adresse und Port angeben, um die Verbindung mit dem primären syslog-Server anzupassen. Der Wert der IP-Adresse darf nur im Format IPv4 angegeben werden.
Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist	Wird nicht verwendet	Sie können mithilfe dieses Kontrollkästchens die Verwendung eines syslog-Spiegelservers aktivieren und deaktivieren.
Einstellungen der Verbindung mit dem zusätzlichen syslog-Server	IP-Adresse: 127.0.0.1 Port: 514	Sie können in den entsprechenden Feldern die Werte für IP-Adresse und Port angeben, um die Verbindung mit dem gespiegelten syslog-Server anzupassen. Der Wert der IP-Adresse darf nur im Format IPv4 angegeben werden.

► *Um die Einstellungen der SIEM-Integration zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Benachrichtigungen**.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Einstellungen für Berichte und Benachrichtigungen** wird geöffnet.
3. Wählen Sie die Registerkarte **SIEM-Integration** aus.

4. Aktivieren Sie im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Ereignisse über das syslog-Protokoll an den externen syslog-Server senden**.

   Das Kontrollkästchen aktiviert/deaktiviert die Verwendung der Funktion zum Versand der zu veröffentlichenden Ereignisse an den externen syslog-Server.

   Wenn das Kontrollkästchen aktiviert ist, sendet das Programm die zu veröffentlichenden Ereignisse an SIEM gemäß der Konfiguration der SIEM-Integration.

   Wenn das Kontrollkästchen deaktiviert ist, nimmt das Programm keine SIEM-Integration vor. Sie können die Einstellungen der SIEM-Integration nicht anpassen, wenn das Kontrollkästchen deaktiviert ist.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

5. Aktivieren Sie bei Bedarf im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen**.

   Das Kontrollkästchen aktiviert/deaktiviert das Löschen der lokalen Kopien der Protokolle nach ihrem Versand an SIEM.

   Wenn das Kontrollkästchen aktiviert ist, löscht das Programm die lokalen Kopien der Ereignisse, sobald sie erfolgreich in SIEM veröffentlicht wurden. Es wird empfohlen, diesen Modus auf leistungsschwachen Computern zu verwenden.

   Wenn das Kontrollkästchen deaktiviert ist, sendet das Programm lediglich die Ereignisse an SIEM. Die Kopien der Protokolle werden weiterhin lokal gespeichert.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

> Der Status des Kontrollkästchens **Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen** beeinflusst nicht die Einstellungen zum Speichern der Ereignisse des Sicherheitsprotokolls: Das Programm löscht niemals automatisch die Ereignisse des Sicherheitsprotokolls.

6. Geben Sie im Abschnitt **Format der Ereignisse** das Format an, in das Sie die Ereignisse bei der Programmausführung für den Versand an SIEM konvertieren möchten.

   Standardmäßig konvertiert das Programm die Ereignisse in ein Format für strukturierte Daten.

7. Gehen Sie im Abschnitt **Verbindungseinstellungen** wie folgt vor:

   - Geben Sie das Protokoll für die Verbindung zu SIEM an.
   - Geben Sie die Einstellungen der Verbindung mit dem primären syslog-Server an.

     Die IP-Adresse darf nur im Format IPv4 angegeben werden.

   - Aktivieren Sie das Kontrollkästchen **Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist**, wenn Sie möchten, dass das Programm andere Verbindungseinstellungen verwendet, wenn der Versand der Ereignisse an den primären syslog-Server nicht verfügbar ist.
     - Geben Sie die folgenden Einstellungen für die Verbindung mit dem zusätzlichen syslog-Server an: **IP-Adresse** und **Port**.

       Die Felder **IP-Adresse** und **Port** des syslog-Spiegelservers können nicht bearbeitet werden, wenn das Kontrollkästchen **Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist** deaktiviert ist.

       Die IP-Adresse darf nur im Format IPv4 angegeben werden.

8. Klicken Sie auf **OK**.

   Die angepassten Einstellungen der SIEM-Integration werden übernommen.

Benachrichtigungseinstellungen

Dieser Abschnitt enthält Informationen über Möglichkeiten zur Benachrichtigung von Benutzern und Administratoren von Kaspersky Embedded Systems Security über Programmereignisse und den Schutzstatus des Computers sowie Anleitungen zur Anpassung von Benachrichtigungen.

In diesem Kapitel

Methoden zur Benachrichtigung von Administrator und Benutzer

Sie können die Benachrichtigung des Administrators und der Benutzer, die auf den geschützten Computer zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Embedded Systems Security und dem Status des Antiviren-Schutzes auf dem Computer zusammenhängen, anpassen.

Das Programm gewährleistet die Ausführung folgender Aufgaben:

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerks, die auf den geschützten Computer zugreifen, sowie die Benutzer des Terminalcomputers können Informationen über Ereignisse des Typs *Objekt gefunden* erhalten, die in der Aufgabe Echtzeitschutz für Dateien auftreten.

In der Programmkonsole können Sie die Benachrichtigungen für den Administrator oder die Benutzer auf unterschiedliche Weise aktivieren:

- Methoden für die Benachrichtigung der Benutzer:
  a. Werkzeuge für Terminaldienst.

     Sie können diese Methode für die Benachrichtigung von Benutzern des Terminalcomputers anwenden, wenn der geschützte Computer als Terminal verwendet wird.

  b. Werkzeuge für den Windows Messenger Dienst.

     Sie können diese Methode für die Benachrichtigung über den Windows Messenger Dienst anwenden.
- Methoden für Benachrichtigung von Administratoren:
  a. Werkzeuge für den Windows Messenger Dienst.

     Sie können diese Methode für die Benachrichtigung über den Windows Messenger Dienst anwenden.

  b. Starten einer ausführbaren Datei.

     Diese Methode wird aufgrund des Ereignisses ausführbare Datei gestartet, die auf der lokalen Festplatte des geschützten Computers gespeichert ist.

  c. Per E-Mail senden.

     Diese Methode dient der Zustellung von Nachrichten per E-Mail-Nachricht.

Sie können einen Nachrichtentext für die einzelnen Ereignistypen festlegen. In den Text können Sie Felder mit Informationen zum Ereignis aufnehmen. Standardmäßig wird für die Benachrichtigung von Benutzern ein bereits vorgegebener 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.

► *Um die Benachrichtigungen über Ereignisse zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Knoten **Protokolle und Benachrichtigungen** und wählen Sie den Punkt **Eigenschaften** aus.

   Das Fenster **Einstellungen für Berichte und Benachrichtigungen** wird geöffnet.

2. Geben Sie auf der Registerkarte **Benachrichtigungen** den Modus der Benachrichtigungen an:

   a. Wählen Sie in der Liste **Ereignistyp** das Ereignis aus, für das Sie eine Benachrichtigungsmethode festlegen möchten.

   b. Aktivieren Sie in der Parametergruppe **Benachrichtigung für die Administratoren** oder **Benachrichtigung für die Benutzer** das Kontrollkästchen für die Benachrichtigungsarten, die Sie verwenden möchten.

   > Sie können Benutzerbenachrichtigungen nur für das Ereignis **Objekt gefunden**, das Ereignis **Nicht vertrauenswürdiger Massenspeicher gefunden und eingeschränkt** und das Ereignis **Computer wurde der Liste der nicht vertrauenswürdigen Computer hinzugefügt** anpassen.

3. Um einen Benachrichtigungstext zu erstellen, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Text der Nachricht**.

   b. Geben Sie im nächsten Fenster den Text ein, der in der Benachrichtigung über das Ereignis angezeigt werden soll.

   > So können Sie den gleichen Nachrichtentext für mehrere Ereignistypen festlegen: Wählen Sie zuerst die Benachrichtigungsmethode für einen Ereignistyp aus. Markieren Sie dann mithilfe der Tasten **Strg** oder **Umschalt** die übrigen Ereignistypen, für die Sie den gleichen Nachrichtentext festlegen möchten. Klicken Sie erst dann auf die Schaltfläche **Text der Nachricht**.

   c. Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Makros** 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.

   d. Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**.

4. Um die gewählten Benachrichtigungsarten für Administratoren anzupassen, wählen Sie die Registerkarte **Benachrichtigungen** aus, klicken Sie auf die Schaltfläche **Einstellungen** im Abschnitt **Benachrichtigung für die Administratoren** und passen Sie im Fenster **Erweiterte Einstellungen** die ausgewählten Einstellungen an. Gehen Sie hierzu wie folgt vor:

   a. Für Benachrichtigungen, die per E-Mail erfolgen sollen, öffnen Sie die Registerkarte **E-Mail** und tragen in die entsprechenden Felder die E-Mail-Adressen der Empfänger (durch Semikolon getrennt), den Namen oder die Netzwerkadresse des SMTP-Servers sowie dessen Port ein. Tragen Sie bei Bedarf den Text ein, der in den Feldern **Betreff** und **Von** angezeigt werden soll. In den Text des Feldes **Betreff** können auch Variable mit Informationen über Ereignisse aufgenommen werden (s. Tabelle unten).

Wenn Sie bei der Verbindung mit einem SMTP-Server die Authentifizierung für Benutzerkonten verwenden möchten, aktivieren Sie in der Gruppe **Einstellungen für die Authentifizierung** das Kontrollkästchen **SMTP-Authentifizierung verwenden** und tragen Sie Name und Kennwort des Benutzers ein, dessen Benutzerkonto geprüft werden soll.

b. Damit Benachrichtigung über den **Windows Messenger Dienst** erfolgen, erstellen Sie auf der Registerkarte **Windows Messenger Dienst** eine Liste der Computer, die Benachrichtigungen erhalten sollen: Klicken Sie für jeden Computer, den Sie hinzufügen möchten, auf **Hinzufügen** und tragen Sie im Eingabefeld den entsprechenden Netzwerknamen ein.

c. Wenn eine ausführbare Datei gestartet werden soll, wählen Sie auf der Registerkarte **Ausführbare Datei** eine Datei auf einem lokalen Laufwerk des geschützten Computers aus, die nach Eintreten des Ereignisses auf dem Computer ausgeführt werden soll, oder geben Sie den vollständigen Pfad der Datei an. 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.

   Wenn Sie die Anzahl der Benachrichtigungen, die für einen Ereignistyp innerhalb eines bestimmten Zeitraums gesendet werden sollen, begrenzen möchten, aktivieren Sie auf der Registerkarte **Erweitert** das Kontrollkästchen **Die gleiche Benachrichtigung senden höchstens** und legen Sie eine Anzahl und eine Zeiteinheit fest.

5. Klicken Sie auf **OK**.

Die festgelegten Benachrichtigungseinstellungen werden gespeichert.

Tabelle 38. 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 "Echtzeit-Computerschutz" und "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.
%VIRUS_NAME%	Name des gefundenen Objekts gemäß der Klassifizierung der Viren-Enzyklopädie https://encyclopedia.kaspersky.com/knowledge/classification/. Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Embedded Systems Security beim Fund eines Objekts zurückgibt. Sie können den vollständigen Namen des gefundenen Objekts im Protokoll der Aufgabenausführung aufrufen (siehe Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in Protokollen der Aufgabenausführung anzeigen" auf Seite 218).
%VIRUS_TYPE%	Typ des gefundenen Objekts gemäß der Klassifizierung von Kaspersky Lab, beispielsweise "Virus" oder "Trojaner". Gehört zur vollständigen Bezeichnung eines gefundenen Objekts, die Kaspersky Embedded Systems Security zurückgibt, nachdem ein Objekt als infiziert oder möglicherweise infiziert eingestuft wurde. Den vollständigen Namen des gefundenen Objekts finden Sie im Protokoll der Aufgabenausführung.

Variable	Beschreibung
%USER_COMPUTER%	In der Aufgabe "Echtzeitschutz für Dateien" ist das der Name des Computers, der auf das Objekt auf dem Computer zugegriffen hat.
%USER_NAME%	In den Aufgaben "Echtzeitschutz für Dateien" und "Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern" ist das der Name des Benutzers, der auf das Objekt auf dem Server zugegriffen hat.
%FROM_COMPUTER%	Name des geschützten Computers, von dem die Benachrichtigung geschickt wurde.
%EVENT_REASON%	Grund für Eintreten eines Ereignisses (Dieses Feld ist für bestimmte Ereignisse nicht verfügbar).
%ERROR_CODE%	Fehlercode (Wird nur das Ereignis "Interner Aufgabenfehler" verwendet).
%TASK_NAME%	Aufgabenname (nur für Ereignisse, die mit der Aufgabenausführung verbunden sind).

Starten und Beenden von Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zum Start der Programmkonsole sowie zum Start und zum Beenden von Kaspersky Security Service.

In diesem Kapitel

Plug-in für Kaspersky Embedded Systems Security starten

In Kaspersky Security Center sind für den Start des Plug-in für Kaspersky Embedded Systems Security keine weiteren Aktionen erforderlich. Nach der Installation des Plug-Ins auf dem Computer des Administrators wird dieses zusammen mit Kaspersky Security Center gestartet. Ausführliche Informationen über den Start von Kaspersky Security Center finden Sie im *Hilfesystem von Kaspersky Security Center*.

Start der Konsole für Kaspersky Embedded Systems Security aus dem Startmenü

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

► *So öffnen Sie die Programmkonsole über das **Startmenü**:*

1. Wählen Sie im **Startmenü Programme** > **Kaspersky Embedded Systems Security** > **Administrations-Tools** > **Konsole für Kaspersky Embedded Systems Security**.

Wenn Sie planen, andere Snap-ins zur Programmkonsole hinzuzufügen, starten Sie die Programmkonsole im Autorenmodus.

► *Gehen Sie wie folgt vor, um die Programmkonsole im Autorenmodus zu starten:*

1. Wählen Sie im **Startmenü Programme** > **Kaspersky Embedded Systems Security** > **Administrations-Tools** aus.
2. Wählen Sie im Kontextmenü der Programmkonsole den Befehl **Autor**.

Die Programmkonsole wird im Autorenmodus gestartet.

Wenn die Programmkonsole auf dem geschützten Computer gestartet wurde, wird das Fenster der Programmkonsole geöffnet.

Wenn Sie die Programmkonsole nicht auf dem geschützten, sondern auf einem anderen Computer gestartet haben, stellen Sie eine Verbindung mit dem geschützten Computer her.

► *Gehen Sie wie folgt vor, um eine Verbindung mit dem geschützten Computer herzustellen:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
2. Wählen Sie den Befehl **Verbindung mit anderem Computer herstellen** aus.

   Das Fenster **Computer auswählen** wird geöffnet.
3. Wählen Sie im folgenden Fenster **Anderer Computer** aus.
4. Geben Sie im Eingabefeld den Netzwerknamen des geschützten Computers ein.
5. Klicken Sie auf **OK**.

Die Programmkonsole wird mit einem geschützten Computer verbunden.

Wenn das Benutzerkonto, mit dem Sie sich bei Microsoft Windows angemeldet haben, nicht über die erforderlichen Rechte für den Zugriff auf den Dienst zur Verwaltung von Kaspersky Security Management Service auf dem Computer verfügt, aktiveren Sie das Kontrollkästchen **Verbindung mit Rechten des folgenden Benutzerkontos herstellen** und geben Sie ein anderes Benutzerkonto an, das über die entsprechenden Rechte verfügt.

Kaspersky Security Service starten und anhalten

Standardmäßig wird der Dienst von Kaspersky Security Service automatisch unmittelbar nach dem Hochfahren des Betriebssystems gestartet. Kaspersky Security Service verwaltet die Programmprozesse, bei denen die Aufgaben "Echtzeit-Computerschutz", "Computer-Kontrolle", "Schutz von Netzwerkspeichern", "Untersuchung auf Befehl" und "Update" ausgeführt werden.

Beim Start von Kaspersky Embedded Systems Security werden standardmäßig folgende Aufgaben gestartet: "Echtzeitschutz für Dateien", "Untersuchung beim Hochfahren des Betriebssystems" sowie andere Aufgaben, für deren Zeitplan die Startfrequenz **Bei Programmstart** gilt.

Wenn Sie den Dienst von Kaspersky Security Service beenden, werden alle laufenden Aufgaben beendet. Nachdem Sie Kaspersky Security Service neu gestartet haben, startet das Programm nur jene Aufgaben automatisch, bei denen im Zeitplan das Startintervall **Bei Programmstart** festgelegt ist; die anderen Aufgaben müssen manuell gestartet werden.

Sie können den Dienst Kaspersky Security Service über das Kontextmenü des Knotens **Kaspersky Embedded Systems Security** oder mithilfe des Snap-Ins Dienste von Microsoft Windows starten und beenden.

Sie können Kaspersky Embedded Systems Security starten und beenden, wenn Sie zur Gruppe "Administratoren" auf dem geschützten Computer gehören.

► *Um das Programm mithilfe der Programmkonsole zu beenden oder zu starten, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
2. Wählen Sie einen der folgenden Befehle:
   - **Dienst beenden**
   - **Dienst starten**

Der Dienst von Kaspersky Security Service wird gestartet oder beendet.

Start der Komponenten von Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems

Dieser Abschnitt enthält Informationen über die Ausführung von Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems.

In diesem Kapitel

Über die Ausführung von Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems

Die Komponenten von Kaspersky Embedded Systems Security können nach dem Laden des Betriebssystems im abgesicherten Modus gestartet werden. Neben dem Kaspersky Security Service (kavfs.exe) wird auch der Treiber "klam.sys" geladen, der beim Start des Betriebssystems zur Registrierung des Kaspersky Security Service als geschützter Dienst dient. Nähere Informationen finden Sie im Abschnitt Kaspersky Security Service als geschützten Dienst registrieren.

Kaspersky Embedded Systems Security kann in den folgenden abgesicherten Modi gestartet werden:

- Minimaler abgesicherter Modus – Dieser Modus wird gestartet, wenn die Standardoption für den abgesicherten Modus ausgewählt wird. Kaspersky Embedded Systems Security kann die folgenden Komponenten starten:
  - Echtzeitschutz für Dateien
  - Untersuchung auf Befehl
  - Kontrolle des Programmstarts und automatisches Erstellen von Regeln für die Kontrolle des Programmstarts
  - Protokollanalyse
  - Überwachung der Datei-Integrität
  - Integritätsprüfung für Programme
- Abgesicherter Modus mit Netzwerktreibern – Dieser Modus wird gestartet, wenn das Betriebssystem im abgesicherten Modus mit Netzwerktreibern geladen wird. Neben den im minimalen abgesicherten Modus startenden Komponenten kann Kaspersky Embedded Systems Security die folgenden Komponenten starten:
  - Update der Programm-Datenbanken
  - Update der Programm-Module

Starten von Kaspersky Embedded Systems Security im abgesicherten Modus

Standardmäßig wird Kaspersky Embedded Systems Security im abgesicherten Modus nicht gestartet.

► *Um Kaspersky Embedded Systems Security im abgesicherten Modus zu starten, gehen Sie wie folgt vor:*

1. Starten Sie den Windows-Registrierungs-Editor (C:\Windows\regedit.exe).
2. Öffnen Sie den Schlüssel [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] der Systemregistrierung.
3. Öffnen Sie den Parameter "LoadInSafeMode".
4. Stellen Sie den Wert auf `1` ein.
5. Klicken Sie auf **OK**.

► *Um den Start von Kaspersky Embedded Systems Security im abgesicherten Modus abzubrechen, gehen Sie wie folgt vor:*

1. Starten Sie den Windows-Registrierungs-Editor (C:\Windows\regedit.exe).
2. Öffnen Sie den Schlüssel [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] der Systemregistrierung.
3. Öffnen Sie den Parameter "LoadInSafeMode".
4. Stellen Sie den Wert auf `0` ein.
5. Klicken Sie auf **OK**.

Selbstverteidigung in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zu den Selbstverteidigungsmechanismen von Kaspersky Embedded Systems Security.

In diesem Kapitel

Über die Selbstverteidigung von Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security beinhaltet Selbstverteidigungsmechanismen, die das Programm davor schützt, dass Ordner auf der Festplatte, Speicherprozesse und Einträge in der Systemregistrierung gelöscht oder geändert werden.

Schutz vor Änderungen an Ordnern mit installierten Komponenten von Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security beschränkt das Umbenennen und Löschen von Ordnern mit den installierten Programmkomponenten für jedes Benutzerkonto. Standardmäßig lauten die Pfade der Programminstallationsordner wie folgt:

- In der 32-Bit-Version von Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- In der 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

Schutz vor Änderungen der Registrierungsschlüssel von Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security beschränkt den Zugriff auf die folgenden Registrierungszweige und -schlüssel, die zum Laden der Programmtreiber und -dienste verwendet werden:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\CrashDump] (in der 64-Bit-Version von Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.3\Trace]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.3\Trace] (in der 64-Bit-Version von Microsoft Windows)

Die Berechtigung zum Bearbeiten dieser Registrierungszweige und -schlüssel sind nur dem Benutzerkonto Lokales System (SYSTEM) zugeordnet. Die Konten Benutzer und Administrator verfügen nur über Leseberechtigung.

Kaspersky Security Service als geschützten Dienst registrieren

Die Technologie *Protected Process Light* (auch "PPL" genannt) stellt sicher, dass das Betriebssystem nur vertrauenswürdige Dienste und Prozesse lädt. Damit ein Dienst als geschützter Dienst ausgeführt werden kann, muss auf dem geschützten Computer ein Treiber für den *frühen Start der Antischadsoftware* installiert sein.

Ein Treiber für den *frühen Start der Antischadsoftware* (auch "ELAM" genannt) schützt die Computer in Ihrem Netzwerk beim Start und vor der Initialisierung der Drittanbietertreiber.

Der ELAM-Treiber wird automatisch während der Installation von Kaspersky Embedded Systems Security installiert und wird für die Registrierung von Kaspersky Security Service als PPL beim Start des Betriebssystems verwendet. Wenn Kaspersky Security Service (KAVFS) als systemgeschützter Prozess gestartet wird, können andere nicht geschützte Prozesse keine Threads einschleusen, nicht in den virtuellen Speicher des geschützten Prozesses schreiben und den Dienst nicht anhalten.

Wenn ein Prozess als PPL gestartet wird, kann er unabhängig von den zugewiesenen Benutzerberechtigungen nicht von Benutzern verwaltet werden. Die Registrierung von Kaspersky Security Service als PPL mittels ELAM-Treiber wird von den Betriebssystemen Microsoft Windows 10 und höher unterstützt. Wenn Sie Kaspersky Embedded Systems Security auf einem Server installieren, auf dem ein Betriebssystem mit PPL-Unterstützung läuft, steht die Berechtigungsverwaltung für Kaspersky Security Service (KAVFS) nicht zur Verfügung.

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security als PPL zu installieren:*

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen über die Rechte zur Verwaltung von Kaspersky Embedded Systems Security und der Windows-Dienste, die das Programm registriert, sowie eine Anleitung zur Konfiguration dieser Rechte.

In diesem Kapitel

Über Rechte zur Verwaltung von Kaspersky Embedded Systems Security

Standardmäßig haben die Benutzer der Gruppe "Administratoren" auf dem geschützten Computer und die Benutzer der Gruppe "ESS Administrators", die auf einem geschützten Computer bei der Installation von Kaspersky Embedded Systems Security erstellt wird, und die Gruppe "SYSTEM" Zugriff auf alle Funktionen von Kaspersky Embedded Systems Security .

Benutzer, die Zugriff auf die Funktionen Rechte **ändern** von Kaspersky Embedded Systems Security haben, können auch anderen Benutzern, die am geschützten Computer registriert sind oder zur Domäne gehören, den Zugriff auf Funktionen von Kaspersky Embedded Systems Security gewähren.

Wenn ein Benutzer nicht in die Liste der Benutzer von Kaspersky Embedded Systems Security registriert ist, kann er die Programmkonsole nicht öffnen.

Sie können für einen Benutzer oder eine Benutzergruppe eine der folgenden vordefinierten Zugriffsstufen auswählen:

- **Vollständige Kontrolle** – Zugriff auf alle Programmfunktionen: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Embedded Systems Security, der Komponenteneinstellungen, der Rechte von Benutzern von Kaspersky Embedded Systems Security, sowie Anzeigen der Statistik für Kaspersky Embedded Systems Security.
- **Ändern** – Zugang zu allen Programmfunktionen mit Ausnahme der Veränderung der Benutzerrechte: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Embedded Systems Security und der Einstellungen der Komponenten von Kaspersky Embedded Systems Security.
- **Lesen** – Anzeigen der allgemeinen Einstellungen von Kaspersky Embedded Systems Security, der Einstellungen der Komponenten von Kaspersky Embedded Systems Security, der Statistik für Kaspersky Embedded Systems Security und der Benutzerrechte für Kaspersky Embedded Systems Security.

Sie können ferner erweiterte Zugriffsberechtigungen anpassen: Zugriff auf bestimmte Funktionen von Kaspersky Embedded Systems Security erlauben oder verweigern.

Wenn Sie die Zugriffsrechte für einen Benutzer oder eine Gruppe manuell konfiguriert haben, so wird für diesen Benutzer bzw. diese Gruppe die Zugriffsstufe **Sonderrechte** festgelegt.

Tabelle 39. Über Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security

Zugriffsrechte	Beschreibung
Aufgabenverwaltung	Berechtigung zum Starten, Beenden, Anhalten bzw. Fortsetzen der Aufgaben von Kaspersky Embedded Systems Security.
Erstellen und Löschen von Aufgaben zur Untersuchung auf Befehl	Berechtigung zum Erstellen und Löschen von Aufgabe zur Untersuchung auf Befehl.
Ändern von Parametern	Berechtigungen: • Einstellungen von Kaspersky Embedded Systems Security aus einer Konfigurationsdatei importieren • Programmeinstellungen bearbeiten
Lesen von Parametern	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 über Aufgabenausführung, für das Systemaudit-Protokoll und für Benachrichtigungen anzeigen.
Datenverwaltung 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
Lesen von Protokollen	Berechtigung zur Anzeige der Ereignisse von Anti-Virus in Protokollen der Aufgabenausführung und im Systemaudit-Protokoll.
Lesen der Statistik	Berechtigung zum Anzeigen der Statistik für die einzelnen Aufgaben von Kaspersky Embedded Systems Security.
Lizenzverwaltung für das Programm	Berechtigung zum Aktivieren von Kaspersky Embedded Systems Security.
Programm entfernen	Berechtigung zum Deinstallieren von Kaspersky Embedded Systems Security.
Lesen von Benutzerrechten	Berechtigung zum Anzeigen der Liste der Benutzer von Kaspersky Embedded Systems Security und der Benutzerzugriffsrechte.

Zugriffsrechte	Beschreibung
Ändern von Rechten	Berechtigungen: • Liste der Benutzer ändern, die Zugriff auf die Programmverwaltung haben • Benutzerzugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security bearbeiten

Über die Rechte zur Verwaltung von registrierten Diensten

Während der Installation registriert Kaspersky Embedded Systems Security in Windows den Dienst Kaspersky Security Service (KAVFS), den Programmverwaltungsdienst Kaspersky Security Management Service (KAVFSGT) und Kaspersky Security Exploit-Prävention (KAVFSSLP).

Die Registrierung von Kaspersky Security Service als Protected Process Light mittels ELAM-Treiber wird von den Betriebssystemen Microsoft Windows 10 und höher unterstützt. Wenn ein Prozess als PPL gestartet wird, kann er unabhängig von den zugewiesenen Benutzerberechtigungen nicht von Benutzern verwaltet werden. Wenn Sie Kaspersky Embedded Systems Security auf einem Computer installieren, auf dem ein Betriebssystem mit PPL-Unterstützung läuft, steht die Berechtigungsverwaltung für Kaspersky Security Service (KAVFS) nicht zur Verfügung.

Kaspersky Security Service

Standardmäßig haben diejenigen Benutzer Zugriff auf die Verwaltung von Kaspersky Security Service, die der Gruppe "Administratoren" auf dem geschützten Computer angehören, sowie die Systemgruppen "SERVICE" und "INTERACTIVE" mit Leserechten und die Systemgruppe "SYSTEM" mit Rechten zum Lesen und Ausführen.

Benutzer, die Zugriff auf Funktionen der Stufe "Rechte ändern" haben (siehe Abschnitt "Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security" auf Seite 246), können anderen Benutzern, die auf dem geschützten Computer registriert sind oder zur Domäne gehören, Zugriff auf die Verwaltung von Kaspersky Security Service gewähren.

Dienst von Kaspersky Security Management Service

Zur Verwaltung des Programms über die auf einem anderen Computer installierte Programmkonsole muss das Benutzerkonto, mit dessen Rechten die Verbindung zu Kaspersky Embedded Systems Security hergestellt wird, unbeschränkten Zugriff auf Kaspersky Security Management Service auf dem geschützten Computer haben.

Folgende Benutzer besitzen standardmäßig Zugriff zur Verwaltung von Kaspersky Security Management Service: Benutzer, die auf dem geschützten Computer zur Gruppe "Administratoren" gehören, und Benutzer der Gruppe "ESS Administrators", die bei der Installation von Kaspersky Embedded Systems Security auf dem geschützten Computer erstellt wird.

Sie können Kaspersky Security Management Service nur über das Snap-In Dienste von Microsoft Windows verwalten.

Kaspersky Security-Exploit-Prävention

Standardmäßig haben diejenigen Benutzer Zugriff auf die Verwaltung des Kaspersky Security Exploit Prevention Service, die der Gruppe "Administratoren" auf dem geschützten Computer angehören, und die Systemgruppe "SYSTEM" mit Rechten zum Lesen und Ausführen.

Über die Rechte zur Verwaltung des Dienstes Kaspersky Security Service

Während der Installation registriert Kaspersky Embedded Systems Security den Dienst Kaspersky Security Service (KAVFS) in Windows und aktiviert intern die funktionalen Komponenten, die beim Hochfahren des Betriebssystems gestartet werden. Um die Gefahr des Zugriffs Unbefugter auf die Programmfunktionen und Sicherheitseinstellungen auf einem geschützten Computer über die Verwaltung von Kaspersky Security Service zu reduzieren, können Sie die Rechte zur Verwaltung von Kaspersky Security Service mithilfe der Programmkonsole oder des Verwaltungs-Plug-ins beschränken.

Standardmäßig werden Benutzern in der Gruppe "Administratoren" auf dem geschützten Computer Zugriffsrechte zur Verwaltung von Kaspersky Security Service eingeräumt. Den Gruppen "SERVICE" und "INTERACTIVE" werden Leserechte gewährt und die Gruppe "SYSTEM" erhält Rechte zum Lesen und Ausführen.

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 Benutzerkonto wiederhergestellt.

Benutzer, die Zugriff auf Funktionen haben (siehe Abschnitt "Über Rechte zur Verwaltung von Kaspersky Embedded Systems Security" auf S. 239), für welche die Berechtigung Rechte ändern erforderlich ist, können anderen Benutzern, die auf dem geschützten Computer registriert sind oder zur Domäne gehören, Zugriff auf die Verwaltung von Kaspersky Security Service gewähren.

Sie können für einen Benutzer oder eine Benutzergruppe von Kaspersky Embedded Systems Security eine der folgenden vordefinierten Zugriffsstufen auf die Verwaltung von Kaspersky Security Service auswählen:

- **Vollständige Kontrolle** – Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Security Service sowie zum Starten und Beenden von Kaspersky Security Service.
- **Lesen** – Berechtigung zum Aufrufen der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
- **Änderung** – Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
- **Ausführung** – Berechtigung zum Starten und Beenden von Kaspersky 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).

Wenn Sie die Zugriffsrechte für einen Benutzer oder eine Gruppe manuell konfiguriert haben, so wird für diesen Benutzer bzw. diese Gruppe die Zugriffsstufe **Sonderrechte** festgelegt.

Tabelle 40. Zugriffsrechte für die Funktionen von Kaspersky Security Service

Funktion	Beschreibung
Einstellungen des Dienstes lesen	Berechtigung zum Anzeigen der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
Status des Dienstes beim Service Control Manager abfragen	Berechtigung zur Abfrage des Ausführungsstatus von Kaspersky Security Service beim Service Control Manager von Microsoft Windows
Status beim Dienst abfragen	Berechtigung zur Abfrage des Ausführungsstatus des Dienstes bei Kaspersky Security Service.
Liste der abhängigen Dienste auslesen	Berechtigung zum Anzeigen einer Liste der Dienste, von denen Kaspersky Security Service abhängt, sowie der Dienste, die von Kaspersky Security Service abhängen.
Einstellungen des Dienstes anpassen	Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
Dienst starten	Berechtigung zum Starten von Kaspersky Security Service.
Dienst beenden	Berechtigung zum Beenden von Kaspersky Security Service.
Dienst anhalten / fortsetzen	Berechtigung zum Anhalten und Fortsetzen von Kaspersky Security Service.
Lesen von Benutzerrechten	Berechtigung zum Anzeigen der Benutzerlisten von Kaspersky Security Service und der Zugriffsrechte der einzelnen Benutzer
Ändern von Rechten	Berechtigungen: • Benutzer von Kaspersky Security Service hinzufügen und löschen • Zugriffsrechte der Benutzer auf Kaspersky Security Service ändern.
Dienst entfernen	Berechtigung zum Entfernen von Kaspersky Security Service aus der Registrierung über den Service Control Manager von Microsoft Windows.
Benutzeranfragen an den Dienst	Berechtigung zur Erstellung und zum Versand von Benutzeranfragen an Kaspersky Security Service.

Über Zugriffsrechte für Kaspersky Security Management Service

Sie können die Liste der Dienste von Kaspersky Embedded Systems Security überprüfen.

Während der Installation registriert Kaspersky Embedded Systems Security den Dienst Kaspersky Security Management Service (KAVFSGT). Zur Verwaltung des Programms über die auf einem anderen Computer installierte Programmkonsole muss das Benutzerkonto, das für die Verbindung zu Kaspersky Embedded Systems Security verwendet wird, unbeschränkten Zugriff auf Kaspersky Security Management Service auf dem geschützten Computer haben.

Folgende Benutzer besitzen standardmäßig Zugriff zur Verwaltung von Kaspersky Security Management Service: Benutzer, die auf dem geschützten Server zur Gruppe "Administratoren" gehören, und Benutzer der Gruppe KAVWSEE Administrators, die bei der Installation von Kaspersky Embedded Systems Security auf dem geschützten Server erstellt wird.

Sie können Kaspersky Security Management Service nur über das Snap-In Dienste von Microsoft Windows verwalten.

Sie können den Benutzerzugriff auf Kaspersky Security Management Service nicht durch Anpassen von Kaspersky Embedded Systems Security erlauben oder verweigern.

Sie können unter dem lokalen Benutzerkonto eine Verbindung mit Kaspersky Embedded Systems Security herstellen, wenn auf dem geschützten Computer ein Konto mit dem gleichen Benutzernamen und dem gleichen Kennwort registriert ist.

Konfigurieren der Zugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security und Kaspersky Security Service

Sie können die Liste der Benutzer und Benutzergruppen, die Zugriff auf die Funktionen von Kaspersky Embedded Systems Security haben und den Dienst Kaspersky Security Service verwalten dürfen, bearbeiten. Sie können auch die Zugriffsrechte dieser Benutzer und Benutzergruppen ändern.

► *Gehen Sie wie folgt vor, um Benutzer oder Gruppen zur Liste hinzuzufügen oder aus dieser zu entfernen:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen durch:

   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.
   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Verwaltung von Kaspersky Security Service** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die über Zugriffrechte zur Verwaltung des Dienstes Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** wird geöffnet.

5. Im sich öffnenden Fenster gehen Sie wie folgt vor:

   - Um einen Benutzer oder eine Gruppe zur Liste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie den Benutzer oder die Gruppe aus, der Sie Rechte einräumen möchten.
   - Um einen Benutzer oder eine Gruppe aus der Liste zu löschen, wählen Sie den Benutzer oder die Gruppe, deren Zugriff Sie einschränken möchten, aus und klicken Sie auf **Löschen**.

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die ausgewählten Benutzer (Gruppen) werden hinzugefügt bzw. entfernt.

► *Gehen Sie wie folgt vor, um die Rechte eines Benutzers oder einer Gruppe zur Verwaltung von Kaspersky Embedded Systems Security oder des Dienstes Kaspersky Security Service zu ändern:*

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen durch:

   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung ändern** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.
   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Verwaltung von Kaspersky Security Service ändern** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung des Programms mithilfe von Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** wird geöffnet.

5. Wählen Sie im nächsten Fenster in der Liste **Gruppen- oder Benutzernamen** den Benutzer oder die Benutzergruppe aus, dessen bzw. deren Rechte Sie ändern möchten.
6. Aktivieren Sie im Abschnitt **Berechtigungen für <Benutzer (Gruppe)>** die Kontrollkästchen **Erlauben** oder **Verbieten** für die folgenden Zugriffsstufen:
   - **Vollständige Kontrolle**: Uneingeschränkte Rechte zur Verwaltung von Kaspersky Embedded Systems Security oder Kaspersky Security Service.
   - **Lesen**:
     - Folgende Rechte für die Verwaltung von Kaspersky Embedded Systems Security: **Statistik abrufen**, **Einstellungen lesen**, **Protokolle lesen** und **Rechte lesen**.
     - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Lesen der Einstellungen des Dienstes**, **Statusanfrage für den Dienst beim Service Control Manager**, **Statusanfrage beim Dienst**, **Lesen der Liste der abhängigen Dienste**, **Rechte lesen**.
   - **Änderung**:
     - Alle Rechte zur Verwaltung von Kaspersky Embedded Systems Security mit Ausnahme von **Rechte ändern**.
     - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Diensteinstellungen konfigurieren**, **Rechte lesen**.
   - **Sonderrechte**: Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Dienst starten**, **Dienst beenden**, **Dienst anhalten/fortsetzen**, **Rechte lesen**, **Benutzeranfragen an den Dienst**.
7. Um erweiterte Rechte für einen Benutzer oder eine Gruppe (**Sonderrechte**) anzupassen, klicken Sie auf die Schaltfläche **Erweitert**.
   a. Wählen Sie im nächsten Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Embedded Systems Security** den gewünschten Benutzer bzw. die Gruppe aus.
   b. Klicken Sie auf die Schaltfläche **Ändern**.
   c. Wählen Sie in der Dropdown-Liste im oberen Fensterbereich die Art der Zugriffskontrolle aus (**Erlauben** oder **Blockieren**).
   d. Aktivieren Sie die Kontrollkästchen neben denjenigen Funktionen, die Sie dem betreffenden Benutzer bzw. der betreffenden Gruppe erlauben oder verbieten möchten.
   e. Klicken Sie auf **OK**.
   f. Klicken Sie im Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Embedded Systems Security** auf **OK**.
8. Klicken Sie im Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** auf die Schaltfläche **Übernehmen**.
9. Die konfigurierten Rechte für die Verwaltung von Kaspersky Embedded Systems Security oder Kaspersky Security Service werden gespeichert.

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste mithilfe der Einstellungen der Rechte der Benutzer (siehe Abschnitt "Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security" auf Seite 239) beschränken. Außerdem können Sie für zusätzlichen Schutz in den Einstellungen von Kaspersky Embedded Systems Security einen Kennwortschutz einrichten. Ein Kennwortschutz erlaubt Ihnen, den Zugriff auf die Verwaltung der Programmkonsole und die Ausführung von Befehlen in der Befehlszeilen zusätzlich einzuschränken. Wenn der Kennwortschutz übernommen wird, fordert Kaspersky Embedded Systems Security von allen Benutzern die Eingabe des Kennworts, wenn sie die Programmkonsole starten oder Befehle der Befehlszeile ausführen wollen.

► *Um den Zugriff auf Funktionen von Kaspersky Embedded Systems Security zu schützen, gehen Sie wie folgt vor:*

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** aus.

   Das Fenster **Programmeinstellungen** wird geöffnet.
2. Klicken Sie auf der Registerkarte **Sicherheit und Zuverlässigkeit** in den **Einstellungen für den Kennwortschutz** auf das Kontrollkästchen **Kennwortschutz verwenden**.

   Die Felder **Kennwort** und **Kennwort bestätigen** werden aktiv.
3. Geben Sie im Feld **Kennwort** den Wert ein, den Sie für den Schutz des Zugriffes auf die Funktionen von Kaspersky Embedded Systems Security verwenden möchten.
4. Geben Sie im Feld **Kennwort bestätigen** das Kennwort erneut ein.
5. Klicken Sie auf **OK**.

Das festgelegte Kennwort kann nicht wiederhergestellt werden. Wenn Sie das Kennwort verlieren, führt das zum vollständigen Verlust der Kontrolle über das Programm. Darüber hinaus kann das Programm nicht vom geschützten Computer entfernt werden.

Sie können das Kennwort jederzeit zurücksetzen. Deaktivieren Sie dazu das Kontrollkästchen **Kennwortschutz verwenden** und speichern Sie die Änderungen. Der Kennwortschutz wird deaktiviert und die alte Prüfsumme des Kennworts entfernt. Wiederholen Sie den Kennworteingabeprozess mit einem neuen Kennwort.

Zugriffsrechte in Kaspersky Security Center anpassen

Sie können die Rechte für den Zugriff auf die Programmverwaltung und die Verwaltung von Kaspersky Security Service in Kaspersky Security Center für Computergruppen und für einzelne Computer konfigurieren.

► *Gehen Sie wie folgt vor, um die Zugriffsrechte für die Programmverwaltung und die Verwaltung des Dienstes von Kaspersky Security Service zu konfigurieren:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Öffnen Sie den Abschnitt **Zusätzlich** und gehen Sie wie folgt vor:
   - Wenn Sie die Zugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security für Benutzer oder eine Benutzergruppe konfigurieren möchten, klicken Sie im Abschnitt **Benutzerrechte für die Programmverwaltung** auf die Schaltfläche **Einstellungen**.
   - Wenn Sie die Zugriffsrechte zur Verwaltung von Kaspersky Security Service für Benutzer oder eine Benutzergruppe konfigurieren möchten, klicken Sie im Abschnitt **Benutzerrechte für die Verwaltung von Security Service** auf die Schaltfläche **Einstellungen**.
5. Passen Sie im nächsten Fenster die Zugriffsrechte (siehe Abschnitt "Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security" auf Seite 239) entsprechend Ihren Bedürfnissen an.

Die vorgenommenen Einstellungen werden gespeichert.

Echtzeitschutz für Dateien

Dieser Abschnitt informiert über die Aufgabe Echtzeitschutz für Dateien und erläutert die Konfiguration dieser Aufgabe.

In diesem Kapitel

Über die Aufgabe zum Echtzeitschutz für Dateien

Bei Ausführung der Aufgabe zum Echtzeitschutz für Dateien untersucht Kaspersky Embedded Systems Security folgende Objekte des geschützten Computers, wenn auf diese zugegriffen wird:

- Dateien
- Alternative Datenströme der Dateisysteme (NTFS-Streams).
- Master Boot Records und Bootsektoren von lokalen Festplatten und externen Geräten

Wenn ein Programm eine Datei auf dem Computer speichert oder eine Datei vom Server abruft, fängt Kaspersky Embedded Systems Security diese Datei ab, untersucht sie auf Bedrohungen und führt bei gefundenen Bedrohungen die in den Einstellungen der Aufgabe festgelegten bzw. standardmäßigen Aktionen aus: Es wird versucht, die Datei zu desinfizieren, die Datei in die Quarantäne zu verschieben oder sie zu löschen, falls eine Desinfektion nicht möglich ist. Vor der Desinfektion oder dem Löschen speichert Kaspersky Embedded Systems Security eine verschlüsselte Kopie der Quelldatei im Backup-Ordner. Kaspersky Embedded Systems Security stellt die Datei aus der Quarantäne wieder im ursprünglichen Ordner her, wenn sie erfolgreich desinfiziert wurde.

Kaspersky Embedded Systems Security erkennt außerdem Schadsoftware für Prozesse, die unter Windows Subsystem for Linux® laufen. Bei solchen Prozessen wendet die Aufgabe "Echtzeitschutz für Dateien" die von der aktuellen Konfiguration festgelegte Aktion an.

Über den Schutzbereich von Aufgaben und Sicherheitseinstellungen

Standardmäßig schützt die Aufgabe für den Echtzeitschutz für Dateien alle Objekte im Dateisystem des Computers. 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 Programmkonsole wird der Schutzbereich als Struktur oder Liste jener Dateiressourcen des Computers dargestellt, die von Kaspersky Embedded Systems Security überwacht werden können. Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Computers als Liste angezeigt.

Im Verwaltungs-Plug-in steht nur die Listenansicht zur Verfügung.

► *Um freigegebene Netzwerkordner in der Programmkonsole in der Baumstruktur anzuzeigen, gehen Sie wie folgt vor:*

Wählen Sie im linken unteren Teil des Fensters Schutzbereich aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.

Die Elemente oder Knoten werden in einer Listenansicht oder in einer Baumstruktur der Dateiressourcen des Computers auf folgende Weise dargestellt:

☑ Der Knoten ist im Schutzbereich.

☐ Der Knoten ist nicht im Schutzbereich.

☑ Mindestens ein diesem Knoten untergeordneter Knoten gehört nicht zum Schutzbereich oder die Sicherheitsparameter des oder der untergeordneten Knoten unterscheiden sich von den Sicherheitsparametern dieses Knotens (nur für die Baumstruktur-Ansicht).

Das Symbol ☑ wird angezeigt, wenn alle untergeordneten Knoten ausgewählt sind, nicht jedoch der übergeordnete Knoten. In diesem Fall werden Änderungen der Datei- und Ordnerzusammensetzung des übergeordneten Knotens bei der Einrichtung eines Schutzbereichs für den ausgewählten untergeordneten Knoten nicht automatisch berücksichtigt.

Mithilfe der Programmkonsole können Sie zum Schutzbereich auch virtuelle Festplatten hinzufügen (siehe Abschnitt "Virtuellen Schutzbereich erstellen" auf Seite 281). Die Namen von virtuellen Nodes werden in blauer Schrift dargestellt.

Parameter für Sicherheit

Die Sicherheitseinstellungen für Aufgaben können als allgemeine Einstellungen für alle Knoten oder Elemente im Schutzbereich, oder als unterschiedliche Einstellungen für jeden Knoten bzw. jedes Element in der Baumstruktur oder Liste der Computerdateiressourcen konfiguriert werden.

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:

- Eine von drei vordefinierten Sicherheitsstufen auswählen (auf Seite 252).
- Für die ausgewählten Nodes oder Elemente in der Struktur oder Liste der Dateiressourcen die Sicherheitseinstellungen manuell konfigurieren (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 265) (die Sicherheitsstufe ändert sich zu Benutzerdefiniert).

Sie können einen Einstellungssatz für einen Knoten oder ein Element in einer Vorlage speichern, um diese Vorlage später für andere Nodes oder Elemente zu übernehmen.

Über den virtuellen Schutzbereich

Kaspersky Embedded Systems Security kann nicht nur vorhandene Ordner und Dateien auf Festplatten und Wechseldatenträgern untersuchen, sondern auch Datenträger, die von verschiedenen Anwendungen und Diensten dynamisch auf dem Computer angelegt werden.

Wenn Sie alle Computerobjekte in den Schutzbereich aufgenommen haben, gehören automatisch auch diese dynamischen Knoten zum Schutzbereich. Wenn Sie allerdings spezielle Werte für die Sicherheitsparameter dieser dynamischen Knoten festlegen möchten oder den Schutz nicht für den gesamten Computer, sondern nur für einzelne Bereiche aktiviert haben, dann muss, um dynamische Laufwerke, Ordner oder Dateien in den Schutzbereich aufzunehmen, zuvor in der Programmkonsole ein virtueller Schutzbereich angelegt werden. Die von Ihnen angelegten Laufwerke, Ordner und Dateien existieren nur in der Programmkonsole, nicht aber in der Dateisystemstruktur des geschützten Computers.

Wenn Sie einen Schutzbereich anlegen und alle untergeordneten Ordner oder Dateien auswählen, nicht aber den übergeordneten Ordner, dann werden die dynamischen Ordner oder Dateien, die sich darin befinden, nicht automatisch in den Schutzbereich aufgenommen. Es ist erforderlich, in der Programmkonsole "virtuelle Kopien" davon anzulegen und zum Schutzbereich hinzuzufügen.

Vordefinierte Schutzbereiche

Die Dateistruktur oder Liste der Dateiressourcen des Computers enthält die Knoten, für die Sie nach den Sicherheitseinstellungen in Microsoft Windows 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 Computers.
- Wechseldatenträger. Kaspersky Embedded Systems Security schützt Dateien auf externen Geräten, z. B. auf CDs oder USB-Laufwerken. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Schutzbereich aufnehmen oder aus diesem ausschließen.
- Netzwerkumgebung. Kaspersky Embedded Systems Security schützt die Dateien, die in Netzwerkordnern gespeichert sind oder aus diesen von auf dem Computer laufenden Programmen abgefragt werden. Kaspersky Embedded Systems Security schützt Dateien in Netzwerkordnern nicht, wenn Programme von anderen Rechnern aus darauf zugreifen.

- Virtuelle Festplatten. Sie können in den Schutzbereich dynamische Ordner und Dateien sowie Laufwerke aufnehmen, die vorübergehend auf dem Computer eingebunden werden, z. B. gemeinsame Cluster-Laufwerke.

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 Einstellungen des Schutzbereichs verfügbar.

Standardmäßig sind alle vordefinierten Bereiche mit Ausnahme von virtuellen Festplatten in den Schutzbereich eingeschlossen.

Virtuelle Festplatten, die mit dem Befehl SUBST erzeugt wurden, werden nicht in der Struktur der Computerdateiressourcen in der Programmkonsole angezeigt. Um Objekte auf einer virtuellen Festplatte in den Schutzbereich aufzunehmen, schließen Sie den Ordner auf dem Computer, mit dem diese virtuelle Festplatte verbunden ist, in den Schutzbereich ein.

Verbundene Netzlaufwerke werden ebenfalls nicht in der Dateiressourcenliste des Computers 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).

Vordefinierte Sicherheitsstufen

Für in der Struktur oder Liste der Dateiressourcen des Computers ausgewählte Knoten können Sie eine der folgenden vordefinierten Sicherheitsstufen festlegen: Maximale Leistung, Empfohlen oder Maximale Sicherheit. Jede dieser Stufen besitzt eine eigene Auswahl von Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe Maximale Leistung wird empfohlen, wenn es zusätzlich zur Verwendung von Kaspersky Embedded Systems Security auf Computern noch weitere Sicherheitsmaßnahmen innerhalb Ihres Netzwerks gibt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien.

Empfohlen

Die Sicherheitsstufe Empfohlen bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Computer. Diese Stufe ist laut Empfehlung der Experten von Kaspersky Lab für den Schutz von Computern in den meisten Unternehmensnetzwerken ausreichend. Die Sicherheitsstufe Empfohlen gilt als Standard.

Maximale Sicherheit

Die Sicherheitsstufe Maximale Sicherheit wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Computersicherheit hat.

Tabelle 41. Vordefinierte Sicherheitsstufen und entsprechende Einstellungswerte

Einstellungen	Sicherheitsstufe		
	Maximale Leistung	Empfohlen	Maximale Sicherheit
Schutz von Objekten	Nach Erweiterung	Nach Format	Nach Format
Nur neue und veränderte Dateien schützen	Aktiviert	Aktiviert	Deaktiviert
Aktion für infizierte und andere Objekte	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen	Zugriff verweigern und empfohlene Aktion ausführen	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte	Zugriff verweigern und in die Quarantäne verschieben	Zugriff verweigern und empfohlene Aktion ausführen	Zugriff verweigern und in die Quarantäne verschieben
Dateien ausschließen	Nein	Nein	Nein
Nicht erkennen	Nein	Nein	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	60 Sek.	60 Sek.	60 Sek.
Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	8 MB	8 MB	Nicht konfiguriert.
Alternative NTFS-Ströme	Ja	Ja	Ja
Bootsektoren und MBR	Ja	Ja	Ja
Schutz von zusammengesetzten Objekten	• Gepackte Objekte* *Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Alle Objekte
Vom Programm nicht modifizierbare zusammengesetzte Datei vollständig entfernen, wenn ein eingebettetes Objekt gefunden wird	Nein	Nein	Ja

Die Einstellungen Schutz von Objekten, iChecker-Technologie verwenden, iSwift-Technologie verwenden und Heuristische Analyse verwenden sind nicht in den vordefinierten Sicherheitsstufen enthalten. Wenn Sie nach der Auswahl einer der vordefinierten Sicherheitsstufen die Sicherheitseinstellungen für Schutz von Objekten, iChecker-Technologie verwenden, iSwift-Technologie verwenden, Heuristische Analyse verwenden verändern, wird dadurch die gewählte voreingestellte Sicherheitsstufe nicht geändert.

Dateierweiterungen, die in der Aufgabe zum 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?*

Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien

Die Aufgabe zum Echtzeitschutz für Dateien weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 42. Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien

Einstellung	Standardwert	Beschreibung
Schutzbereich	Gesamter Computer ohne virtuelle Festplatten	Sie können den Schutzbereich beschränken.
Schutzmodus für Objekte	Beim Öffnen und Ändern	Sie können den Schutzmodus für Objekte festlegen, also die Zugriffsart angeben, bei der Objekte von Kaspersky Embedded Systems Security überprüft werden.
Heuristische Analyse	Es wird die Sicherheitsstufe Mittel angewendet.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
Vertrauenswürdige Zone anwenden	Wird verwendet	Einheitliche Liste mit Ausnahmen, die Sie in bestimmten Aufgaben verwenden können.
KSN zum Schutz verwenden	Wird verwendet	Sie können Ihren Server durch die Nutzung der Cloud-Dienste von Kaspersky Security Network effektiver schützen (nur verfügbar, wenn die KSN-Erklärung akzeptiert wurde).
Zeitplan für den Aufgabenstart	Bei Programmstart.	Sie können die Ausführung einer Aufgabe nach Zeitplan konfigurieren.
Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen	Wird nicht verwendet.	Sie können Hosts, die schädliche Aktivitäten zeigen, zur Liste der blockierten Hosts hinzufügen.

Aufgabe zum Echtzeitschutz für Dateien über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Aufgabeneinstellungen für einen oder alle Computer im Netzwerk konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen

► *Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien über die Richtlinie für Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Richtlinien: <Name der Richtlinie>** den Abschnitt Echtzeit-Computerschutz aus.
6. Klicken Sie auf die Schaltfläche Einstellungen im Unterabschnitt Echtzeitschutz für Dateien.

   Das Fenster Echtzeitschutz für Dateien wird geöffnet.

Wenn ein Computer durch eine aktive Richtlinie von Kaspersky Security Center verwaltet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht über die Programmkonsole geändert werden.

Aufgabeneigenschaften für den Echtzeitschutz für Dateien öffnen

► *Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien für einen einzelnen*

Netzwerkcomputer zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des geschützten Computers.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Computers aus.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
5. Wählen Sie im Abschnitt **Aufgaben** die Aufgabe Echtzeitschutz für Dateien aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Eigenschaften:** Echtzeitschutz für Dateien wird geöffnet.

Aufgabe zum Echtzeitschutz für Dateien anpassen

► *Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite 258).
2. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Auf der Registerkarte Allgemein:
     - Schutzmodus für Objekte (siehe Abschnitt "**Schutzmodus auswählen**" auf Seite 260)
     - Heuristische Analyse
     - Integration mit anderen Komponenten (siehe Abschnitt "**Heuristische Analyse und Integration mit anderen Programmkomponenten**" auf Seite 261).
   - Auf der Registerkarte Aufgabenverwaltung:
     - Einstellungen für den Start der Aufgabe nach Zeitplan (siehe Abschnitt "Einstellungen für den Zeitplan für den Aufgabenstart anpassen" auf Seite. 139).
3. Wählen Sie die Registerkarte Schutzbereich aus und gehen Sie wie folgt vor:
   - Klicken Sie auf die Schaltfläche Hinzufügen oder Ändern, um den Schutzbereich zu ändern (siehe Abschnitt "Schutzbereich erstellen" auf Seite 278).
     - Wählen Sie im geöffneten Fenster alles aus, was Sie in den Schutzbereich der Aufgabe aufnehmen wollen:
       - Vordefinierter Bereich
       - Laufwerk, Ordner oder Netzwerkobjekt
       - Datei
     - Wählen Sie eine der vordefinierten Sicherheitsstufen aus (auf S. 252) oder passen Sie den Schutz manuell an (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf S. 265).
4. Klicken Sie im Fenster Echtzeitschutz für Dateien auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

In diesem Abschnitt

Schutzmodus auswählen

Sie können den Schutzmodus in der Aufgabe Echtzeitschutz für Dateien auswählen. Im Abschnitt Schutzmodus für Objekte können Sie festlegen, bei welcher Art des Zugriffs auf die Objekte Kaspersky Embedded Systems Security eine Untersuchung durchführt.

Die Einstellung Schutzmodus für Objekte hat einen einheitlichen Wert für den gesamten Schutzbereich, der in der Aufgabe vorgegeben ist. Für diese Einstellung können keine unterschiedlichen Werte für einzelne Knoten des Schutzbereichs festgelegt werden.

► *Um den Schutzmodus auszuwählen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite 258).
2. Wählen Sie im folgenden Fenster auf der Registerkarte Allgemein den Schutzmodus aus, den Sie festlegen möchten:
   - Intelligenter Modus

     Kaspersky Embedded Systems Security wählt die Objekte für die Untersuchung selbstständig aus. Das Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn ein Prozess mehrmals auf das Objekt zugreift und es verändert, untersucht Kaspersky Embedded Systems Security das Objekt erst dann erneut, wenn es von diesem Prozess zum letzten Mal gespeichert wird.
   - Beim Öffnen und Ändern

     Kaspersky Embedded Systems Security untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern.

     Diese Variante gilt als Standard.
   - Beim Öffnen

     Kaspersky Embedded Systems Security untersucht alle Objekte, wenn diese zum Lesen, zur Ausführung oder zum Ändern geöffnet werden.
   - Beim Ausführen

     Kaspersky Embedded Systems Security untersucht die Datei nur beim Öffnen zum Ausführen.
3. Klicken Sie auf **OK**.

Der ausgewählte Schutzmodus für die Objekte wird eingestellt.

Heuristische Analyse und Integration mit anderen Programmkomponenten

Die Aufgabe "Verwendung von KSN" kann nur gestartet werden, wenn die Erklärung zu Kaspersky Security Network akzeptiert wurde.

► *Um die heuristische Analyse und Integration mit anderen Programmkomponenten zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite 258).
2. Deaktivieren oder aktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen Heuristische Analyse verwenden.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der heuristischen Analyse bei der Objektuntersuchung.

   Wenn dieses Kontrollkästchen aktiviert ist, ist die heuristische Analyse aktiviert.

   Wurde dieses Kontrollkästchen deaktiviert, ist die heuristische Analyse deaktiviert.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
3. Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.

   Mit dem Schieberegler lässt sich die Stufe die Ebene der heuristischen Analyse regulieren. Die Genauigkeitsstufe der Untersuchung regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach Bedrohungen, dem Auslastungsniveau der Betriebssystemressourcen und der Untersuchungsdauer.

   Für die Untersuchung sind folgende Genauigkeitsstufen vorgesehen:

   - Oberflächlich. Bei der heuristischen Analyse wird eine relativ geringe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. In diesem Modus besteht eine geringere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung beansprucht weniger Systemressourcen und wird schneller ausgeführt.
   - Mittel. Die Anzahl der Befehle, die bei der heuristischen Analyse in der ausführbaren Datei ausgeführt werden, richtet sich nach den Empfehlungen der Kaspersky-Lab-Experten.

     Diese Stufe gilt als Standard.
   - Tief. Bei der heuristischen Analyse wird eine relativ hohe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. Bei dieser Einstellung besteht eine höhere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung benötigt mehr Systemressourcen und mehr Zeit und kann eine erhöhte Anzahl an Fehlalarmen auslösen.

     Der Schieberegler ist aktiv, wenn das Kontrollkästchen Heuristische Analyse verwenden aktiviert ist.

4. Konfigurieren Sie im Abschnitt Integration mit anderen Komponenten die folgenden Einstellungen:
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen Vertrauenswürdige Zone anwenden.

     Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

     Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

     Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs für die Aufgabe.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen KSN zum Schutz verwenden.

     Mit diesem Kontrollkästchen wird die Verwendung der KSN-Dienste aktiviert und deaktiviert.

     Wenn das Kontrollkästchen aktiviert ist, verwendet das Programm die Daten von Kaspersky Security Network um sicherzustellen, dass das Programm schneller auf neue Bedrohungen reagiert und die Wahrscheinlichkeit von Fehlalarmen verringert wird.

     Ist das Kontrollkästchen deaktiviert, werden die KSN-Dienste von der Aufgabe nicht verwendet.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     Dieses Feld wird angezeigt, wenn das Kontrollkästchen Daten über untersuchte Dateien senden in den Aufgabeneinstellungen für die Verwendung von KSN aktiviert ist.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen Zugriff auf freigegebene Netzwerkordner für Computer blockieren, die bösartige Aktivität zeigen.
5. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe werden unverzüglich während der Ausführung der Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Einstellungen des Zeitplans für den Aufgabenstart anpassen

In der Programmkonsole können Sie den Startzeitplan für lokale Systemaufgaben und benutzerdefinierte Aufgaben anpassen. Für den Start von Gruppenaufgaben kann der Zeitplan nicht angepasst werden.

► *Um die Zeitplan-Einstellungen für den Gruppenaufgabenstart anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Wählen Sie die Gruppe aus, zu der der geschützte Server gehört.
3. Wählen Sie im Ergebnisbereich die Registerkarte **Aufgaben** aus.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie auf den Namen der Aufgabe.
   - Öffnen Sie das Kontextmenü für den Namen der Aufgabe und wählen Sie den Punkt "Eigenschaften".
5. Wählen Sie den Abschnitt **Zeitplan** aus.
6. Aktivieren Sie im Block **Zeitplan-Einstellungen** das Kontrollkästchen Aufgabe nach Zeitplan starten.

   Die Felder mit den Zeitplan-Einstellungen der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe stehen nicht zur Verfügung, wenn der Start der Aufgabe durch eine Richtlinie von Kaspersky Security Center verboten ist.

7. Passen Sie die Zeitplaneinstellungen entsprechend Ihren Anforderungen an. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie in der Liste Startintervall einen der folgenden Werte aus:
      - Stündlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Stunden gestartet wird, wobei Sie die Anzahl der Stunden im Feld **Alle <Anzahl> Std.** eingeben müssen.
      - Täglich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Tagen gestartet wird, wobei Sie die Anzahl der Tage im Feld **Alle <Anzahl> Tage** eingeben müssen.
      - Wöchentlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl von Wochen gestartet wird, wobei Sie die Anzahl der Wochen im Feld **Alle <Anzahl> Wochen** eingeben müssen. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (Standardmäßig werden Aufgaben montags gestartet).
      - Bei Programmstart, wenn Sie möchten, dass die Aufgabe bei jedem Start von Kaspersky Embedded Systems Security ausgeführt wird.
      - Nach dem Update der Programm-Datenbanken, wenn Sie möchten, dass die Aufgabe nach jedem Update der Programm-Datenbanken gestartet wird.

   b. Legen Sie im Feld Startzeit die Uhrzeit des erstmaligen Aufgabenstarts fest.
   c. Tragen Sie im Feld Startdatum das Startdatum des Zeitplans ein.

      Nachdem Sie das Startintervall der Aufgabe, die Uhrzeit für den erstmaligen Aufgabenstart und das Datum, ab dem der Zeitplan gelten soll, angegeben haben, wird im oberen Bereich des Fensters im Feld Nächster Start der berechnete Zeitpunkt des nächsten Aufgabenstarts angezeigt. Aktualisierte Informationen über die Zeit, die bis zum nächsten Start verbleibt, werden jedes Mal angezeigt, wenn Sie das Fenster Aufgabeneinstellungen auf der Registerkarte Zeitplan öffnen.
      Der Wert Durch Richtlinie verboten im Feld Nächster Start wird angezeigt, wenn der Start von geplanten Systemaufgaben durch die Einstellungen der aktiven Richtlinie des Programms Kaspersky Security Center verboten ist (siehe Abschnitt "Zeitplan für den Start von lokalen Systemaufgaben anpassen" auf S. 103).

8. Passen Sie auf der Registerkarte Erweitert die folgenden Zeitplaneinstellungen gemäß Ihren Anforderungen an.

- Im Abschnitt Einstellungen für das Anhalten der Aufgabe:
  a. Aktivieren Sie das Kontrollkästchen Dauer und geben Sie die erforderliche Anzahl an Stunden und Minuten in den Feldern rechts davon ein, um so die maximale Dauer der Aufgabenausführung vorzugeben.
  b. Aktivieren Sie das Kontrollkästchen Anhalten von und geben Sie die Anfangszeit und Endzeit des Zeitintervalls in den Feldern rechts davon ein, um einen Zeitraum innerhalb von 24 Stunden anzugeben, in dem die Aufgabenausführung angehalten wird.
- Im Abschnitt Erweiterte Einstellungen:
  a. Aktivieren Sie das Kontrollkästchen Zeitplan deaktivieren ab und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.
  b. Aktivieren Sie das Kontrollkästchen Übersprungene Aufgaben starten, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.
  c. Aktivieren Sie das Kontrollkästchen Aufgabenstart zufällig wählen innerhalb von und geben Sie einen Wert in Minuten ein.

9. Klicken Sie auf OK.
10. 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, gehen Sie wie im Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen (auf Seite 126) beschrieben vor.

Schutzbereich von Aufgaben erstellen und konfigurieren

► *Um den Schutzbereich von Aufgaben über das Kaspersky Security Center zu erstellen und zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite 258).
2. Wählen Sie die Registerkarte Schutzbereich aus.
3. Alle bereits durch die Aufgabe geschützten Elemente sind in der Tabelle Schutzbereich aufgelistet.
4. Klicken Sie auf die Schaltfläche Hinzufügen, um ein neues Element zur Liste hinzuzufügen.

   Das Fenster Objekte zum Schutzbereich hinzufügen wird geöffnet.
5. Wählen Sie einen Objekttyp aus, um ihm zu einem Schutzbereich hinzuzufügen:
   - Vordefinierter Bereich, wenn Sie in den Schutzbereich einen der vordefinierten Bereiche auf dem Server aufnehmen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Schutzbereich aus.
   - Laufwerk, Ordner oder Netzwerkobjekt, wenn Sie in den Schutzbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Schutzbereich über die Schaltfläche Durchsuchen aus.
   - Datei, wenn Sie in den Schutzbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Schutzbereich über die Schaltfläche Durchsuchen aus.

Sie können ein Objekt nicht zum Schutzbereich hinzufügen, wenn es bereits als Ausnahme aus dem Schutzbereich hinzugefügt wurde.

6. Um einzelne Elemente aus dem Schutzbereich auszuschließen, deaktivieren Sie die Kontrollkästchen neben den Namen dieser Elemente, oder führen Sie die folgenden Schritte durch:
   a. Öffnen Sie das Kontextmenü des Schutzbereichs mit der rechten Maustaste.
   b. Wählen Sie im Kontextmenü den Punkt Ausnahme hinzufügen.
   c. Wählen Sie im geöffneten Fenster Ausnahme hinzufügen den Typ des Objektes aus, das Sie als Ausnahme aus dem Schutzbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Schutzbereich.
7. Um den Schutzbereich oder eine hinzugefügte Ausnahme zu ändern, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option Bereich ändern.
8. Um die Anzeige eines zuvor hinzugefügten Schutzbereich bzw. einer Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option Aus Liste löschen aus.

   Der Schutzbereich wird aus dem Gültigkeitsbereich der Aufgabe zum Echtzeitschutz für Dateien bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner ausgeschlossen.

9. Klicken Sie auf die Schaltfläche **Speichern**.

Das Einstellungsfenster des Schutzbereichs wird geschlossen. Ihre neu konfigurierten Einstellungen werden gespeichert.

Die Aufgabe Echtzeitschutz für Dateien kann gestartet werden, wenn mindestens ein Knoten der Struktur der Dateiressourcen des Computers in den Schutzbereich aufgenommen wurde.

Sicherheitseinstellungen manuell anpassen

Standardmäßig werden in der Aufgabe Echtzeitschutz für Dateien die gleichen Sicherheitsparameter verwendet wie für den gesamten Schutzbereich. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe Empfohlen (siehe Abschnitt "Vordefinierte Sicherheitsstufen " auf S. 252).

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des Computers oder den Knoten in der Struktur festlegen.

► *So passen Sie die Sicherheitsparameter eines bestimmten Knotens manuell an:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite 258).
2. Wählen Sie auf der Registerkarte Schutzbereich den Knoten aus, dessen Sicherheitseinstellungen Sie anpassen möchten, und klicken Sie auf die Schaltfläche Anpassen.

   Das Fenster Einstellungen für den Echtzeitschutz für Dateien anpassen wird geöffnet.

3. Klicken Sie auf der Registerkarte Sicherheitsstufe auf die Schaltfläche Einstellungen, um eine benutzerdefinierte Konfiguration einzurichten.
4. Sie können die benutzerdefinierten Sicherheitseinstellungen des ausgewählten Knotens gemäß Ihren Bedürfnissen anpassen:
   - Allgemeine Einstellungen (siehe Abschnitt "Allgemeine Aufgabeneinstellungen anpassen" auf Seite 266)
   - Aktionen (siehe Abschnitt "Aktionen anpassen" auf Seite 269)
   - Optimierung (siehe Abschnitt "Leistung optimieren" auf Seite 271)
5. Klicken Sie im Fenster Echtzeitschutz für Dateien auf **OK**.

Die neuen Einstellungen des Schutzbereichs werden gespeichert.

In diesem Abschnitt

Allgemeine Aufgabeneinstellungen anpassen

► *So passen Sie die allgemeinen Sicherheitseinstellungen der Aufgabe zum Echtzeitschutz für Dateien an:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite 258).
2. Wählen Sie die Registerkarte Allgemein aus.
3. Geben Sie im Abschnitt Schutz von Objekten die Objektarten an, die Sie in den Schutzbereich einschließen möchten:
   - Alle Objekte

     Kaspersky Embedded Systems Security untersucht alle Objekte.
   - Objekte, die nach Format untersucht werden

     Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats.

     Die Liste der Dateiformate wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
   - Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden

     Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung.

     Die Erweiterungsliste wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.

- Objekte, die nach der angegebenen Erweiterungsliste untersucht werden

  Kaspersky Embedded Systems Security untersucht Dateien auf der Grundlage der Dateierweiterung. Die Dateierweiterungsliste können Sie im Fenster Erweiterungsliste mithilfe der Schaltfläche Ändern manuell anpassen.

- Bootsektoren und MBR

  Aktivierung des Schutzes für Laufwerk-Bootsektoren und Master Boot Records (MBR)

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security die Bootsektoren und Master Boot Records auf Festplatten und Wechseldatenträgern des Computers.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Alternative NTFS-Ströme

  Untersuchung zusätzlicher Ströme von Dateien und Ordnern auf den Laufwerken des NTFS-Dateisystems.

  Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm ein möglicherweise infiziertes Objekt und alle NTFS-Streams, die mit diesem Objekte verbunden sind.

  Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm nur das Objekt, das gefunden und als möglicherweise infiziert betrachtet wurde.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Aktivieren oder deaktivieren Sie im Abschnitt Optimierung das Kontrollkästchen Nur neue und veränderte Dateien schützen.

   Mit diesem Kontrollkästchen werden die Untersuchung und der Schutz von Dateien, die Kaspersky Embedded Systems Security als neu oder seit der letzten Untersuchung geändert erkennt, aktiviert oder deaktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, untersucht und schützt Kaspersky Embedded Systems Security nur die Dateien, die als neu oder seit der letzten Untersuchung verändert erkannt wurden.

   Wenn das Kontrollkästchen deaktiviert ist, können Sie auswählen, ob Sie nur neue Dateien oder alle Dateien unabhängig von deren Änderungsstatus untersuchen möchten.

   Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert. Wurde die Sicherheitsstufe Maximale Sicherheit oder Empfohlen ausgewählt, ist das Kontrollkästchen deaktiviert.

   Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

5. Geben Sie im Abschnitt Schutz von zusammengesetzten Objekten die zusammengesetzten Objekte an, die Sie in den Schutzbereich einschließen möchten:

   - **Alle /** nur neue Archive

     Untersuchung von Archiven in den Formaten ZIP, CAB, RAR, ARJ u. a.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Embedded

Systems Security bei der Untersuchung übersprungen.

Der Standardwert ist von der aktuellen Schutzebene abhängig.

- **Alle /** Nur neue SFX-Archive

  Selbstentpackende Archive untersuchen.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security SFX-Archive.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

  Diese Einstellung ist aktiv, wenn das Kontrollkästchen Archive deaktiviert ist.

- **Alle /** Nur neue E-Mail-Datenbanken

  Dateien in Mail-Datenbanken für Microsoft Outlook und Microsoft Outlook Express werden untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Mail-Datenbankdateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Mail-Datenbankdateien von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** nur neue gepackte Objekte

  Untersuchung von ausführbaren Dateien, die mit Packprogrammen für Binärcode wie beispielsweise UPX oder ASPack gepackt wurden.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security ausführbare Dateien, die mit Packprogrammen gepackt wurden.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden ausführbare Dateien, die mit Packprogrammen gepackt wurden, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

- **Alle /** nur neue Dateien in Mail-Formaten

  Dateien in Mail-Formaten werden untersucht. Dazu zählen beispielsweise Nachrichten der Formate Microsoft Outlook und Microsoft Outlook Express.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien in Mail-Formaten.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Dateien in Mail-Formaten von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** Nur neue eingebettete OLE-Objekte

  Untersuchung von Objekten, die in eine Datei eingebettet sind (beispielsweise Excel-Tabellen, Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten).

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte, die in eine Datei eingebettet sind.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Objekte, die in eine Datei eingebettet sind, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

6. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

► *So passen Sie die Aktionen für infizierte und andere gefundene Objekte für die Aufgabe zum Echtzeitschutz für Dateien an:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien (siehe Abschnitt "**Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen**" auf Seite 258).
2. Wählen Sie die Registerkarte Aktionen aus.
3. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.
   - Zugriff verweigern.

     Ist diese Einstellung ausgewählt, verweigert Kaspersky Embedded Systems Security den Zugriff auf das gefundene und möglicherweise infizierte Objekt. Sie können in der Dropdown-Liste weitere Aktionen für gesperrte Objekte auswählen.
   - Weitere Aktion ausführen.

     Wählen Sie in der Dropdown-Liste die Aktion:
     - Desinfizieren.
     - Desinfizieren. Irreparable Objekte löschen.
     - Löschen.
     - Empfohlen.

4. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:

   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.

   - Zugriff verweigern.

     Ist diese Einstellung ausgewählt, verweigert Kaspersky Embedded Systems Security den Zugriff auf das gefundene und möglicherweise infizierte Objekt. Sie können in der Dropdown-Liste weitere Aktionen für gesperrte Objekte auswählen.

   - Weitere Aktion ausführen.

     Wählen Sie in der Dropdown-Liste die Aktion:

     - In Quarantäne verschieben.
     - Löschen.
     - Empfohlen.

5. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen Aktionen je nach Typ des erkannten Objekts ausführen.

      Wenn das Kontrollkästchen aktiviert ist, können Sie für jeden gefundenen Objekttyp einzeln eine primäre und eine sekundäre Aktion festlegen, indem Sie auf die Schaltfläche Einstellungen neben dem Kontrollkästchen klicken. Unabhängig von Ihrer Auswahl gestattet Kaspersky Embedded Systems Security Ihnen nicht, ein infiziertes Objekt zu öffnen oder auszuführen.

      Wenn das Kontrollkästchen deaktiviert ist, führt Kaspersky Embedded Systems Security Aktionen durch, die in den Abschnitten Aktion für infizierte und andere Objekte und Aktion für möglicherweise infizierte Objekte für die jeweils benannten Objekttypen ausgewählt sind.

      Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Klicken Sie auf die Schaltfläche Einstellungen.

   c. Wählen Sie im nächsten Fenster für jeden Typ des gefundenen Objekts die primäre und die sekundäre Aktion (falls die primäre Aktion nicht durchgeführt werden kann) aus.

   d. Klicken Sie auf **OK**.

6. Wählen Sie Aktion für nicht veränderbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen Vom Programm nicht modifizierbare zusammengesetzte Datei vollständig entfernen, wenn ein eingebettetes Objekt gefunden wird.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert das erzwungene Löschen der übergeordneten zusammengesetzten Datei, wenn ein schädliches und möglicherweise infiziertes oder ein anderes untergeordnetes und eingebettetes Objekt gefunden wird.

   Wenn das Kontrollkästchen aktiviert und die Aufgabe so konfiguriert ist, dass infizierte und möglicherweise infizierte Objekte gelöscht werden, erzwingt Kaspersky Embedded Systems Security das Löschen des gesamten übergeordneten zusammengesetzten Objekts, wenn ein schädliches oder ein anderes eingebettetes Objekt gefunden wird. Das erzwungene Löschen einer übergeordneten Datei mit ihrem Gesamtinhalt wird durchgeführt, wenn es dem Programm nicht gelingt, nur das gefundene untergeordnete Objekt zu löschen (zum Beispiel, wenn das übergeordnete Objekt nicht bearbeitet werden kann).

   Wenn das Kontrollkästchen deaktiviert und die Aufgabe so konfiguriert ist, das infizierte und möglicherweise infizierte Objekte gelöscht werden, führt Kaspersky Embedded Systems Security die festgelegte Aktion nicht aus, wenn das übergeordnete Objekt nicht bearbeitet werden kann.

7. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

► *So optimieren Sie die Leistung der Aufgabe zum Echtzeitschutz für Dateien:*

1. Öffnen Sie das Fenster Echtzeitschutz für Dateien **(siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen" auf Seite** 258**)**.
2. Wählen Sie die Registerkarte Optimierung aus.
3. Im Abschnitt Ausnahmen:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Dateien ausschließen.

     Ausnahme von Dateien nach Dateiname oder Dateinamensmaske von der Untersuchung.

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen Objekte bei der Untersuchung.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security alle Objekte.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Nicht erkennen.

     Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie https://encyclopedia.kaspersky.de/knowledge/classification/ .

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen erkennbaren Objekte bei der Untersuchung.

Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security alle Objekte, die im Programm standardmäßig angegeben sind.

Das Kontrollkästchen ist standardmäßig deaktiviert.

- Klicken Sie für jede Einstellung auf die Schaltfläche Ändern, um Ausnahmen hinzuzufügen.

4. Im Abschnitt Erweiterte Einstellungen:

- Untersuchung beenden, wenn sie länger dauert als (Sek.)

  Beschränkung der Untersuchungsdauer für ein Objekt. Als Standard gilt der Wert 60 Sek.

  Wenn dieses Kontrollkästchen aktiviert ist, wird die maximale Untersuchungsdauer für ein Objekt auf den festgelegten Wert begrenzt.

  Wenn dieses Kontrollkästchen deaktiviert ist, gilt keine Beschränkung für die Untersuchungsdauer.

  Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

- Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)

  Ausnahme zusammengesetzter Objekte, die die maximale Größe übersteigen, von der Untersuchung.

  Wenn dieses Kontrollkästchen aktiviert ist, werden zusammengesetzte Objekte, deren Größe über dem festgelegten Wert liegt, von Kaspersky Embedded Systems Security bei der Untersuchung auf Viren übersprungen.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security zusammengesetzte Objekte jeder Größe.

  Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

- iSwift-Technologie verwenden

  iSwift vergleicht die NTFS-ID der Datei, die in einer Datenbank gespeichert ist, mit einer aktuellen ID. Es werden nur Dateien, deren IDs sich geändert haben (neue Dateien und seit der letzten Untersuchung des NTFS-Dateisystems geänderte Dateien), untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte des NTFS-Systems unabhängig vom Erstellungs- oder Änderungsdatum, ausgenommen Dateien aus Netzwerkordnern.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- iChecker-Technologie verwenden

  iChecker berechnet und speichert Prüfsummen von untersuchten Dateien. Wenn ein Objekt geändert wird, ändert sich die Prüfsumme. Das Programm vergleicht alle Prüfsummen während der Untersuchung und untersucht nur neue und seit der letzten Untersuchung veränderte Dateien.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder veränderte Dateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien unabhängig vom Erstellungs- oder Änderungsdatum.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Aufgabe zum Echtzeitschutz für Dateien über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem lokalen Computer konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen

► *Um das Einstellungsfenster des Schutzbereiches für die Aufgabe zum Echtzeitschutz für Dateien zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten Echtzeitschutz für Dateien aus.
3. Klicken Sie im Detailbereich auf den Link Schutzbereich konfigurieren.

   Das Fenster Schutzbereichseinstellungen wird geöffnet.

Aufgabeneinstellungen für den Echtzeitschutz für Dateien öffnen

► *Um das Fenster für die allgemeinen Aufgabeneinstellungen zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten Echtzeitschutz für Dateien aus.
3. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster Aufgabeneinstellungen wird geöffnet.

Aufgabe zum Echtzeitschutz für Dateien anpassen

► *Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "Aufgabeneinstellungen für den Echtzeitschutz für Dateien öffnen" auf Seite 273).
2. Passen Sie auf der Registerkarte Allgemein folgende Aufgabenparameter an:
   - Schutzmodus für Objekte (siehe Abschnitt "**Schutzmodus auswählen**" auf Seite 274)
   - Heuristische Analyse
   - Integration mit anderen Komponenten (siehe Abschnitt "**Heuristische Analyse und Integration mit anderen Programmkomponenten**" auf Seite 275).
3. Geben Sie auf den Registerkarten Zeitplan und Erweitert die geplanten Starteinstellungen an (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160).
4. Klicken Sie im Fenster Aufgabeneinstellungen auf **OK**.

   Die Änderung der Einstellungen wird gespeichert.
5. Klicken Sie im Detailbereich des Knotens Echtzeitschutz für Dateien auf den Link Schutzbereich anpassen.
6. Führen Sie folgende Aktionen aus:
   - Wählen Sie in der Dateistruktur oder Liste der Dateiressourcen des Computers die Knoten oder Elemente aus, die Sie in den Schutzbereich der Aufgabe aufnehmen möchten.
   - Wählen Sie eine der voreingestellten Sicherheitsstufen aus oder passen Sie die Sicherheitseinstellungen der Objekte manuell an (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 461).
7. Klicken Sie im Fenster Schutzbereichseinstellungen auf die Schaltfläche Speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

In diesem Abschnitt

Schutzmodus auswählen

Sie können den Schutzmodus in der Aufgabe Echtzeitschutz für Dateien auswählen. Im Abschnitt Schutzmodus für Objekte können Sie festlegen, bei welcher Art des Zugriffs auf die Objekte Kaspersky Embedded Systems Security eine Untersuchung durchführt.

Die Einstellung Schutzmodus für Objekte hat einen einheitlichen Wert für den gesamten Schutzbereich, der in der Aufgabe vorgegeben ist. Für diese Einstellung können keine unterschiedlichen Werte für einzelne Knoten des Schutzbereichs festgelegt werden.

► *Um den Schutzmodus für Objekte auszuwählen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "Aufgabeneinstellungen für den Echtzeitschutz für Dateien öffnen" auf Seite 273).
2. Wählen Sie im folgenden Fenster auf der Registerkarte Allgemein den Schutzmodus aus, den Sie festlegen möchten:
   - Intelligenter Modus

     Kaspersky Embedded Systems Security wählt die Objekte für die Untersuchung selbstständig aus. Das Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn ein Prozess mehrmals auf das Objekt zugreift und es verändert, untersucht Kaspersky Embedded Systems Security das Objekt erst dann erneut, wenn es von diesem Prozess zum letzten Mal gespeichert wird.
   - Beim Öffnen und Ändern

     Kaspersky Embedded Systems Security untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern.

     Diese Variante gilt als Standard.
   - Beim Öffnen

     Kaspersky Embedded Systems Security untersucht alle Objekte, wenn diese zum Lesen, zur Ausführung oder zum Ändern geöffnet werden.
   - Beim Ausführen

     Kaspersky Embedded Systems Security untersucht die Datei nur beim Öffnen zum Ausführen.
3. Klicken Sie auf **OK**.

Der ausgewählte Schutzmodus für die Objekte wird eingestellt.

Heuristische Analyse und Integration mit anderen Programmkomponenten

Die Aufgabe "Verwendung von KSN" kann nur gestartet werden, wenn die Erklärung zu Kaspersky Security Network akzeptiert wurde.

► *Um die heuristische Analyse und Integration mit anderen Programmkomponenten zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "**Aufgabeneinstellungen für den Echtzeitschutz für Dateien öffnen**" auf Seite 273).
2. Deaktivieren oder aktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen Heuristische Analyse verwenden.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der heuristischen Analyse bei der Objektuntersuchung.

   Wenn dieses Kontrollkästchen aktiviert ist, ist die heuristische Analyse aktiviert.

   Wurde dieses Kontrollkästchen deaktiviert, ist die heuristische Analyse deaktiviert.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

3. Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.

   Mit dem Schieberegler lässt sich die Stufe die Ebene der heuristischen Analyse regulieren. Die Genauigkeitsstufe der Untersuchung regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach Bedrohungen, dem Auslastungsniveau der Betriebssystemressourcen und der Untersuchungsdauer.

   Für die Untersuchung sind folgende Genauigkeitsstufen vorgesehen:

   - Oberflächlich. Bei der heuristischen Analyse wird eine relativ geringe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. In diesem Modus besteht eine geringere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung beansprucht weniger Systemressourcen und wird schneller ausgeführt.
   - Mittel. Die Anzahl der Befehle, die bei der heuristischen Analyse in der ausführbaren Datei ausgeführt werden, richtet sich nach den Empfehlungen der Kaspersky-Lab-Experten.

     Diese Stufe gilt als Standard.
   - Tief. Bei der heuristischen Analyse wird eine relativ hohe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. Bei dieser Einstellung besteht eine höhere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung benötigt mehr Systemressourcen und mehr Zeit und kann eine erhöhte Anzahl an Fehlalarmen auslösen.

     Der Schieberegler ist aktiv, wenn das Kontrollkästchen Heuristische Analyse verwenden aktiviert ist.

4. Konfigurieren Sie im Abschnitt Integration mit anderen Komponenten die folgenden Einstellungen:

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen Vertrauenswürdige Zone anwenden.

     Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

     Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

     Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs für die Aufgabe.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Klicken Sie auf den Link **Vertrauenswürdige Zone**, um die Einstellungen der vertrauenswürdigen Zone zu öffnen.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen KSN zum Schutz verwenden.

     Mit diesem Kontrollkästchen wird die Verwendung der KSN-Dienste aktiviert und deaktiviert.

     Wenn das Kontrollkästchen aktiviert ist, verwendet das Programm die Daten von Kaspersky Security Network um sicherzustellen, dass das Programm schneller auf neue Bedrohungen reagiert und die Wahrscheinlichkeit von Fehlalarmen verringert wird.

     Ist das Kontrollkästchen deaktiviert, werden die KSN-Dienste von der Aufgabe nicht verwendet.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Dieses Feld wird angezeigt, wenn das Kontrollkästchen Daten über untersuchte Dateien senden in den Aufgabeneinstellungen für die Verwendung von KSN aktiviert ist.

- Aktivieren oder deaktivieren Sie das Kontrollkästchen Zugriff auf freigegebene Netzwerkordner für Computer blockieren, die bösartige Aktivität zeigen.

5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden angewandt.

Einstellungen des Zeitplans für den Aufgabenstart anpassen

In der Programmkonsole können Sie den Startzeitplan für lokale Systemaufgaben und benutzerdefinierte Aufgaben anpassen. Für den Start von Gruppenaufgaben kann der Zeitplan nicht angepasst werden.

► *Um die Zeitplan-Einstellungen für den Aufgabenstart anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Kontextmenü des Namens der Aufgabe, deren Startzeitplan angepasst werden soll.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster Aufgabeneinstellungen wird geöffnet.
3. Aktivieren Sie im folgenden Fenster auf der Registerkarte Zeitplan das Kontrollkästchen Aufgabe nach Zeitplan starten.
4. Passen Sie die Zeitplaneinstellungen entsprechend Ihren Anforderungen an. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie unter Startintervall einen der folgenden Werte aus:
      - Stündlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Stunden gestartet wird, wobei Sie die Anzahl der Stunden im Feld Alle **<Anzahl>** Std. eingeben müssen.
      - Täglich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Tagen gestartet wird, wobei Sie die Anzahl der Tage im Feld Alle **<Anzahl>** Tage eingeben müssen.
      - Wöchentlich, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl von Wochen gestartet wird, wobei Sie die Anzahl der Wochen im Feld Alle **<Anzahl>** Wochen eingeben müssen. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (Standardmäßig werden Aufgaben montags gestartet).
      - Bei Programmstart, wenn Sie möchten, dass die Aufgabe bei jedem Start von Kaspersky Embedded Systems Security ausgeführt wird.
      - Nach dem Update der Programm-Datenbanken, wenn Sie möchten, dass die Aufgabe nach jedem Update der Programm-Datenbanken gestartet wird.

   b. Legen Sie im Feld Startzeit die Uhrzeit des erstmaligen Aufgabenstarts fest.
   c. Tragen Sie im Feld Startdatum das Startdatum des Zeitplans ein.

Nachdem Sie das Startintervall der Aufgabe, die Uhrzeit für den erstmaligen Aufgabenstart und das Datum, ab dem der Zeitplan gelten soll, angegeben haben, wird im oberen Bereich des Fensters im Feld Nächster Start der berechnete Zeitpunkt des nächsten Aufgabenstarts angezeigt. Aktualisierte Informationen über die Zeit, die bis zum nächsten Start verbleibt, werden jedes Mal angezeigt, wenn Sie das Fenster Aufgabeneinstellungen auf der Registerkarte Zeitplan öffnen.
Der Wert Durch Richtlinie verboten im Feld Nächster Start wird angezeigt, wenn der Start von Systemaufgaben nach Zeitplan durch die Einstellungen der geltenden Richtlinie von Kaspersky Security Center festgelegt wird.

5. Passen Sie auf der Registerkarte Erweitert die folgenden Zeitplaneinstellungen gemäß Ihren Anforderungen an.
   - Im Abschnitt Einstellungen für das Anhalten der Aufgabe:
     a. Aktivieren Sie das Kontrollkästchen Dauer und geben Sie die erforderliche Anzahl an Stunden und Minuten in den Feldern rechts davon ein, um so die maximale Dauer der Aufgabenausführung vorzugeben.
     b. Aktivieren Sie das Kontrollkästchen Anhalten von und geben Sie die Anfangszeit und Endzeit des Zeitintervalls in den Feldern rechts davon ein, um einen Zeitraum innerhalb von 24 Stunden anzugeben, in dem die Aufgabenausführung angehalten wird.
   - Im Abschnitt Erweiterte Einstellungen:
     a. Aktivieren Sie das Kontrollkästchen Zeitplan deaktivieren ab und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.
     b. Aktivieren Sie das Kontrollkästchen Übersprungene Aufgaben starten, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.
     c. Aktivieren Sie das Kontrollkästchen Aufgabenstart zufällig wählen innerhalb von und geben Sie einen Wert in Minuten ein.
6. Klicken Sie auf **OK**.

Die Einstellungen im Zeitplan für den Start der ausgewählten Aufgabe werden gespeichert.

Schutzbereich erstellen

Dieser Abschnitt enthält Informationen über die Einrichtung und Nutzung eines Schutzbereichs in der Aufgabe Echtzeitschutz für Dateien und dessen weitere Verwendung.

In diesem Abschnitt

Schutzbereich erstellen

Die Vorgehensweise beim Erstellen des Schutzbereichs in der Aufgabe zum Echtzeitschutz für Dateien hängt vom Typ der Anzeige der freigegebenen Netzwerkordner ab (siehe Abschnitt "Über den Schutzbereich von Aufgaben und Sicherheitseinstellungen" auf Seite 250). Sie können die Anzeige der freigegebenen Netzwerkordner in Form einer Liste (wird standardmäßig verwendet) oder in Form einer Baumstruktur festlegen.

Um auf die Aufgabe neue Einstellungen des Schutzbereichs anzuwenden, muss die Aufgabe zum Echtzeitschutz für Dateien neu gestartet werden.

► *Um mithilfe der Struktur der freigegebenen Netzwerkordner einen Schutzbereich zu erstellen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Öffnen Sie im rechten Teil des geöffneten Fensters die Struktur mit den freigegebenen Netzwerkordnern des Computers, um alle Knoten anzuzeigen.
3. Führen Sie folgende Aktionen aus:
   - Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Schutzbereich ausschließen möchten.
   - Deaktivieren Sie das Kontrollkästchen Arbeitsplatz, um einzelne Knoten in den Schutzbereich einzuschließen, und gehen Sie wie folgt vor:
     - Um alle Laufwerke eines bestimmten Typs in den Schutzbereich aufzunehmen, aktivieren Sie das Kontrollkästchen neben dem Namen des entsprechenden Laufwerkstyps (z. B. um alle Wechseldatenträger auf dem Computer einzuschließen, aktivieren Sie das Kontrollkästchen Wechseldatenträger).
     - Um ein einzelnes Laufwerk eines bestimmten Typs in den Schutzbereich aufzunehmen, öffnen Sie den Knoten, der die Liste dieses Laufwerkstyps enthält, und aktivieren Sie das Kontrollkästchen für das entsprechende Laufwerk. Um beispielsweise den Wechseldatenträger F: auszuwählen, öffnen Sie den Knoten Wechseldatenträger und aktivieren Sie das Kontrollkästchen für Laufwerk **F:**.
     - Wenn Sie nur einen einzelnen Ordner oder eine einzelne Datei auf dem Laufwerk in den Schutzbereich einschließen möchten, aktivieren Sie das Kontrollkästchen neben dem Namen dieses Ordners bzw. dieser Datei.
4. Klicken Sie auf die Schaltfläche Speichern.

Das Einstellungsfenster des Schutzbereichs wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

► *Um mithilfe der Liste der freigegebenen Netzwerkordner einen Schutzbereich zu erstellen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Deaktivieren Sie das Kontrollkästchen Arbeitsplatz, um einzelne Knoten in den Schutzbereich einzuschließen, und gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü des Schutzbereichs mit der rechten Maustaste.
   b. Wählen Sie im Kontextmenü der Tabelle den Punkt Schutzbereich hinzufügen aus.
   c. Wählen Sie im geöffneten Fenster Schutzbereich hinzufügen den Typ des Objektes aus, das Sie zum Schutzbereich hinzufügen möchten:
      - Vordefinierter Bereich, wenn Sie in den Schutzbereich einen der vordefinierten Bereiche auf dem Computer aufnehmen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Schutzbereich aus.
      - Laufwerk, Ordner oder Netzwerkobjekt, wenn Sie in den Schutzbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Gültigkeitsbereich über die Schaltfläche Durchsuchen aus.
      - Datei, wenn Sie in den Schutzbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Gültigkeitsbereich über die Schaltfläche Durchsuchen aus.

   Sie können ein Objekt nicht zum Schutzbereich hinzufügen, wenn es bereits als Ausnahme aus dem Schutzbereich hinzugefügt wurde.
3. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Schutzbereich ausschließen möchten, oder gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü des Schutzbereichs mit der rechten Maustaste.
   b. Wählen Sie im Kontextmenü den Punkt Ausnahme hinzufügen.
   c. Wählen Sie im geöffneten Fenster Ausnahme hinzufügen den Typ des Objektes aus, das Sie als Ausnahme aus dem Schutzbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Schutzbereich.
4. Um den Schutzbereich oder eine hinzugefügte Ausnahme zu ändern, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option Bereich ändern.
5. Um die Anzeige eines zuvor hinzugefügten Schutzbereichs bzw. einer Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option Aus Liste löschen aus.

   Der Schutzbereich wird aus dem Gültigkeitsbereich der Aufgabe zum Echtzeitschutz für Dateien bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner ausgeschlossen.
6. Klicken Sie auf die Schaltfläche Speichern.

Das Einstellungsfenster des Schutzbereichs wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Die Aufgabe *Echtzeitschutz für Dateien* kann gestartet werden, wenn mindestens ein Knoten der Struktur der Dateiressourcen des Computers in den Schutzbereich aufgenommen wurde.

Wenn Sie einen ungültigen Schutzbereich angeben, Sie beispielsweise verschiedene Sicherheitsparameterwerte für viele einzelne Knoten in der Dateistruktur des Computers setzen, so kann dadurch die Untersuchung der Objekte bei Zugriff verlangsamt werden.

Virtuellen Schutzbereich erstellen

Sie können separate virtuelle Festplatten, Ordner oder Dateien nur dann zum Schutzbereich bzw. Untersuchungsbereich hinzufügen, wenn der Schutzbereich bzw. Untersuchungsbereich in Form einer Struktur der Dateiressourcen angezeigt wird (siehe Abschnitt "Einstellungen für die Anzeige der freigegebenen Netzwerkordner des Untersuchungsbereichs anpassen" auf Seite 456).

► *Um eine virtuelle Festplatte zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Wählen Sie im linken unteren Teil des Fensters aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.
3. Öffnen Sie das Kontextmenü des Knotens Virtuelle Festplatten.
4. Wählen Sie die Option Virtuelle Festplatte hinzufügen aus.
5. Wählen Sie in der Liste der verfügbaren Namen den Namen für die gerade entstehende virtuelle Festplatte aus.
6. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Datenträger, um diesen Datenträger in den Schutzbereich zu übernehmen.
7. Klicken Sie im Fenster Schutzbereichseinstellungen auf die Schaltfläche Speichern.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

► *Um einen virtuellen Ordner oder eine virtuelle Datei zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Wählen Sie im linken unteren Teil des Fensters aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.

3. Öffnen Sie das Kontextmenü der virtuellen Festplatte, der Sie den Ordner oder die Datei hinzufügen möchten, und wählen Sie einen der folgenden Punkte aus:
   - Virtuellen Ordner hinzufügen, wenn Sie einen virtuellen Ordner zum Schutzbereich hinzufügen möchten.
   - Virtuelle Datei hinzufügen, wenn Sie eine virtuelle Datei zum Schutzbereich hinzufügen möchten.
4. Tragen Sie im Eingabefeld den Namen für den Ordner bzw. die Datei ein.
5. In der Zeile mit dem Namen des erstellten Ordners bzw. der erstellten Datei aktivieren Sie das Kontrollkästchen, um den Ordner bzw. die Datei in den Schutzbereich zu übernehmen.
6. Klicken Sie im Fenster Schutzbereichseinstellungen auf die Schaltfläche Speichern.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

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 (siehe Abschnitt "Vordefinierte Sicherheitsstufen " auf S. 252).

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des Computers oder den Knoten in der Struktur festlegen.

Bei der Arbeit mit der Struktur der Dateiressourcen auf dem Server 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.

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

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Wählen Sie im linken Bereich des Fensters den Knoten, dessen Sicherheitsanstellungen Sie konfigurieren möchten.

   Für einen ausgewählten Knoten oder ein Element im Schutzbereich kann eine vordefinierte Vorlage mit Sicherheitseinstellungen übernommen werden (siehe Abschnitt "Über Vorlagen für Sicherheitseinstellungen" auf Seite 167).

3. Passen Sie die Sicherheitseinstellungen des ausgewählten Knotens oder Elements entsprechend ihren Anforderungen an:
   - Allgemeine Einstellungen (siehe Abschnitt "**Allgemeine Aufgabeneinstellungen anpassen**" auf Seite 283)
   - Aktionen (siehe Abschnitt "**Aktionen anpassen**" auf Seite 286)
   - Optimierung (siehe Abschnitt "**Leistung optimieren**" auf Seite 288)
4. Klicken Sie im Fenster Schutzbereichseinstellungen auf die Schaltfläche Speichern.

Die neuen Einstellungen des Schutzbereichs werden gespeichert.

In diesem Abschnitt

Allgemeine Aufgabeneinstellungen anpassen

► *So passen Sie die allgemeinen Sicherheitseinstellungen der Aufgabe zum Echtzeitschutz für Dateien an:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Wählen Sie die Registerkarte Allgemein aus.
3. Geben Sie im Abschnitt Schutz von Objekten die Objekte an, die Sie in den Schutzbereich einschließen möchten:
   - Alle Objekte

     Kaspersky Embedded Systems Security untersucht alle Objekte.
   - Objekte, die nach Format untersucht werden

     Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats.

     Die Liste der Dateiformate wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
   - Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden

     Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung.

     Die Erweiterungsliste wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
   - Objekte, die nach der angegebenen Erweiterungsliste untersucht werden

     Kaspersky Embedded Systems Security untersucht Dateien auf der Grundlage der Dateierweiterung. Die Dateierweiterungsliste können Sie im Fenster Erweiterungsliste mithilfe der Schaltfläche Ändern manuell anpassen.
   - Bootsektoren und MBR

     Aktivierung des Schutzes für Laufwerk-Bootsektoren und Master Boot Records (MBR)

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security die Bootsektoren und Master Boot Records auf Festplatten und Wechseldatenträgern des Computers.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Alternative NTFS-Ströme

  Untersuchung zusätzlicher Ströme von Dateien und Ordnern auf den Laufwerken des NTFS-Dateisystems.

  Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm ein möglicherweise infiziertes Objekt und alle NTFS-Streams, die mit diesem Objekte verbunden sind.

  Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm nur das Objekt, das gefunden und als möglicherweise infiziert betrachtet wurde.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Aktivieren oder deaktivieren Sie im Abschnitt Optimierung das Kontrollkästchen Nur neue und veränderte Dateien schützen.

   Mit diesem Kontrollkästchen werden die Untersuchung und der Schutz von Dateien, die Kaspersky Embedded Systems Security als neu oder seit der letzten Untersuchung geändert erkennt, aktiviert oder deaktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, untersucht und schützt Kaspersky Embedded Systems Security nur die Dateien, die als neu oder seit der letzten Untersuchung verändert erkannt wurden.

   Wenn das Kontrollkästchen deaktiviert ist, können Sie auswählen, ob Sie nur neue Dateien oder alle Dateien unabhängig von deren Änderungsstatus untersuchen möchten.

   Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert. Wurde die Sicherheitsstufe Maximale Sicherheit oder Empfohlen ausgewählt, ist das Kontrollkästchen deaktiviert.

Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

5. Geben Sie im Abschnitt Schutz von zusammengesetzten Objekten die zusammengesetzten Objekte an, die Sie in den Schutzbereich einschließen möchten:

   - **Alle /** nur neue Archive

     Untersuchung von Archiven in den Formaten ZIP, CAB, RAR, ARJ u. a.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Schutzebene abhängig.

   - **Alle /** Nur neue SFX-Archive

     Selbstentpackende Archive untersuchen.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security SFX-Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Schutzebene abhängig.

     Diese Einstellung ist aktiv, wenn das Kontrollkästchen Archive deaktiviert ist.

- **Alle /** Nur neue E-Mail-Datenbanken

  Dateien in Mail-Datenbanken für Microsoft Outlook und Microsoft Outlook Express werden untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Mail-Datenbankdateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Mail-Datenbankdateien von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** nur neue gepackte Objekte

  Untersuchung von ausführbaren Dateien, die mit Packprogrammen für Binärcode wie beispielsweise UPX oder ASPack gepackt wurden.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security ausführbare Dateien, die mit Packprogrammen gepackt wurden.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden ausführbare Dateien, die mit Packprogrammen gepackt wurden, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

- **Alle /** nur neue Dateien in Mail-Formaten

  Dateien in Mail-Formaten werden untersucht. Dazu zählen beispielsweise Nachrichten der Formate Microsoft Outlook und Microsoft Outlook Express.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien in Mail-Formaten.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Dateien in Mail-Formaten von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** Nur neue eingebettete OLE-Objekte

  Untersuchung von Objekten, die in eine Datei eingebettet sind (beispielsweise Excel-Tabellen, Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten).

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte, die in eine Datei eingebettet sind.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Objekte, die in eine Datei eingebettet sind, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

6. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

► *So passen Sie die Aktionen für infizierte und andere gefundene Objekte für die Aufgabe zum Echtzeitschutz für Dateien an:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Wählen Sie die Registerkarte Aktionen aus.
3. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.
   - Zugriff verweigern.

     Ist diese Einstellung ausgewählt, verweigert Kaspersky Embedded Systems Security den Zugriff auf das gefundene und möglicherweise infizierte Objekt. Sie können in der Dropdown-Liste weitere Aktionen für gesperrte Objekte auswählen.
   - Weitere Aktion ausführen.

     Wählen Sie in der Dropdown-Liste die Aktion:
     - Desinfizieren.
     - Desinfizieren. Irreparable Objekte löschen.
     - Löschen.
     - Empfohlen.
4. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.
   - Zugriff verweigern.

     Ist diese Einstellung ausgewählt, verweigert Kaspersky Embedded Systems Security den Zugriff auf das gefundene und möglicherweise infizierte Objekt. Sie können in der Dropdown-Liste weitere Aktionen für gesperrte Objekte auswählen.

- Weitere Aktion ausführen.

  Wählen Sie in der Dropdown-Liste die Aktion:

  - In Quarantäne verschieben.
  - Löschen.
  - Empfohlen.

5. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen Aktionen je nach Typ des erkannten Objekts ausführen.

      Wenn das Kontrollkästchen aktiviert ist, können Sie für jeden gefundenen Objekttyp einzeln eine primäre und eine sekundäre Aktion festlegen, indem Sie auf die Schaltfläche Einstellungen neben dem Kontrollkästchen klicken. Unabhängig von Ihrer Auswahl gestattet Kaspersky Embedded Systems Security Ihnen nicht, ein infiziertes Objekt zu öffnen oder auszuführen.

      Wenn das Kontrollkästchen deaktiviert ist, führt Kaspersky Embedded Systems Security Aktionen durch, die in den Abschnitten Aktion für infizierte und andere Objekte und Aktion für möglicherweise infizierte Objekte für die jeweils benannten Objekttypen ausgewählt sind.

      Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Klicken Sie auf die Schaltfläche Einstellungen.

   c. Wählen Sie im nächsten Fenster für jeden Typ des gefundenen Objekts die primäre und die sekundäre Aktion (falls die primäre Aktion nicht durchgeführt werden kann) aus.

   d. Klicken Sie auf **OK**.

6. Wählen Sie Aktion für nicht veränderbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen Vom Programm nicht modifizierbare zusammengesetzte Datei vollständig entfernen, wenn ein eingebettetes Objekt gefunden wird.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert das erzwungene Löschen der übergeordneten zusammengesetzten Datei, wenn ein schädliches und möglicherweise infiziertes oder ein anderes untergeordnetes und eingebettetes Objekt gefunden wird.

   Wenn das Kontrollkästchen aktiviert und die Aufgabe so konfiguriert ist, dass infizierte und möglicherweise infizierte Objekte gelöscht werden, erzwingt Kaspersky Embedded Systems Security das Löschen des gesamten übergeordneten zusammengesetzten Objekts, wenn ein schädliches oder ein anderes eingebettetes Objekt gefunden wird. Das erzwungene Löschen einer übergeordneten Datei mit ihrem Gesamtinhalt wird durchgeführt, wenn es dem Programm nicht gelingt, nur das gefundene untergeordnete Objekt zu löschen (zum Beispiel, wenn das übergeordnete Objekt nicht bearbeitet werden kann).

   Wenn das Kontrollkästchen deaktiviert und die Aufgabe so konfiguriert ist, das infizierte und möglicherweise infizierte Objekte gelöscht werden, führt Kaspersky Embedded Systems Security die festgelegte Aktion nicht aus, wenn das übergeordnete Objekt nicht bearbeitet werden kann.

7. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

► *So optimieren Sie die Leistung der Aufgabe zum Echtzeitschutz für Dateien:*

1. Öffnen Sie das Fenster Einstellungen des Schutzbereichs (siehe Abschnitt "Einstellungen für den Schutzbereich des Echtzeitschutzes für Dateien öffnen" auf Seite 273).
2. Wählen Sie die Registerkarte Optimierung aus.
3. Im Abschnitt Ausnahmen:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Dateien ausschließen.

     Ausnahme von Dateien nach Dateiname oder Dateinamensmaske von der Untersuchung.

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen Objekte bei der Untersuchung.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security alle Objekte.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Nicht erkennen.

     Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie https://encyclopedia.kaspersky.de/knowledge/classification/ .

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen erkennbaren Objekte bei der Untersuchung.

     Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security alle Objekte, die im Programm standardmäßig angegeben sind.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Klicken Sie für jede Einstellung auf die Schaltfläche Ändern, um Ausnahmen hinzuzufügen.
4. Im Abschnitt Erweiterte Einstellungen:
   - Untersuchung beenden, wenn sie länger dauert als (Sek.)

     Beschränkung der Untersuchungsdauer für ein Objekt. Als Standard gilt der Wert 60 Sek.

     Wenn dieses Kontrollkästchen aktiviert ist, wird die maximale Untersuchungsdauer für ein Objekt auf den festgelegten Wert begrenzt.

     Wenn dieses Kontrollkästchen deaktiviert ist, gilt keine Beschränkung für die Untersuchungsdauer.

     Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

- Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)

  Ausnahme zusammengesetzter Objekte, die die maximale Größe übersteigen, von der Untersuchung.

  Wenn dieses Kontrollkästchen aktiviert ist, werden zusammengesetzte Objekte, deren Größe über dem festgelegten Wert liegt, von Kaspersky Embedded Systems Security bei der Untersuchung auf Viren übersprungen.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security zusammengesetzte Objekte jeder Größe.

  Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

- iSwift-Technologie verwenden

  iSwift vergleicht die NTFS-ID der Datei, die in einer Datenbank gespeichert ist, mit einer aktuellen ID. Es werden nur Dateien, deren IDs sich geändert haben (neue Dateien und seit der letzten Untersuchung des NTFS-Dateisystems geänderte Dateien), untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte des NTFS-Systems unabhängig vom Erstellungs- oder Änderungsdatum, ausgenommen Dateien aus Netzwerkordnern.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- iChecker-Technologie verwenden

  iChecker berechnet und speichert Prüfsummen von untersuchten Dateien. Wenn ein Objekt geändert wird, ändert sich die Prüfsumme. Das Programm vergleicht alle Prüfsummen während der Untersuchung und untersucht nur neue und seit der letzten Untersuchung veränderte Dateien.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder veränderte Dateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien unabhängig vom Erstellungs- oder Änderungsdatum.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Statistik für die Aufgabe zum Echtzeitschutz für Dateien

Während die Aufgabe zum Echtzeitschutz für Dateien ausgeführt wird, können Sie in Echtzeit Informationen über die Anzahl der Objekte, die Kaspersky Embedded Systems Security seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen lassen.

► *Um die Statistik der Aufgabe Echtzeitschutz für Dateien anzusehen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten Echtzeitschutz für Dateien aus.

Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt Statistik eine Statistik der Aufgabe angezeigt.

Sie können Informationen über Objekte anzeigen, die Kaspersky Embedded Systems Security seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat (siehe Tabelle unten):

Tabelle 43. Statistik für die Aufgabe zum Echtzeitschutz für Dateien

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 dieselbe Schadsoftware, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Infizierte und andere gefundene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security als infiziert eingestuft hat, oder gefundene legale Software, die von Eindringlingen verwendet werden kann, um Ihren Computer oder persönliche Daten zu beschädigen.
Möglicherweise infizierte Objekte gefunden	Anzahl der von Kaspersky Embedded Systems Security gefundenen Objekte, die als möglicherweise infiziert eingestuft wurden
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security aus folgenden Gründen nicht desinfiziert wurden: • Der Typ des gefundenen Objekts kann nicht desinfiziert werden • Bei der Desinfektion ist eine Störung aufgetreten
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos versucht hat, in die Quarantäne zu verschieben, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Nicht gelöschte 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 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 anders Programm gesperrt war.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu kopieren versucht hat, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Verarbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.

Feld	Beschreibung
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden.
In Quarantäne verschoben	Anzahl der Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Embedded Systems Security im Backup gespeichert wurden.
Gelöschte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security entfernt 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.
Verarbeitete Objekte	Objekte insgesamt, die von Kaspersky Embedded Systems Security verarbeitet wurden.

Sie können auch eine Statistik über die Ausführung der Aufgabe zum Echtzeitschutz für Dateien im Protokoll der Aufgabenausführung über den Link Protokoll der Aufgabenausführung öffnen im Abschnitt Verwaltung des Detailbereichs anzeigen.

Wenn der Wert im Feld Anzahl der Ereignisse im Fenster des Protokolls der Aufgabenausführung zum Echtzeitschutz für Dateien größer als 0 ist, wird empfohlen, die Ereignisse im Protokoll der Aufgabenausführung auf der Registerkarte Ereignisse manuell zu bearbeiten.

Verwendung von KSN

Dieser Abschnitt informiert über die Aufgabe Verwendung von KSN und erläutert die Konfiguration dieser Aufgabe.

In diesem Kapitel

Über die Aufgabe "Verwendung von KSN"

Kaspersky Security Network (im Weiteren auch KSN) ist eine Infrastruktur von Online-Diensten, die den umfassenden Zugriff auf die Kaspersky Lab-Wissensdatenbank über die Reputation von Dateien, Web-Ressourcen und Programmen gewährleistet. Die Nutzung der Daten des Kaspersky Security Network gewährleistet eine schnellere Reaktion von Kaspersky Embedded Systems Security auf neue Bedrohungen, erhöht die Effektivität der Arbeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

Die Aufgabe "Verwendung von KSN" kann nur gestartet werden, wenn die Erklärung zu Kaspersky Security Network akzeptiert wurde.

Kaspersky Embedded Systems Security erhält von Kaspersky Security Network ausschließlich Informationen über die Reputation von Programmen.

Die Teilnahme von Benutzern an KSN ermöglicht es Kaspersky Lab, schnell Informationen über Typen und Quellen neuer Bedrohungen zu erhalten, Neutralisierungsmethoden zu entwickeln und die Anzahl an Fehlalarmen der Programmkomponenten zu reduzieren.

Ausführliche Informationen über die Übertragung, Verarbeitung, Speicherung und Vernichtung von Daten über die Programmnutzung finden Sie im Fenster **Datenverarbeitung** der Aufgabe "Verwendung von KSN" sowie in der Datenschutzrichtlinie auf der Website von Kaspersky Lab.

Die Teilnahme an Kaspersky Security Network ist freiwillig. Sie können nach der Installation von Kaspersky Embedded Systems Security entscheiden, ob Sie an Kaspersky Security Network teilnehmen möchten. Sie können

Ihre Entscheidung über die Teilnahme an Kaspersky Security Network jederzeit ändern.

Das Kaspersky Security Network kann in den folgenden Aufgaben von Kaspersky Embedded Systems Security verwendet werden:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Kontrolle des Programmstarts

Kaspersky Private Security Network

Ausführliche Informationen über die Konfiguration von Kaspersky Private Security Network (im Weiteren "Private KSN") finden Sie im *Hilfesystem von Kaspersky Security Center*.

Wenn Sie Private KSN auf dem geschützten Computer verwenden, können Sie im Fenster **Datenverarbeitung** (siehe Abschnitt "Datenverarbeitung über das Verwaltungs-Plug-in konfigurieren" auf Seite 297) der Aufgabe zur Verwendung von KSN die KSN-Erklärung lesen und die Aufgabe mithilfe des Kontrollkästchens **Ich akzeptiere die Kaspersky Private Security Network-Erklärung** aktivieren. Indem Sie die Bedingungen akzeptieren, erklären Sie sich damit einverstanden, dass alle Datentypen, die in der KSN-Erklärung genannt werden (Sicherheitsanfragen, Statistikdaten), an den KSN-Dienst gesendet werden.

Nach der Annahme der Private-KSN-Bedingungen sind die Kontrollkästchen für die Verwendung von Global KSN nicht mehr verfügbar.

Wenn Sie Private KSN deaktivieren, während die Aufgabe "Verwendung von KSN" läuft, wird der Fehler *Lizenzverletzung* angezeigt und die Aufgabe beendet. Um den Computer weiterhin zu schützen, müssen Sie die KSN-Erklärung manuell im Fenster **Datenverarbeitung** annehmen und die Aufgabe neu starten.

Widerrufen der Zustimmung zur KSN-Erklärung

Sie können jederzeit Ihre Zustimmung widerrufen und den Datenaustausch mit dem Kaspersky Security Network beenden. Die folgenden Aktionen werden als vollständiger oder teilweiser Widerruf der KSN-Erklärung angesehen:

- Deaktivieren des Kontrollkästchens **Daten über untersuchte Dateien senden**: Das Programm stellt das Senden von Prüfsummen untersuchter Dateien zu Analysezwecken an den KSN-Dienst ein.
- Deaktivieren des Kontrollkästchens **Statistiken zu Kaspersky Security Network senden**: Das Programm stellt die Aufbereitung von Daten mit zusätzlichen KSN-Statistiken ein.
- Deaktivieren des Kontrollkästchens **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network**: Das Programm stellt jegliche KSN-bezogene Datenverarbeitung ein und die Aufgabe "Verwendung von KSN" wird gestoppt.
- Deinstallation der Komponente "Verwendung von KSN": Jegliche Verarbeitung KSN-bezogener Daten wird gestoppt.
- Deinstallation von Kaspersky Embedded Systems Security: Jegliche Verarbeitung KSN-bezogener Daten wird gestoppt.

Standardeinstellungen der Aufgabe "Verwendung von KSN"

Sie können die Standard-Einstellungen der Aufgabe "Verwendung von KSN" anpassen (siehe Tabelle unten).

Tabelle 44. Standardeinstellungen der Aufgabe "Verwendung von KSN"

Einstellung	Standardwert	Beschreibung
Aktion für Objekte, die in KSN nicht vertrauenswürdig sind	Löschen	Sie können die Aktionen festlegen, die Kaspersky Embedded Systems Security in Bezug auf Objekte ausführen soll, die laut KSN als nicht vertrauenswürdig eingestuft sind.
Versand von Daten	Die Prüfsumme der Datei (MD5-Hash) wird für Dateien berechnet, deren Größe nicht mehr als 2 MB beträgt.	Sie können die maximale Dateigröße angeben, bis zu der die Prüfsumme nach dem Algorithmus MD5 für den Versand an KSN berechnet werden soll. Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security den MD5-Hash für Dateien beliebiger Größe.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.
Kaspersky Security Center als KSN-Proxyserver verwenden	Aktiviert	Standardmäßig werden die Daten über Kaspersky Security Center an KSN gesendet. Sie können diese Einstellung nur über das Verwaltungs-Plug-in ändern.
Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network	Deaktiviert	Wenn diese Option ausgewählt ist, wird die Teilnahme an KSN nach der Installation gewährt. Sie können Ihre Entscheidung jederzeit ändern.
Statistiken zu Kaspersky Security Network senden	Ausgewählt (wird nur angewendet, wenn die KSN-Erklärung akzeptiert wurde)	Wenn die KSN-Erklärung akzeptiert wurde, wird die KSN-Statistik automatisch gesendet, wenn Sie dieses Kontrollkästchen nicht deaktivieren.
Daten über untersuchte Dateien senden	Ausgewählt (wird nur angewendet, wenn die KSN-Erklärung akzeptiert wurde)	Wenn die KSN-Erklärung akzeptiert wird, werden die Daten bezüglich Dateien, die untersucht und analysiert wurden, seit die Aufgabe gestartet wurde, automatisch gesendet. Sie können das Kontrollkästchen jederzeit deaktivieren.
Daten über untersuchte URLs senden	Ausgewählt (wird nur angewendet, wenn die KSN-Erklärung akzeptiert wurde)	Wenn die KSN-Erklärung akzeptiert wird, sendet das Programm Informationen über die aufgerufenen URLs an Kaspersky Lab.
Bedingungen der Erklärung zu Kaspersky Managed Protection akzeptieren	Deaktiviert	Sie können den KMP-Dienst aktivieren oder deaktivieren. Dieser Dienst ist nur verfügbar, wenn beim Kauf des Programms der zusätzliche Lizenzvertrag unterzeichnet wurde.

Verwendung von KSN über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe zur Verwendung von KSN und die Datenverwaltung über das Verwaltungs-Plug-in konfigurieren.

In diesem Abschnitt

Aufgabe zur Verwendung von KSN über das Verwaltungs-Plug-in konfigurieren

► *Um die Einstellungen der Aufgabe Verwendung von KSN zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Echtzeit-Computerschutz** auf die Schaltfläche **Einstellungen** im Block **Verwendung von KSN**.

   Das Fenster **Verwendung von KSN** wird geöffnet.
5. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:
   - Geben Sie im Abschnitt **Aktion für Objekte, die in KSN nicht vertrauenswürdig sind** die Aktion an, die Kaspersky Embedded Systems Security ausführen soll, wenn ein Objekt gefunden wird, das laut KSN als nicht vertrauenswürdig eingestuft ist:
     - **Löschen**

       Kaspersky Embedded Systems Security löscht das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, und verschiebt eine Kopie davon ins Backup.

       Diese Variante gilt als Standard.

- **Informationen protokollieren**

  Kaspersky Embedded Systems Security nimmt Informationen über das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, in das Protokoll der Aufgabenausführung auf. Das nicht vertrauenswürdige Objekt wird von Kaspersky Embedded Systems Security nicht gelöscht.

- Begrenzen Sie im Abschnitt **Versand von Daten** die Größe der Dateien, für die eine Prüfsumme berechnet werden soll:
  - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Keine Prüfsumme für den Versand an KSN berechnen für Dateien, die größer sind als (MB)**.

    Über dieses Kontrollkästchen lässt sich die Ermittlung der Prüfsumme von Dateien ab einer bestimmten Größe für den Versand dieser Informationen an die KSN-Dienste aktivieren bzw. deaktivieren.

    Wie viel Zeit die Ermittlung der Prüfsumme beansprucht, hängt von der Dateigröße ab.

    Ist das Kontrollkästchen aktiviert, wird die Prüfsumme für Dateien, deren Größe den in MB festgelegten Wert übersteigt, von Kaspersky Embedded Systems Security nicht ermittelt.

    Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security die Prüfsumme für Dateien beliebiger Größe.

    Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  - Ändern Sie bei Bedarf im Feld rechts die maximale Dateigröße, bis zu der Kaspersky Embedded Systems Security die Prüfsumme berechnen soll.
- Aktivieren oder deaktivieren Sie im Abschnitt **KSN-Proxyserver** das Kontrollkästchen **Kaspersky Security Center als KSN-Proxyserver verwenden**.

  Mithilfe dieses Kontrollkästchens können Sie die Datenübertragung zwischen den geschützten Computern und KSN verwalten.

  Wenn das Kontrollkästchen deaktiviert ist, werden keine Daten vom Administrationsserver und von geschützten Computern direkt an KSN gesendet (nicht über das Kaspersky Security Center). Die aktive Richtlinie legt fest, welche Datentypen direkt an KSN gesendet werden können.

  Wenn das Kontrollkästchen aktiviert ist, werden alle Daten über das Kaspersky Security Center an KSN gesendet.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Der KSN-Proxyserver kann nur aktiviert werden, wenn die KSN-Erklärung akzeptiert wurde und Kaspersky Security Center ordnungsgemäß konfiguriert ist. Weitere Informationen finden Sie im *Hilfesystem von Kaspersky Security Center*.

6. Passen Sie bei Bedarf den Zeitplan für den Aufgabenstart auf der Registerkarte **Aufgabenverwaltung** an. Sie können beispielsweise die Aufgabe nach Zeitplan starten und als Intervall **Bei Programmstart** angeben, wenn Sie möchten, dass die Aufgabe nach dem Neustart des Servers automatisch gestartet wird.

   Das Programm startet die Aufgabe Verwendung von KSN zukünftig nach Zeitplan.

7. Konfigurieren Sie die Datenverarbeitung (s. Abschnitt "Datenverarbeitung über das Verwaltungs-Plug-in konfigurieren" auf Seite 297), bevor Sie die Aufgabe starten.
8. Klicken Sie auf **OK**.

Die vorgenommenen Änderungen der Aufgabe werden übernommen. Datum und Uhrzeit der Änderung sowie Informationen über die Einstellungen der Aufgabe vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Datenverwaltung über das Verwaltungs-Plug-in konfigurieren

► *Um festzulegen, welche Daten von den KSN-Diensten verarbeitet werden, und die KSN-Erklärung zu akzeptieren, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Echtzeit-Computerschutz** auf die Schaltfläche **Datenverarbeitung** im Block **Verwendung von KSN**.

   Das Fenster **Datenverarbeitung** wird geöffnet.
5. Lesen Sie auf der Registerkarte **Dienste** die Erklärung und wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network**.
6. Um die Sicherheitsstufe zu erhöhen, werden die folgenden Kontrollkästchen automatisch aktiviert:
   - **Daten über untersuchte Dateien senden**.

     Ist dieses Kontrollkästchen aktiviert, sendet Kaspersky Embedded Systems Security die Prüfsumme der untersuchten Dateien an Kaspersky Lab. Die Einstufung der Sicherheit jeder Datei basiert auf der von KSN bereitgestellten Reputation.

     Ist dieses Kontrollkästchen deaktiviert, sendet Kaspersky Embedded Systems Security die Prüfsumme der Dateien nicht an KSN.

     Beachten Sie, dass die Anfragen bezüglich der Reputation von Dateien möglicherweise in einem eingeschränkten Modus gesendet werden. Die Einschränkungen werden zum Schutz der Reputationsserver von Kaspersky Lab vor DDoS-Angriffen verwendet. In diesem Szenario werden die Parameter von Anfragen bezüglich der Reputation

von Dateien, die gesendet werden, durch die von den Spezialisten von Kaspersky Lab festgelegten Regeln und Methoden definiert und können nicht von einem Benutzer eines geschützten Computers konfiguriert werden. Aktualisierungen dieser Regeln und Methoden erfolgen zusammen mit den Datenbank-Updates des Programms. Wenn die Einschränkungen angewendet werden, wird der Status *Von Kaspersky Lab zum Schutz der KSN-Server gegen DDoS-Angriffe aktiviert* in den Statistiken der Aufgabe "Verwendung von KSN" angezeigt.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Statistiken zu Kaspersky Security Network senden.**

  Wenn dieses Kontrollkästchen aktiviert ist, sendet Kaspersky Embedded Systems Security zusätzliche Statistikdaten, zu denen auch persönliche Daten gehören können. Die Liste mit allen Datenarten, die als KSN-Statistiken gesendet werden, ist in der KSN-Erklärung enthalten. Die von Kaspersky Lab erhaltenen Daten werden dazu verwendet, um die Qualität der Programme und das Niveau des Erkennens von Bedrohungen zu steigern.

  Ist das Kontrollkästchen deaktiviert, versendet Kaspersky Embedded Systems Security keine zusätzlichen Statistikdaten.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Sie können diese Kontrollkästchen deaktivieren und das Senden zusätzlicher Daten jederzeit unterbinden.

7. Lesen Sie sich auf der Registerkarte **Kaspersky Managed Protection** die Erklärung durch und aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection**.

   Wenn das Kontrollkästchen aktiviert ist, stimmen Sie dem Versand von Statistikdaten über die Aktivität des geschützten Computers an die Spezialisten von Kaspersky Lab zu. Die empfangenen Daten werden für Analysen und Berichte rund um die Uhr verwendet, die zur Vermeidung von Sicherheitsverletzungen erforderlich sind.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Durch die Änderungen des Kontrollkästchens **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection** wird die Verarbeitung der Daten nicht sofort gestartet oder gestoppt. Um die Änderungen zu übernehmen, müssen Sie Kaspersky Embedded Systems Security neu starten.

Um den KMP-Dienst zu verwenden, müssen Sie den entsprechenden Vertrag unterzeichnen und die Konfigurationsdateien auf einem geschützten Computer ausführen.

Um den KMP-Dienst zu verwenden, müssen die Bedingungen zur Datenverarbeitung der KSN-Erklärung auf der Registerkarte **Dienste** akzeptiert werden.

8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen der Datenverarbeitung werden gespeichert.

Verwendung von KSN über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe zur Verwendung von KSN und die Datenverwaltung über die Programmkonsole konfigurieren.

In diesem Abschnitt

Aufgabe zur Verwendung von KSN über die Programmkonsole konfigurieren

► *Um die Einstellungen der Aufgabe Verwendung von KSN zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Verwendung von KSN**.
3. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Passen Sie die Aufgabeneinstellungen an:
   - Geben Sie im Abschnitt **Aktion für Objekte, die in KSN nicht vertrauenswürdig sind** die Aktion an, die Kaspersky Embedded Systems Security ausführen soll, wenn ein Objekt gefunden wird, das laut KSN als nicht vertrauenswürdig eingestuft ist:
     - **Löschen**

       Kaspersky Embedded Systems Security löscht das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, und verschiebt eine Kopie davon ins Backup.

       Diese Variante gilt als Standard.
     - **Informationen protokollieren**

       Kaspersky Embedded Systems Security nimmt Informationen über das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, in das Protokoll der Aufgabenausführung auf. Das nicht vertrauenswürdige Objekt wird von Kaspersky Embedded Systems Security nicht gelöscht.
   - Begrenzen Sie im Abschnitt **Versand von Daten** die Größe der Dateien, für die eine Prüfsumme berechnet werden soll:
     - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Keine Prüfsumme für den Versand an KSN berechnen für Dateien, die größer sind als (MB)**.

       Über dieses Kontrollkästchen lässt sich die Ermittlung der Prüfsumme von Dateien ab einer bestimmten Größe für den Versand dieser Informationen an die KSN-Dienste aktivieren bzw. deaktivieren.

       Wie viel Zeit die Ermittlung der Prüfsumme beansprucht, hängt von der Dateigröße ab.

Ist das Kontrollkästchen aktiviert, wird die Prüfsumme für Dateien, deren Größe den in MB festgelegten Wert übersteigt, von Kaspersky Embedded Systems Security nicht ermittelt.

Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security die Prüfsumme für Dateien beliebiger Größe.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Ändern Sie bei Bedarf im Feld rechts die maximale Dateigröße, bis zu der Kaspersky Embedded Systems Security die Prüfsumme berechnen soll.

5. Passen Sie bei Bedarf den Zeitplan für den Aufgabenstart auf den Registerkarten **Zeitplan** und **Erweitert** an. Sie können beispielsweise den Aufgabenstart nach Zeitplan aktivieren und als Intervall für den Aufgabenstart **Bei Programmstart** angeben, wenn Sie möchten, dass die Aufgabe nach dem Neustart des Computers automatisch gestartet wird.

   Das Programm startet die Aufgabe Verwendung von KSN zukünftig nach Zeitplan.

6. Konfigurieren Sie die Datenverarbeitung (s. Abschnitt "Datenverwaltung über die Programmkonsole konfigurieren" auf Seite 300), bevor Sie die Aufgabe starten.

7. Klicken Sie auf **OK**.

Die vorgenommenen Änderungen der Aufgabe werden übernommen. Datum und Uhrzeit der Änderung sowie Informationen über die Einstellungen der Aufgabe vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Datenverwaltung über die Programmkonsole konfigurieren

► *Um festzulegen, welche Daten von den KSN-Diensten verarbeitet werden, und die KSN-Erklärung zu akzeptieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Verwendung von KSN**.
3. Klicken Sie im Detailbereich auf den Link **Datenverarbeitung**.

   Das Fenster **Datenverarbeitung** wird geöffnet.

4. Lesen Sie auf der Registerkarte **Dienste** die Erklärung und wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network**.
5. Um die Sicherheitsstufe zu erhöhen, werden die folgenden Kontrollkästchen automatisch aktiviert:

   - **Daten über untersuchte Dateien senden**.

     Ist dieses Kontrollkästchen aktiviert, sendet Kaspersky Embedded Systems Security die Prüfsumme der untersuchten Dateien an Kaspersky Lab. Die Einstufung der Sicherheit jeder Datei basiert auf der von KSN bereitgestellten Reputation.

     Ist dieses Kontrollkästchen deaktiviert, sendet Kaspersky Embedded Systems Security die Prüfsumme der Dateien nicht an KSN.

Beachten Sie, dass die Anfragen bezüglich der Reputation von Dateien möglicherweise in einem eingeschränkten Modus gesendet werden. Die Einschränkungen werden zum Schutz der Reputationsserver von Kaspersky Lab vor DDoS-Angriffen verwendet. In diesem Szenario werden die Parameter von Anfragen bezüglich der Reputation von Dateien, die gesendet werden, durch die von den Spezialisten von Kaspersky Lab festgelegten Regeln und Methoden definiert und können nicht von einem Benutzer eines geschützten Computers konfiguriert werden. Aktualisierungen dieser Regeln und Methoden erfolgen zusammen mit den Datenbank-Updates des Programms. Wenn die Einschränkungen angewendet werden, wird der Status *Von Kaspersky Lab zum Schutz der KSN-Server gegen DDoS-Angriffe aktiviert* in den Statistiken der Aufgabe "Verwendung von KSN" angezeigt.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Statistiken zu Kaspersky Security Network senden.**

  Wenn dieses Kontrollkästchen aktiviert ist, sendet Kaspersky Embedded Systems Security zusätzliche Statistikdaten, zu denen auch persönliche Daten gehören können. Die Liste mit allen Datenarten, die als KSN-Statistiken gesendet werden, ist in der KSN-Erklärung enthalten. Die von Kaspersky Lab erhaltenen Daten werden dazu verwendet, um die Qualität der Programme und das Niveau des Erkennens von Bedrohungen zu steigern.

  Ist das Kontrollkästchen deaktiviert, versendet Kaspersky Embedded Systems Security keine zusätzlichen Statistikdaten.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Sie können diese Kontrollkästchen deaktivieren und das Senden zusätzlicher Daten jederzeit unterbinden.

6. Lesen Sie sich auf der Registerkarte **Kaspersky Managed Protection** die Erklärung durch und aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection**.

   Wenn das Kontrollkästchen aktiviert ist, stimmen Sie dem Versand von Statistikdaten über die Aktivität des geschützten Computers an die Spezialisten von Kaspersky Lab zu. Die empfangenen Daten werden für Analysen und Berichte rund um die Uhr verwendet, die zur Vermeidung von Sicherheitsverletzungen erforderlich sind.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Durch die Änderungen des Kontrollkästchens **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection** wird die Verarbeitung der Daten nicht sofort gestartet oder gestoppt. Um die Änderungen zu übernehmen, müssen Sie Kaspersky Embedded Systems Security neu starten.

Um den KMP-Dienst zu verwenden, müssen Sie den entsprechenden Vertrag unterzeichnen und die Konfigurationsdateien auf einem geschützten Computer ausführen.

Um den KMP-Dienst zu verwenden, müssen die Bedingungen zur Datenverarbeitung der KSN-Erklärung auf der Registerkarte **Dienste** akzeptiert werden.

7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen der Datenverarbeitung werden gespeichert.

Konfiguration des zusätzlichen Versands von Daten

Kaspersky Embedded Systems Security kann konfiguriert werden, um die folgenden Daten an Kaspersky Lab zu senden:

- Prüfsummen untersuchter Dateien (Kontrollkästchen **Daten über untersuchte Dateien senden**).
- Zusätzliche Statistiken, einschließlich persönlicher Daten (Kontrollkästchen **Statistiken zu Kaspersky Security Network senden**).

Genauere Informationen zu Daten, die an Kaspersky Lab gesendet werden, finden Sie im Abschnitt "Lokale Datenverarbeitung" dieses Handbuchs.

Die entsprechenden Kontrollkästchen können nur dann aktiviert bzw. deaktiviert werden (s. Abschnitt "Datenverwaltung über die Programmkonsole konfigurieren" auf Seite 300), wenn das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network** aktiviert ist.

Kaspersky Embedded Systems Security sendet standardmäßig Prüfsummen von Dateien sowie zusätzliche Statistiken, nachdem Sie die KSN-Erklärung akzeptiert haben.

Tabelle 45. Mögliche Status von Kontrollkästchen und zugehörige Bedingungen

Kontrollkästchen-Status	**Bedingungen für den Status des Kontrollkästchens** Daten über untersuchte Dateien senden	**Bedingungen für den Status des Kontrollkästchens** Statistiken zu Kaspersky Security Network senden	**Bedingungen für den Status des Kontrollkästchens** Daten über untersuchte URLs senden	**Bedingungen für den Status des Kontrollkästchens** Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection	**Bedingungen für den Status des Kontrollkästchens** Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network
☑	• Anfragen bezüglich der Reputation werden gesendet • Kontrollkästchen ist editierbar	• Zusätzliche Statistiken werden gesendet • Kontrollkästchen ist editierbar	• Daten über untersuchte URLs werden gesendet • Kontrollkästchen ist editierbar	• Die Bedingungen der Erklärung zu Kaspersky Managed Protection werden akzeptiert • Kontrollkästchen ist editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network Statement werden akzeptiert • Kontrollkästchen ist editierbar

Kontrollkästchen-Status	**Bedingungen für den Status des Kontrollkästchens** Daten über untersuchte Dateien senden	**Bedingungen für den Status des Kontrollkästchens** Statistiken zu Kaspersky Security Network senden	**Bedingungen für den Status des Kontrollkästchens** Daten über untersuchte URLs senden	**Bedingungen für den Status des Kontrollkästchens** Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection	**Bedingungen für den Status des Kontrollkästchens** Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network
☑	• Anfragen bezüglich der Reputation werden gesendet • Kontrollkästchen ist nicht editierbar	• Zusätzliche Statistiken werden gesendet • Kontrollkästchen ist nicht editierbar	• Daten über untersuchte URLs werden gesendet • Kontrollkästchen ist nicht editierbar	• Die Bedingungen der Erklärung zu Kaspersky Managed Protection werden akzeptiert • Kontrollkästchen ist nicht editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network Statement werden akzeptiert • Kontrollkästchen ist nicht editierbar
☐	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist editierbar	• Daten über untersuchte URLs werden nicht gesendet • Kontrollkästchen ist editierbar	• Die Bedingungen der Erklärung zu Kaspersky Managed Protection werden nicht akzeptiert • Kontrollkästchen ist editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network Statement werden nicht akzeptiert • Kontrollkästchen ist editierbar

Kontrollkästchen-Status	Bedingungen für den Status des Kontrollkästchens Daten über untersuchte Dateien senden	Bedingungen für den Status des Kontrollkästchens Statistiken zu Kaspersky Security Network senden	Bedingungen für den Status des Kontrollkästchens Daten über untersuchte URLs senden	Bedingungen für den Status des Kontrollkästchens Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection	Bedingungen für den Status des Kontrollkästchens Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network
☐	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Daten über untersuchte URLs werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Die Bedingungen der Erklärung zu Kaspersky Managed Protection werden nicht akzeptiert • Kontrollkästchen ist nicht editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network Statement werden nicht akzeptiert • Kontrollkästchen ist nicht editierbar

Statistik für die Aufgabe Verwendung von KSN

Während die Aufgabe zur Verwendung von KSN ausgeführt wird, können Sie in Echtzeit Informationen über die Anzahl der Objekte, die Kaspersky Embedded Systems Security seit seinem Start bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen lassen. Informationen über alle Ereignisse, die während der Aufgabenausführung eintreten, werden in das Protokoll der Aufgabenausführung aufgenommen (siehe Abschnitt "Über die Protokoll der Aufgabenausführung" auf Seite 216).

► *Um die Statistik der Aufgabe Verwendung von KSN anzuzeigen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Verwendung von KSN**.

Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Sie können Informationen über Objekte aufrufen, die Kaspersky Embedded Systems Security während der Ausführung der Aufgabe verarbeitet hat (siehe Tabelle unten).

Tabelle 46. Statistik für die Aufgabe Verwendung von KSN

Feld	Beschreibung
Fehler beim Versand von Anfragen	Anzahl der Anfragen an KSN, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Statistiken erstellt	Anzahl der erstellten Statistikpakete, die an KSN gesendet wurden.
Gelöschte Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security während der Ausführung der Aufgabe zur Verwendung von KSN entfernt hat.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Embedded Systems Security im Backup gespeichert wurden.
Nicht gelöschte 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. Die Informationen über diese Objekte werden in das Protokoll der Aufgabenausführung aufgenommen.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu kopieren versucht hat, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war. Dateien, die nicht in den Backup verschoben werden konnten, werden durch das Programm weder desinfiziert noch gelöscht. Die Informationen über diese Objekte werden in das Protokoll der Aufgabenausführung aufgenommen.
Begrenzter Modus	Der Status gibt an, ob die Anwendung Datei-Reputationsanforderungen in einem begrenzten Modus sendet.

Kontrolle des Programmstarts

Dieser Abschnitt informiert über die Aufgabe zur Kontrolle des Programmstarts und erläutert die Konfiguration dieser Aufgabe.

In diesem Kapitel

Über die Aufgabe zur Kontrolle des Programmstarts

Wenn die Aufgabe zur Kontrolle des Programmstarts ausgeführt wird, überwacht Kaspersky Embedded Systems Security die versuchten Programmstarts des Benutzers und erlaubt oder verbietet den Start dieser Programme. Die Aufgabe zur Kontrolle des Programmstarts baut auf dem Prinzip "standardmäßig verboten" auf, was bedeutet, dass alle Programme, die in den Aufgabeneinstellungen nicht erlaubt sind, automatisch blockiert werden.

Sie können den Programmstart auf eine der folgenden Weisen erlauben:

- Anhand von Erlaubnisregeln für vertrauenswürdige Programme
- Prüfung der Reputation vertrauenswürdiger Programme in KSN beim Start

Die Aufgabe verleiht dem Startverbot von Programmen oberste Priorität. Wenn ein Programm beispielsweise durch eine der Verbotsregeln am Start gehindert wird, wird der Programmstart unabhängig von der Einstufung von KSN als "vertrauenswürdig" verboten. Wenn ein Programm also von den KSN-Diensten als nicht vertrauenswürdig eingestuft wird, aber in den Gültigkeitsbereich einer Erlaubnisregel fällt, wird der Programmstart verboten.

Alle Versuche, Programme zu starten, werden im Protokoll der Aufgabenausführung festgehalten (siehe Abschnitt "Über Protokolle der Aufgabenausführung" auf Seite 216).

Aufgabe zur Kontrolle des Programmstarts kann in einem von zwei Modi betrieben werden:

- Aktiv. Die Kontrolle durch Kaspersky Embedded Systems Security erfolgt mithilfe eines Regelsatzes zur Kontrolle des Starts von Programmen, die unter den Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts fallen. Der Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts ist in den Einstellungen der Aufgabe angegeben. Fällt ein Programm unter den Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts und entsprechen die Aufgabeneinstellungen keiner der angegebenen

Regeln, ist der Programmstart verboten.

Starts von Programmen, die sich außerhalb des Gültigkeitsbereichs der Regeln befinden, wie er in den Eigenschaften der Aufgabe zur Kontrolle des Programmstarts festgelegt ist, sind unabhängig von den Einstellungen der Regeln für die Kontrolle des Programmstarts erlaubt.

Die Aufgabe zur Kontrolle des Programmstarts kann nicht im aktiven Modus gestartet werden, wenn keine Regeln erstellt wurden oder wenn es mehr als 65.535 Regeln für einen Computer gibt.

- Nur Statistik. Kaspersky Embedded Systems Security verwendet keine Regel für die Kontrolle des Programmstarts, um den Start von Programmen zu erlauben oder zu verbieten. Stattdessen werden nur Informationen über Programmstarts, Regeln, die von laufenden Programmen erfüllt werden, und Aktionen, die ausgeführt worden wären, wenn die Aufgabe im Modus Aktiv ausgeführt würde, aufgezeichnet. Allen Programmen wird der Start erlaubt. Dieser Modus ist standardmäßig eingestellt.

  Sie können diesen Modus anwenden, um auf der Grundlage der im Protokoll der Aufgabenausführung festgelegten Informationen die Regeln zur Kontrolle des Programmstarts zu erstellen (siehe Abschnitt "Erlaubnisregeln aus Ereignissen der Aufgabe zur Kontrolle des Programmstarts erstellen " auf S. 355).

Sie können die Aufgabe zur Kontrolle des Programmstarts nach einem der folgenden Szenarien gestalten:

- Erweiterte Konfiguration von Regeln (siehe Abschnitt "Über Regeln für die Kontrolle des Programmstarts" auf Seite 307) und Verwendung zur Kontrolle des Programmstarts.
- Minimale Konfiguration der Regeln und die Verwendung von KSN (siehe Abschnitt "Konfiguration der Verwendung von KSN" auf Seite 348) für die Kontrolle des Programmstarts.

Wenn Dateien des Betriebssystems in den Gültigkeitsbereich der Aufgabe zur Kontrolle des Programmstarts fallen, wird empfohlen, beim Erstellen von Regeln für die Kontrolle des Programmstarts sicherzustellen, dass solche Programme von den neu erstellten Regeln erlaubt werden. Andernfalls kann das Betriebssystem möglicherweise nicht mehr starten.

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). Bei solchen Prozessen wendet die Aufgabe zur Kontrolle des Programmstarts die von der aktuellen Konfiguration festgelegte Aktion an. Die Aufgabe "Automatisches 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 für die Kontrolle des Programmstarts können den Start eines Programms erlauben oder verbieten. Demgemäß werden sie als *Erlaubnisregeln* oder *Verbotsregeln* bezeichnet. Zum Erstellen einer Liste von Erlaubnisregeln für die Kontrolle des Programmstarts können Sie die Aufgabe zur Erstellung von Erlaubnisregeln oder den Modus Nur Statistik in der Aufgabe zur Kontrolle des Programmstarts verwenden. Sie können ferner Erlaubnisregeln manuell hinzufügen.

- Benutzer und / oder Benutzergruppe.

Regeln für die Kontrolle des Programmstarts können den Start von festgelegten Programmen durch einen Benutzer und/oder eine Benutzergruppe kontrollieren.

- Gültigkeitsbereich der Regeln

  Regeln für die Kontrolle des Programmstarts können auf *ausführbare Dateien*, *Skripts* und *MSI-Pakete* angewendet werden.

- Auslösekriterium für die Regel.

  Die Regeln für die Kontrolle des Programmstarts kontrollieren den Start derjenigen Dateien, die eines der in den Regeleinstellungen festgelegten Kriterien erfüllen: Sie sind mit dem angegebenen *digitalen Zertifikat* signiert, weisen den angegebenen *SHA256-Hash* auf oder sind unter dem angegebenen *Pfad* gespeichert.

  Ist die Einstellung Digitales Zertifikat als Auslösekriterium für die Regel festgelegt, kontrolliert die erstellte Regel den Start aller vertrauenswürdigen Programme im Betriebssystem. Sie können strengere Bedingungen für dieses Kriterium festlegen, indem Sie die folgenden Kontrollkästchen aktivieren:

  - Header verwenden

    Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers digitaler Zertifikate als Auslösekriterium für die Regel.

    Ist das Kontrollkästchen aktiviert, wird der angegebene Header des digitalen Zertifikats als Auslösekriterium für die Regel verwendet. Die erstellte Regel kontrolliert den Start von Programmen dann lediglich für den im Header genannten Hersteller.

    Ist das Kontrollkästchen deaktiviert, verwendet das Programm den Header des digitalen Zertifikats nicht als Auslösekriterium für die Regel. Ist das Kriterium Digitales Zertifikat ausgewählt, kontrolliert die erstellte Regel Starts von Programmen, die mit einem digitalen Zertifikat mit beliebigem Header signiert sind.

    Den Header des digitalen Zertifikats, mit dem die Datei signiert ist, können Sie nur aus den Eigenschaften der ausgewählten Datei mithilfe der Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben oberhalb des Abschnitts Auslösekriterien für Regeln auswählen.

    Das Kontrollkästchen ist standardmäßig deaktiviert.

  - Fingerabdruck verwenden

    Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Fingerabdrucks digitaler Zertifikate als Auslösekriterium für die Regel.

    Ist das Kontrollkästchen aktiviert, wird der angegebene Fingerabdruck des digitalen Zertifikats als Auslösekriterium für die Regel verwendet. Die erstellte Regel kontrolliert dann den Start von Programmen, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.

    Ist das Kontrollkästchen deaktiviert, verwendet das Programm den Fingerabdruck des digitalen Zertifikats nicht als Auslösekriterium für die Regel. Ist das Kriterium Digitales Zertifikat ausgewählt, kontrolliert das Programm Starts von Programmen, die mit einem digitalen Zertifikat mit beliebigem Fingerabdruck signiert sind.

    Den Fingerabdruck des digitalen Zertifikats, mit dem die Datei signiert ist, können Sie nur aus den Eigenschaften der ausgewählten Datei mithilfe der Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben oberhalb des Abschnitts Auslösekriterien für Regeln auswählen.

    Das Kontrollkästchen ist standardmäßig deaktiviert.

Fingerabdrücke ermöglichen die strengste Einschränkung für das Auslösen der Regeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles Identifikationsmerkmal eines digitalen Zertifikats handelt, welches im Gegensatz zum Header eines digitalen Zertifikats fälschungssicher ist.

Sie können Ausnahmen von der Regel für die Kontrolle des Programmstarts festlegen. Ausnahmen von der Regel für die Kontrolle des Programmstarts basieren auf denselben Kriterien, die für das Auslösen der Regel gelten: digitales Zertifikat, SHA256-Hash und Dateipfad. 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.

Wenn Dateien des Betriebssystems in den Gültigkeitsbereich der Aufgabe zur Kontrolle des Programmstarts fallen, wird empfohlen, beim Erstellen von Regeln für die Kontrolle des Programmstarts sicherzustellen, dass solche Programme von den neu erstellten Regeln erlaubt werden. Andernfalls kann das Betriebssystem möglicherweise nicht mehr starten.

Verwaltung der Regeln für die Kontrolle des Programmstarts

Für die Regel für die Kontrolle des Programmstarts stehen Ihnen die folgenden Aktionen zur Verfügung:

- Regeln manuell hinzufügen
- Regeln automatisch erstellen und hinzufügen
- Regeln löschen
- Regeln in eine Konfigurationsdatei exportieren
- Ausgewählte Dateien auf das Vorhandensein von Regeln prüfen, die den Start dieser Dateien erlauben
- Die Liste der Regeln nach einem festgelegten Kriterium filtern

Über die Kontrolle für Installationspakete

Das Erzeugen von Regeln für die Kontrolle des Programmstarts kann kompliziert sein, wenn Sie auch Installationspakete auf einem geschützten Computer überwachen müssen, beispielsweise auf Computern, auf denen 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 Aufgabe zur Kontrolle des Programmstarts berücksichtigt werden. Um die Startkontrolle bei Installationspakete-Szenarien zu vereinfachen, können Sie das Untersystem "Kontrolle für Installationspakete" verwenden.

Ein Installationspaket (im Weiteren "Paket") stellt eine Software-Anwendung dar, die auf einem Computer installiert werden soll. Jedes Paket enthält mindestens eine Anwendung und kann darüber hinaus einzelne Dateien, Updates oder auch einen bestimmten Befehl enthalten, vor allem wenn Sie eine Software-Anwendung oder ein Update installieren.

Das Untersystem "Kontrolle für Installationspakete" wird als zusätzliche Liste von Ausnahmen implementiert. Wenn Sie ein Installationspaket zu dieser Liste hinzufügen, erlaubt das Programm, dass diese vertrauenswürdigen Pakete dekomprimiert werden und erlaubt, dass Software, die von einem vertrauenswürdigen Paket installiert oder verändert wurde, automatisch gestartet wird. 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 für Installationspakete hinzugefügt wurde und nun als vertrauenswürdiges Paket gilt.

Kaspersky Embedded Systems Security kontrolliert nur vollständige Zyklen von Installationspaketen. Das Programm kann den Start von Dateien, die von einem vertrauenswürdigen Paket modifiziert wurden, nicht korrekt verarbeiten, wenn das Paket das erste Mal ausgeführt wird, wenn die Kontrolle für Installationspakete deaktiviert ist oder wenn die Komponente "Kontrolle des Programmstarts" nicht installiert ist.

Die Kontrolle für Installationspakete ist nicht verfügbar, wenn das Kontrollkästchen Regeln für ausführbare Dateien verwenden in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts deaktiviert ist.

Cache für Softwareverteilung

Kaspersky Embedded Systems Security verwendet einen dynamisch erzeugten Cache für Softwareverteilung (Installations-Cache), 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 Installations-Cache. Anschließend dürfen alle Dateien im Installations-Cache standardmäßig gestartet werden.

Sie können den Installations-Cache nicht über die Benutzeroberfläche überprüfen, löschen oder modifizieren. Der Cache wird von Kaspersky Embedded Systems Security mit Daten gefüllt und kontrolliert.

Sie können den Installations-Cache in eine Konfigurationsdatei exportieren (xml-Format) und den Cache außerdem mithilfe von Befehlszeilenoptionen löschen.

► *Um den Installations-Cache in eine Konfigurationsdatei zu exportieren, führen Sie den folgenden Befehl aus:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Um den Installations-Cache zu löschen, führen Sie den folgenden Befehl aus:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security aktualisiert den Installations-Cache alle 24 Stunden. Wenn die Prüfsumme einer zuvor erlaubten Datei geändert wird, löscht das Programm den Datensatz für diese Datei aus dem Installations-Cache. Wenn die Aufgabe zur Kontrolle des Programmstarts im aktiven Modus gestartet wurde, werden weitere Ausführungsversuche dieser Datei unterbunden. Wenn der vollständige Pfad der zuvor erlaubten Datei geändert wird, werden weitere Ausführungsversuche dieser Datei nicht unterbunden, weil die Prüfsumme im Installations-Cache gespeichert ist.

Verarbeiten der extrahierten Dateien

Alle aus einem vertrauenswürdigen Paket extrahierten Dateien erben beim ersten Start des Pakets das Merkmal für die Vertrauenswürdigkeit. Wenn Sie das Kontrollkästchen nach dem ersten Start deaktivieren, behalten alle aus dem Paket extrahierten Dateien das geerbte Attribut. Um das geerbte Attribut für alle extrahierten Dateien zurückzusetzen, müssen Sie den Installations-Cache löschen und das Kontrollkästchen Start von Dateien in allen Ebenen dieses Installationspakets erlauben deaktivieren, bevor Sie das vertrauenswürdige Installationspaket erneut starten.

Extrahierte Dateien und Pakete, die von einem vertrauenswürdigen Hauptprogrammpaket erstellt wurden, erben das Merkmal für die Vertrauenswürdigkeit, indem ihre Prüfsummen beim ersten Start des Installationspakets in der Liste mit Ausnahmen zum Installations-Cache hinzugefügt werden. Als Folge gelten sowohl das Installationspaket selbst als auch alle extrahierten Dateien des Pakets als vertrauenswürdig. Standardmäßig ist die Anzahl der Ebenen von Vererbung des Merkmals für die Vertrauenswürdigkeit unbegrenzt.

Extrahierte Dateien behalten das Merkmal für die Vertrauenswürdigkeit nachdem das Betriebssystem neu gestartet wurde.

Die Verarbeitung von Dateien wird in den Einstellungen der Kontrolle für Installationspakete angepasst (siehe Abschnitt "Konfiguration der Kontrolle für Installationspakete" auf S. 324). Aktivieren oder deaktivieren Sie dazu das Kontrollkästchen Start von Dateien in allen Ebenen dieses Installationspakets erlauben.

Angenommen, Sie fügen beispielsweise das Paket test.msi, das einige andere Pakete und Programme enthält, zur Ausnahmeliste hinzu und aktivieren das Kontrollkästchen. In diesem Fall wird allen Paketen und Programmen im Paket test.msi erlaubt, zu starten oder ihren Inhalt zu extrahieren, wenn sie andere Dateien enthalten. Dieses Szenario gilt für extrahierte Dateien auf allen Verschachtelungsebenen.

Wenn Sie das Paket test.msi zur Ausnahmeliste hinzufügen und das Kontrollkästchen Start von Dateien in allen Ebenen dieses Installationspakets erlauben deaktivieren, weist das Programm das Merkmal für die Vertrauenswürdigkeit nur solchen Paketen und ausführbaren Dateien zu, die direkt aus dem primären vertrauenswürdigen Paket extrahiert werden (auf der ersten Verschachtelungsebene). Die Prüfsummen dieser Dateien werden im Installations-Cache gespeichert. Alle Dateien, die sich auf der zweiten Verschachtelungsebene und tiefer befinden, werden nach dem Prinzip des standardmäßigen Verbots (Default Deny) blockiert.

Arbeiten mit der Regelliste für die Kontrolle des Programmstarts

Die Liste vertrauenswürdiger Pakete des Untersystems "Kontrolle für Installationspakete" ist eine Liste bestehend aus Ausnahmen. Diese Liste erweitert die allgemeine Liste mit 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 für Installationspakete 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.

Verwendung der KSN-Einstufungen

KSN-Einstufungen, dass eine Datei nicht vertrauenswürdig ist, haben eine höhere Priorität als die Ausnahmen der Kontrolle für Installationspakete: Dekomprimierung von vertrauenswürdigen Paketen und Start von Dateien, die von diesen Paketen erstellt oder geändert werden, werden blockiert, wenn KSN meldet, dass diese Dateien nicht vertrauenswürdig sind.

Nach dem Entpacken eines vertrauenswürdigen Pakets dürfen alle untergeordneten Dateien ausgeführt werden, unabhängig von der Verwendung von KSN innerhalb des Bereichs "Kontrolle des Programmstarts". Die Status der Kontrollkästchen Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten und Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben haben daher keine Auswirkung auf das Kontrollkästchen Start von Dateien in allen Ebenen dieses Installationspakets erlauben.

Über die Verwendung von KSN mit der Aufgabe Kontrolle des Programmstarts

Die Aufgabe Verwendung von KSN kann nur gestartet werden, wenn die KSN-Erklärung akzeptiert wurde.

Wenn KSN-Daten über die Reputation von der Aufgabe zur Kontrolle des Programmstarts verwendet werden, wird die Programmreputation von KSN als Kriterium für das Erlauben oder Blockieren des Starts dieses Programms betrachtet. Wenn KSN an Kaspersky Embedded Systems Security meldet, dass ein Programm nicht vertrauenswürdig ist, wenn der Benutzer versucht, das Programm zu starten, wird der Start des Programms verboten. Wenn KSN an Kaspersky Embedded Systems Security meldet, dass das Programm vertrauenswürdig ist, wenn der Benutzer versucht, das Programm zu starten, wird der Start des Programms erlaubt. Sie können KSN zusammen mit Regeln für die Kontrolle des Programmstarts oder als unabhängiges Kriterium für das Verbot des Starts von Programmen verwenden.

Einstufungen von KSN als unabhängiges Kriterium für die Blockierung des Programmstarts übernehmen

Dieses Szenario ermöglicht es, den Programmstart auf einem geschützten Computer auf sichere Weise zu kontrollieren, ohne erweiterte Einstellungen der Regelliste zu erfordern.

Sie können die KSN-Einstufungen für Kaspersky Embedded Systems Security gemeinsam mit der einzigen angegebenen Regel übernehmen. Das Programm erlaubt nur den Start von Programmen, die von KSN als vertrauenswürdig eingestuft wurden oder durch eine angegebene Regel erlaubt werden.

Für ein solches Szenario wird empfohlen, eine Erlaubnisregel für den Programmstart anhand des digitalen Zertifikats festzulegen.

Alle übrigen Programme werden nach dem Prinzip des standardmäßigen Verbots (Default Deny) verboten. Wenn keine Regeln festgelegt wurden, hilft die Verwendung von KSN dabei, den Computer vor Programmen zu schützen, die laut KSN eine Gefahr darstellen.

Einstufungen von KSN zusammen mit Regeln für die Kontrolle des Programmstarts übernehmen

Für die Verwendung von KSN zusammen mit Regeln für die Kontrolle des Programmstarts gelten die folgenden Bedingungen:

- Kaspersky Embedded Systems Security verbietet immer den Start eines Programms aus dem Gültigkeitsbereich von zumindest einer Verbotsregel. Wenn das Programm von den KSN-Diensten als vertrauenswürdig eingestuft wurde, wird der entsprechenden Einstufung eine niedrigere Priorität zugewiesen, und der Programmstart wird dennoch verboten. Dadurch können Sie die Liste unerwünschter Programme manuell erweitern.
- Kaspersky Embedded Systems Security verbietet den Start eines Programms immer, wenn der Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verboten ist und das Programm in KSN als nicht vertrauenswürdig eingestuft wurde. Wenn für das Programm eine Erlaubnisregel festgelegt wurde, wird dieser Regel eine niedrigere Priorität zugewiesen, und der Programmstart wird dennoch verboten. Auf diese Weise kann der Computer vor Programmen geschützt werden, die laut KSN eine Gefahr darstellen, aber bei der Erstkonfiguration der Regeln nicht berücksichtigt wurden.

Regeln für die Kontrolle des Programmstarts erzeugen

Sie können mithilfe der Aufgaben und Richtlinien von Kaspersky Security Center für alle Computer und Computergruppen im Netzwerk des Unternehmens gleichzeitig Listen mit Regeln für die Kontrolle des Programmstarts erstellen. Dieses Szenario wird empfohlen, wenn das Unternehmensnetzwerk über keinen Referenzcomputer verfügt und Sie keine Liste von Erlaubnisregeln auf der Grundlage von auf den Referenzcomputer installierten Programmen erstellen können. Sie können die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" auch lokal über die Programmkonsole ausführen, um eine Liste von Regeln auf der Grundlage der auf einem einzelnen Computer ausgeführten Programme erstellen.

Die Komponente zur Kontrolle des Programmstarts wird mit zwei voreingestellten Erlaubnisregeln installiert:

- Erlaubnisregel für Skripts und MSI-Dateien mit einem Zertifikat, das vom Betriebssystem als vertrauenswürdig betrachtet wird.
- Erlaubnisregel für ausführbare Dateien mit einem Zertifikat, das vom Betriebssystem als vertrauenswürdig betrachtet wird.

Sie können Listen mit Regeln für die Kontrolle des Programmstarts in der Konsole von Kaspersky Security Center auf eine der folgenden Arten erstellen:

- Mithilfe einer Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts".

  In diesem Szenario erstellt die Gruppenaufgabe für jeden Computer im Netzwerk eine eigene Liste der Regeln für die Kontrolle des Programmstarts und speichert diese Listen im angegebenen freigegebenen Ordner in Form einer XML-Datei. Die XML-Datei, die von der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" erzeugt wurde, enthält die Erlaubnisregel, die in Aufgabeneinstellungen angegeben sind, bevor die Aufgabe gestartet wird. Es werden keine Regeln für Programme erstellt, die in den angegebenen Aufgabeneinstellungen nicht gestartet werden dürfen. Der Start solcher Programme ist standardmäßig verboten. Danach können Sie die erstellten Listen mit Regeln manuell in die Aufgabe Kontrolle des Programmstarts für die Richtlinie von Kaspersky Security Center importieren. Sie können im Kaspersky Security Service eine Richtlinie konfigurieren, um die erstellten Regeln nach Abschluss der Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" automatisch zur Liste der Regeln für die Kontrolle des Programmstarts hinzufügen.

  Sie können die erstellten Regeln so konfigurieren, dass sie automatisch in die Liste der Regeln für die Aufgabe zur Kontrolle des Programmstarts importiert werden.

  Es wird empfohlen, diese Option zu verwenden, wenn die rasche Erstellung von Listen mit Regeln für die Kontrolle des Programmstarts erforderlich ist. Es wird empfohlen, den geplanten Start der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" nur dann einzurichten, wenn die übernommenen Erlaubnisregeln Ordner und Dateien enthalten, von denen Sie wissen, dass sie sicher sind.

  Stellen Sie vor der Verwendung der Aufgabe Kontrolle des Programmstarts im Netzwerk sicher, dass alle geschützten Computer Zugriff auf einen freigegebenen Ordner haben. Falls die Verwendung eines freigegebenen Ordners im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" auf einem Computer in der Test-Computergruppe oder auf einem Referenzcomputer zu starten.

- Auf Grundlage eines Berichts über Aufgabenereignisse, der in Kaspersky Security Center anhand der Ausführung der Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik erstellt wird.

In diesem Szenario verbietet Kaspersky Embedded Systems Security den Start von Programmen nicht. Stattdessen werden bei Ausführung der Kontrolle des Programmstarts im Modus Nur Statistik alle erlaubten und verbotenen Programmstarts für alle Netzwerkcomputer auf der Registerkarte **Ereignisse** des Arbeitsbereichs des Administrationsservers in Kaspersky Security Center gemeldet. Kaspersky Security Center verwendet das Protokoll der Aufgabenausführung, um eine einzelne Liste von Ereignissen zu erstellen, bei denen Programmstarts verboten wurden.

Sie müssen den Zeitraum für die Ausführung der Aufgabe so konfigurieren, dass alle möglichen Szenarien, in denen die geschützten Computer und Computergruppen beteiligt sind und mindestens ein Server-Neustart während der angegebenen Zeitspanne ausgeführt werden. Nachdem Regeln zur Kontrolle des Programmstarts hinzugefügt wurden, können Sie Daten über Programmstarts aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (TXT-Format) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle des Starts der betreffenden Programme erstellen.

Es wird empfohlen, dieses Szenario zu verwenden, wenn in einem Unternehmensnetzwerk sehr viele Computer unterschiedlichen Typs (mit unterschiedlichen installierten Programmen) betrieben werden.

- 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 Aufgabe zur Kontrolle des Programmstarts auf dem lokalen Computer unter der Verwaltung der aktiven Richtlinie für Kaspersky Security Center befinden. Alle Ereignisse auf dem lokalen Computer werden dabei an den Administrationsserver übergeben.

Es wird empfohlen, die Regelliste bei Änderungen an der Zusammensetzung der auf den Computern des Netzwerks installierten Programme zu aktualisieren (beispielsweise bei der Installation von Updates oder nach einer Neuinstallation des Betriebssystems). Es wird empfohlen, eine aktualisierte Liste von Regeln zu erstellen, in dem Sie auf Computern in der Test-Administrationsgruppe die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" oder die Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik ausführen. Die Test-Administrationsgruppe beinhaltet die Computer, die für den Test des Starts von neuen Programmen vor deren Installation auf den Computern des Netzwerks erforderlich sind.

XML-Dateien mit Listen von Erlaubnisregeln werden auf Grundlage einer Analyse der gestarteten Aufgaben auf dem geschützten Computer erstellt. Es wird empfohlen, die Aufgaben "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" und "Kontrolle des Programmstarts" im Modus **Nur Statistik** für die Erstellung von Regellisten auf einem Referenzcomputer zu starten, damit alle im Netzwerk verwendeten Programme berücksichtigt werden.

Überzeugen Sie sich vor dem Erstellen der Liste der Erlaubnisregeln nach Programmen, die auf dem Referenzcomputer des Unternehmens gestartet werden, dass es auf dem Referenzcomputer 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.

Standardeinstellungen der Aufgabe "Kontrolle des Programmstarts"

Die Aufgabe Kontrolle des Programmstarts weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 47. Standardeinstellungen der Aufgabe "Kontrolle des Programmstarts"

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	Nur Statistik. Die Datensätze der Aufgabe haben auf der Grundlage der festgelegten Regeln Startereignisse verboten und Startereignisse erlaubt. Der Programmstart wird nicht explizit verboten.	Sie können den Modus Aktiv auswählen, nachdem die endgültige Liste der Regeln erstellt wurde.
Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten	Wird verwendet	Sie können bei weiteren Starts dieser Datei Aktionen wiederholen, die Sie beim ersten Start der Datei angewendet haben.
Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten	Wird nicht verwendet.	Sie können den Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten.
Verwaltung von Regeln	Lokale Regeln durch Richtlinienregeln ersetzen	Sie können den Modus der gemeinsamen Anwendung der in der Richtlinie festgelegten Regeln und der Regeln auf dem lokalen Computer auswählen.
Gültigkeitsbereich der Regeln	Die Aufgabe kontrolliert den Start von ausführbaren Dateien, Skripten und MSI-Paketen. Außerdem überwacht sie das Laden von DLL-Modulen.	Sie können die Dateitypen angeben, deren Start durch die Regeln kontrolliert werden soll.

Einstellung	Standardwert	Beschreibung
Verwendung von KSN	Daten der KSN-Programmreputation werden nicht verwendet.	Sie können die Daten über die Reputation von Programmen in KSN bei der Ausführung der Aufgabe zur Kontrolle des Programmstarts verwenden.
Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben	Wird nicht verwendet.	Sie können die Softwareverteilung mithilfe der in den Einstellungen angegebenen Installationspakete und Programme erlauben. Standardmäßig ist die Verteilung der Programme nur mithilfe des Dienstes Windows Installer erlaubt.
Verteilung von Programmen mithilfe von Windows Installer immer erlauben	Übernommen (kann nur geändert werden, wenn die Einstellung Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben aktiviert ist).	Sie können die Installation oder das Update einer beliebigen Software erlauben, wenn der entsprechende Vorgang über Windows Installer ausgeführt wird.
Verteilung von Installationspaketen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben.	Übernommen (kann nur geändert werden, wenn die Einstellung Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben aktiviert ist).	Sie können die automatische Verteilung von Installationspaketen mithilfe der Softwarelösung System Center Configuration Manager aktivieren bzw. deaktivieren.
Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Kontrolle des Programmstarts wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Tabelle 48. Standardeinstellungen der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts"

Einstellung	Standardwert	Beschreibung
Präfix für Namen von Erlaubnisregeln	Entspricht dem Namen des Computers, auf dem Kaspersky Embedded Systems Security installiert ist.	Sie können das Präfix für die Namen von Erlaubnisregeln ändern.

Einstellung	Standardwert	Beschreibung
Gültigkeitsbereich der Erlaubnisregeln	Unter den Gültigkeitsbereich der Erlaubnisregeln fallen standardmäßig die folgenden Kategorien von Dateien: • Dateien mit der Erweiterung EXE, die sich in den Ordnern C:\Windows, C:\Program Files (x86) und C:\Program Files befinden • MSI-Pakete im Ordner C:\Windows • Skripte im Ordner C:\Windows Außerdem erstellt die Aufgabe Regeln für alle bereits gestarteten Programme, unabhängig von deren Speicherort und Format.	Sie können den Schutzbereich ändern, indem Sie Ordnerpfade hinzufügen oder entfernen und Typen von Dateien festlegen, deren Start durch die automatisch generierten Regeln erlaubt wird. Sie können bei der Erstellung von Erlaubnisregeln auch bereits gestartete Programme ignorieren.
Kriterien für die Erstellung von Erlaubnisregeln.	Der Header des digitalen Zertifikats und der Fingerabdrucks werden verwendet, Regeln werden für alle Benutzer und Benutzergruppen erstellt.	Sie können den SHA256-Hash bei der Erstellung von Erlaubnisregeln verwenden. Sie können einen Benutzer und eine Benutzergruppe auswählen, für die automatisch Erlaubnisregeln erstellt werden sollen.
Aktionen nach Abschluss der Aufgabe	Die Erlaubnisregeln werden der Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt; neue Regeln werden mit bestehenden Regeln zusammengeführt; doppelte Regeln werden gelöscht.	Sie können die Regeln zu den bereits existierenden Regeln hinzufügen, ohne sie zusammenzuführen und ohne doppelte Regeln zu löschen, oder bestehende Regeln durch die neuen Erlaubnisregeln ersetzen, sowie den Export der Erlaubnisregeln in eine Datei konfigurieren.
Einstellungen für den Aufgabenstart mit Rechten	Die Aufgabe wird mit den Rechten des Systemkontos gestartet.	Sie können den Start der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" unter einem Systemkontos erlauben oder die Rechte eines angegebenen Benutzers verwenden.

Einstellung	Standardwert	Beschreibung
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Kontrolle des Programmstarts über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Aufgabeneinstellungen für einen oder alle Computer im Netzwerk konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Richtlinieneinstellungen für die Aufgabe zur Kontrolle des Programmstarts öffnen

► *Um die Aufgabeneinstellungen für die Kontrolle des Programmstarts über die Richtlinie von Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt Überwachung der Desktop-Aktivitäten.
6. Klicken Sie auf die Schaltfläche Einstellungen im Unterabschnitt Kontrolle des Programmstarts.

   Das Fenster Kontrolle des Programmstarts wird geöffnet.

Konfigurieren Sie die Richtlinie nach Bedarf.

Regelliste für die Kontrolle des Programmstarts öffnen

► *Um die Regelliste für die Kontrolle des Programmstarts über das Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt Überwachung der Desktop-Aktivitäten.
6. Klicken Sie auf die Schaltfläche Einstellungen im Unterabschnitt Kontrolle des Programmstarts.

   Das Fenster Kontrolle des Programmstarts wird geöffnet.
7. Klicken Sie auf der Registerkarte Allgemein auf Regelliste.

   Das Fenster Regeln für die Kontrolle des Programmstarts wird geöffnet.

Konfigurieren Sie die Regelliste nach Bedarf.

Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen

► *Um mit dem Erstellen einer Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu beginnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe**geöffnet.
5. Wählen Sie den untergeordneten Knoten Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts.
6. Klicken Sie auf **Weiter**.

   Das Fenster Einstellungen wird geöffnet.

► *Um der bestehenden Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben von Kaspersky Security Center.

   Daraufhin wird das Fenster **Eigenschaften: Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** geöffnet.

Details darüber, wie Sie die Aufgabe konfigurieren, finden Sie im Abschnitt Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren.

Aufgabeneinstellungen für Kontrolle des Programmstarts konfigurieren

► *Um die allgemeinen Aufgabeneinstellungen für die Kontrolle des Programmstarts zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Kontrolle des Programmstarts (siehe Abschnitt "**Richtlinieneinstellungen für die Aufgabe zur Kontrolle des Programmstarts öffnen**" auf Seite 318).
2. Wählen Sie auf der Registerkarte Allgemein im Abschnitt Modus folgende Einstellungen:
   - Geben Sie in der Dropdown-Liste Aufgabenmodus den Aufgabenmodus an.

     In dieser Dropdown-Liste können Sie den Modus der Aufgabe zur Kontrolle des Programmstarts auswählen:

- Aktiv. Kaspersky Embedded Systems Security verwendet die festgelegten Regeln, um den Start jedes Programms zu kontrollieren.
- Nur Statistik. Kaspersky Embedded Systems Security verwendet die festgelegten Regeln nicht, um den Start von Programmen zu kontrollieren. Stattdessen werden Informationen über Startereignisse im Protokoll der Aufgabenausführung aufgezeichnet. 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 Aufgabenausführung enthaltenen Informationen über verbotene Programmstarts verwenden.

Standardmäßig wird die Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik gestartet.

- Deaktivieren oder aktivieren Sie das Kontrollkästchen Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten.

  Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle wiederholter Programmstarts auf Basis von Einträgen des Caches für Ereignisinformationen.

  Wenn das Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security nachfolgende Starts eines Programms auf der Grundlage der Einstufung der Aufgabe in Bezug auf den ersten Start des Programms. 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.

  Ist das Kontrollkästchen deaktiviert, so analysiert Kaspersky Embedded Systems Security ein Programm bei jedem versuchten Programmstart von neuem.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Deaktivieren oder aktivieren Sie das Kontrollkästchen Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten.

  Wenn das Kontrollkästchen aktiviert ist, verbietet Kaspersky Embedded Systems Security den Start des Kommandozeileninterpreters auch dann, wenn der Start von Interpretern erlaubt ist. Ein Kommandozeileninterpreter kann ohne Befehl nur dann gestartet werden, wenn beide der folgenden Bedingungen erfüllt sind:

  - Der Start des Kommandozeileninterpreters ist erlaubt.
  - Der auszuführende Befehl ist erlaubt.

  Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security nur Erlaubnisregeln, wenn ein Kommandozeileninterpreter gestartet wird. Der Start wird verboten, wenn keine Erlaubnisregel übernommen wurde oder der ausführbare Prozess laut KSN nicht vertrauenswürdig ist. Wenn eine Erlaubnisregel übernommen wird oder der Prozess laut KSN vertrauenswürdig ist, kann ein Kommandozeileninterpreter mit oder ohne auszuführenden Befehl gestartet werden.

  Kaspersky Embedded Systems Security erkennt die folgenden Kommandozeileninterpreter:

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

  Das Kontrollkästchen ist standardmäßig deaktiviert.

3. Passen Sie im Abschnitt Regelverwaltung die Einstellungen für die Anwendung der Regeln an:

   a. Klicken Sie auf die Schaltfläche **RegellisteRegelliste**, um Erlaubnisregeln zur Kontrolle des Aufgabenstarts hinzuzufügen.

   > Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie den Backslash ("\"), um den Pfad korrekt einzutragen.

   b. Wählen Sie den Modus für die Anwendung der Regeln aus:

   - Lokale Regeln durch Richtlinienregeln ersetzen.

     Das Programm wendet die in der Richtlinie festgelegte Regelliste für die zentralisierte Kontrolle des Programmstarts auf der Computergruppe an. Das Erstellen, Bearbeiten und Anwenden der lokalen Regellisten ist nicht verfügbar.

   - Richtlinienregeln zu lokalen Regeln hinzufügen.

     Das Programm wendet die in der Richtlinie festgelegte Regelliste zusammen mit den lokalen Regellisten an. Sie können die lokalen Regellisten mithilfe der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" bearbeiten.

   > Standardmäßig übernimmt Kaspersky Embedded Systems Security zwei vordefinierte Regeln, die eine Liste von Skripts, MSI-Paketen und ausführbaren Dateien erlauben, wenn diese Objekte mit einer vertrauenswürdigen digitalen Signatur unterzeichnet sind.

4. Nehmen Sie im Abschnitt Gültigkeitsbereich der Regeln die folgenden Einstellungen vor:

   - Regeln für ausführbare Dateien verwenden.

     Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von ausführbaren Dateien.

     Ist dieses Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security den Start ausführbarer Dateien mithilfe vorgegebener Regeln, in deren Einstellungen Ausführbare Dateien als Geltungsbereich angegeben ist.

     Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Starts ausführbarer Dateien mithilfe vorgegebener Regeln. Der Start ausführbarer Dateien ist erlaubt.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Laden von DLL-Modulen überwachen.

     Dieses Kontrollkästchen aktiviert oder deaktiviert die Überwachung des Ladens von DLL-Modulen.

     Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security das Laden von DLL-Modulen mithilfe vorgegebener Regeln, in deren Einstellungen Ausführbare Dateien als Geltungsbereich angegeben sind.

     Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Ladens von DLL-Modulen mithilfe vorgegebener Regeln. Laden von DLL-Modulen ist erlaubt.

     Das Kontrollkästchen ist aktiv, wenn das Kontrollkästchen Regeln für ausführbare Dateien verwenden aktiviert ist.

Das Kontrollkästchen ist standardmäßig deaktiviert.

Das Überwachen des Ladens von DLL-Modulen kann sich auf die Leistung des Betriebssystems auswirken.

- Regeln für Skripte und MSI-Pakete verwenden.

  Dieses Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von Skripten und MSI-Paketen.

  Wenn dieses Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security den Start von Skripten und MSI-Paketen mithilfe vorgegebener Regeln, in deren Einstellungen Skripte und MSI-Pakete als Geltungsbereich angegeben sind.

  Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Starts von Skripten und MSI-Paketen mithilfe vorgegebener Regeln. Das Ausführen von Skripten und MSI-Paketen ist gestattet.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

5. Passen Sie in der Gruppe Verwendung von KSN die folgenden Einstellungen des Programmstarts an:

   - Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten.

     Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß der Programmreputation in KSN.

     Ist das Kontrollkästchen aktiviert, blockiert Kaspersky Embedded Systems Security den Start aller Programme, die laut KSN nicht vertrauenswürdig sind. Erlaubnisregeln zur Kontrolle des Programmstarts, die für Programme gelten, die laut KSN nicht vertrauenswürdig sind, werden nicht ausgelöst. Die Aktivierung des Kontrollkästchens gewährleistet zusätzlichen Schutz vor Schadsoftware.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security die Reputation von Programmen, die laut KSN nicht vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die für diese Programme gelten.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben.

     Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß der Programmreputation in KSN.

     Ist das Kontrollkästchen aktiviert, erlaubt Kaspersky Embedded Systems Security den Start von Programmen, wenn sie laut KSN vertrauenswürdig sind. Dabei haben die Verbotsregeln für die Kontrolle des Programmstarts, die für die im KSN vertrauenswürdigen Programme gelten, eine höhere Priorität: wenn ein Programm laut den KSN-Diensten vertrauenswürdig ist, wird der Programmstart verboten.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security die Reputation von Programmen, die laut KSN vertrauenswürdig sind, nicht und erlaubt oder verbietet den Start in Übereinstimmung mit den Regeln, die für solche Programme gelten.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - Benutzer und/oder Benutzergruppen, denen der Start von Programmen, die laut KSN vertrauenswürdig sind, erlaubt ist.

6. Passen Sie auf der Registerkarte Kontrolle für Installationspakete die Einstellungen für die Kontrolle für Installationspakete an (siehe Abschnitt "Konfiguration der Kontrolle für Installationspakete" auf Seite 324).
7. Passen Sie auf der Registerkarte Aufgabenverwaltung die geplanten Einstellungen für den Aufgabenstart an (siehe Abschnitt "Einstellungen für den Zeitplan für den Aufgabenstart anpassen" auf Seite 139).
8. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Konfiguration der Kontrolle für Installationspakete

► *Um ein vertrauenswürdiges Installationspaket hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Kontrolle des Programmstarts (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zur Kontrolle des Programmstarts öffnen" auf Seite 318).
2. Aktivieren Sie auf der Registerkarte Kontrolle für Installationspakete das Kontrollkästchen Verteilung der unten gelisteten Programme und Installationspakete automatisch erlauben.

   Dieses Kontrollkästchen aktiviert/deaktiviert die Möglichkeit, automatisch Ausnahmen für alle Dateien zu erstellen, die mithilfe der in der Liste angegebenen Programme und Installationspakete gestartet werden.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt das Programm automatisch den Start von Dateien, die von vertrauenswürdigen Installationspaketen gestartet wurden. Die Liste der für den Start freigegebenen Programme und Installationspakete kann bearbeitet werden.

   Wenn das Kontrollkästchen deaktiviert ist, verwendet das Programm die in der Liste angegebenen Ausnahmen nicht.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

   Sie können das Kontrollkästchen Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben aktivieren, wenn das Kontrollkästchen Regeln für ausführbare Dateien verwenden auf der Registerkarte Allgemein in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts aktiviert ist.

3. Deaktivieren Sie bei Bedarf das Kontrollkästchen Verteilung von Programmen mithilfe von Windows Installer immer erlauben.

   Dieses Kontrollkästchen aktiviert/deaktiviert die Möglichkeit, Ausnahmen für alle Dateien, die mithilfe von Windows Installer gestartet werden, automatisch zu erstellen.

   Wenn das Kontrollkästchen aktiviert ist, ist der Start von Dateien, die mithilfe von Windows Installer installiert wurden, immer erlaubt.

   Ist das Kontrollkästchen deaktiviert, dürfen Dateien nicht bedingungslos gestartet werden, selbst wenn Sie über Windows Installer gestartet werden.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Dieses Kontrollkästchen kann nicht bearbeitet werden, wenn das Kontrollkästchen Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben nicht aktiviert ist.

Das Kontrollkästchen Verteilung von Programmen mithilfe von Windows Installer immer erlauben sollte nur deaktiviert werden, wenn dies absolut notwendig ist. 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.

4. Aktivieren Sie bei Bedarf das Kontrollkästchen Verteilung von Programmen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben.

   Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Erlauben der Verteilung von Software mithilfe der Softwarelösung System Center Configuration Manager.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt Kaspersky Embedded Systems Security automatisch die Verteilung von Microsoft Windows mithilfe von System Center Configuration Manager. Das Programm erlaubt die Verteilung von Software nur mithilfe des intelligenten Hintergrundübertragungsdienstes (Background Intelligent Transfer Service).

   Das System überwacht den Start von Objekten mit folgenden Erweiterungen:

   - .exe
   - .msi

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an den Computer bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation des Systems auf dem Computer ausgeführt wurde.

5. Um die Liste der vertrauenswürdigen Installationspakete zu bearbeiten, klicken Sie auf die Schaltfläche Liste der Pakete bearbeiten und wählen Sie im nächsten Fenster eine der verfügbaren Methoden aus:

   - Ein Installationspaket hinzufügen.
     a. Klicken Sie auf die Schaltfläche Durchsuchen und wählen Sie die ausführbare Datei oder das Installationspaket aus.

        Im Abschnitt Kriterien für Vertrauenswürdigkeit werden die Daten zur ausgewählten Datei automatisch angezeigt.

     b. Aktivieren oder deaktivieren Sie das Kontrollkästchen Den Start von Dateien in allen Ebenen dieses Installationspakets erlauben.

     c. Wählen Sie eine der beiden verfügbaren Varianten der Kriterien für die Vertrauenswürdigkeit aus, auf deren Grundlage die Datei oder das Installationspaket als vertrauenswürdig gelten:

        - Digitales Zertifikat verwenden
        - SHA256-Hash verwenden.
   - Mehrere Pakete anhand von Hash hinzufügen.

Sie können eine unbegrenzte Anzahl an ausführbaren Dateien und Installationspaketen auswählen und gleichzeitig zur Liste hinzufügen. Kaspersky Embedded Systems Security untersucht den Hash und erlaubt dem Betriebssystem den Start der angegebenen Dateien.

- Ausgewähltes Paket bearbeiten.

  Verwenden Sie diese Variante, um eine andere ausführbare Datei oder ein anderes Installationspaket auszuwählen sowie die Kriterien für die Vertrauenswürdigkeit zu ändern.

- Liste mit Paketen aus Datei importieren.

  Sie können die Liste der vertrauenswürdigen Installationspakete aus einer Konfigurationsdatei importieren. Damit eine solche Datei von Kaspersky Embedded Systems Security erkannt wird, muss sie folgende Voraussetzungen erfüllen:

  - Die Dateierweiterung lautet TXT.
  - Die Datei muss Informationen in Form einer Liste mit Zeilen enthalten, von denen jede die Daten einer einzigen vertrauenswürdigen Datei enthält.
  - Die Datei muss eine Liste enthalten, die einem von zwei Formaten entspricht:
    - <Dateiname>:<SHA256-Hash>.
    - <SHA256-Hash>*<Dateiname>.

  Geben Sie im Fenster **Öffnen** die Konfigurationsdatei mit der Liste der vertrauenswürdigen Installationspakete an.

6. Wenn Sie ein früher hinzugefügtes Programm oder Installationspaket aus der Liste der vertrauenswürdigen Installationspakete löschen möchten, klicken Sie auf die Schaltfläche Installationspakete löschen. Der Start extrahierter Dateien wird erlaubt.

   Um den Start extrahierter Dateien zu verbieten, deinstallieren Sie das Programm vollständig vom geschützten Computer oder erstellen Sie eine Verbotsregel in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts.

7. Klicken Sie auf **OK**.

Ihre neu konfigurierten Einstellungen werden gespeichert.

Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren

► *Gehen Sie wie folgt vor, um die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren:*

1. Öffnen Sie das Fenster **Eigenschaften: Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** (siehe Abschnitt "**Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen**" auf Seite 319).
2. 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*.

3. Im Abschnitt **Einstellungen** können Sie die folgenden Einstellungen konfigurieren:
   - Fügen Sie ein Präfix für Regelnamen hinzu.
   - Konfigurieren Sie den Gültigkeitsbereich der Erlaubnisregeln:
     - Erlaubnisregeln auf Grundlage gestarteter Programme erstellen.
     - Erlaubnisregeln für Programme aus den bestimmten Ordnern erstellen.
4. Im Abschnitt **Einstellungen**können Sie Aktionen festlegen, die bei der Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen:
   - 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. Anschließend erlaubt das Programm den Start von Programmen mithilfe von 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.

Diese Variante gilt als Standard.

- Header und Fingerabdruck des digitalen Zertifikats verwenden

  Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers und des Fingerabdrucks des digitalen Zertifikats der Datei als ein Auslösekriterium für die Erlaubnisregeln für die Kontrolle des Programmstarts. Die Aktivierung dieses Kontrollkästchens ermöglicht die Festlegung strengerer Bedingungen für die Untersuchung digitaler Zertifikate.

  Ist das Kontrollkästchen aktiviert, werden die Werte des Headers und des Fingerabdrucks des digitalen Zertifikats der Dateien, für welche die Regeln erstellt werden, als ein Kriterium für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts festgelegt. Kaspersky Embedded Systems Security erlaubt Programme, die mithilfe von Dateien mit dem angegebenen Fingerabdruck digitalem Zertifikat gestartet werden.

  Die Verwendung dieses Kontrollkästchens stellt eine starke Einschränkung für das Auslösen von Erlaubnisregeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles fälschungssicheres Identifikationsmerkmal eines digitalen Zertifikats handelt.

  Ist das Kontrollkästchen deaktiviert, so wird als ein Kriterium für das Auslösen der Erlaubnisregeln zur Kontrolle des Programmstarts das Vorliegen eines beliebigen digitalen Zertifikats festgelegt, das im Betriebssystem als vertrauenswürdig eingestuft ist.

  Das Kontrollkästchen ist aktiv, wenn die Option Digitales Zertifikat verwenden ausgewählt ist.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Falls kein Zertifikat vorhanden, Folgendes verwenden

  Es handelt sich um eine Dropdown-Liste, welche die Auswahl der Kriterien für das Auslösen einer Erlaubnisregel für die Kontrolle des Programmstarts für den Fall erlaubt, dass die Datei, auf deren Grundlage die Regel erstellt wird, über kein digitales Zertifikat verfügt.

- SHA256-Hash. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.
- Dateipfad. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm keinen Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle Erlaubnisregeln für Programme aus folgenden Ordnern erstellen im Abschnitt Einstellungen angegeben wurden.

- 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. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.

Diese Option wird für Fälle empfohlen, in denen die generierten Regeln die höchste Sicherheitsstufe erreichen müssen: als eindeutige Datei-ID kann eine SHA256-Prüfsumme verwendet werden. Die Verwendung einer SHA256-Prüfsumme als Auslösekriterium für die Regel beschränkt den Gültigkeitsbereich der Regel auf eine Datei.

Diese Option ist standardmäßig deaktiviert.

- Regeln für Benutzer oder Benutzergruppe erstellen

  Es handelt sich um ein Feld, in dem der Benutzer oder die Benutzergruppe angegeben sind. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer oder die angegebene Benutzergruppe.

  Standardmäßig ist die Gruppe **Alle** eingestellt.

Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.

1. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
2. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
3. 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 Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center*

4. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**.

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Konfiguration von Regeln für die Kontrolle des Programmstarts über das Kaspersky Security Center

Erfahren Sie, wie Sie auf der Grundlage von verschiedenen Kriterien eine Liste von Regeln erzeugen oder mithilfe der Aufgabe zur Kontrolle des Programmstarts manuell Erlaubnis- oder Verbotsregeln erstellen können.

In diesem Abschnitt

Regel für die Kontrolle des Programmstarts hinzufügen

► *Um eine Regel für die Kontrolle des Programmstarts hinzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Kontrolle des Programmstarts (siehe Abschnitt "Regelliste für die Kontrolle des Programmstarts öffnen" auf Seite 319).
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt Eine Regel hinzufügen aus.

   Es öffnet sich das Fenster Einstellungen der Regel.
4. Geben Sie die folgenden Einstellungen an:
   a. Geben Sie im Feld Name den Namen der Regel an.
   b. Wählen Sie in der Dropdown-Liste Typ den Typ der Regel:
      - Erlaubnis, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien erlaubt.
      - Verbot, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien verbietet.
   c. Wählen Sie in der Dropdown-Liste Gültigkeitsbereich 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.
   d. Geben Sie im Feld Benutzer und/oder Benutzergruppe die Benutzer an, denen der Programmstart in Übereinstimmung mit dem Regeltyp erlaubt oder verboten werden soll. Gehen Sie hierzu wie folgt vor:
      i. Klicken Sie auf die Schaltfläche Durchsuchen.

ii. Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** wird geöffnet.

iii. Geben Sie die Liste der Benutzer und/oder Benutzergruppen an.

iv. Klicken Sie auf **OK**.

e. Gehen Sie wie folgt vor, wenn Sie die Werte für die im Abschnitt Auslösekriterien für Regeln genannten Auslösekriterien der Regel aus einer Datei entnehmen möchten:

i. Klicken Sie auf die Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben.

Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.

ii. Wählen Sie die Datei aus.

iii. Klicken Sie auf **Öffnen**.

Die Werte der Kriterien in der Dateien werden in den Feldern im Abschnitt Auslösekriterien für Regeln angezeigt. Standardmäßig wird das erste Kriterium der Liste ausgewählt, dessen Daten in den Dateieigenschaften enthalten sind.

f. Wählen Sie im Abschnitt Auslösekriterien für Regeln eine der folgenden Optionen aus:

- Digitales Zertifikat, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, welche mit einem digitalen Zertifikat signiert sind:
  - Aktivieren Sie das Kontrollkästchen Header verwenden, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit dem angegebenen Header signiert sind.
  - Aktivieren Sie das Kontrollkästchen Fingerabdruck verwenden, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.
- SHA256-Hash, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, deren Prüfsumme dem angegebenen Wert entspricht.
- Dateipfad, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, die sich unter dem angegebenen Dateipfad befinden.

> Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie den Backslash ("\"), um den Pfad korrekt einzutragen.

g. Gehen Sie wie folgt vor, wenn Sie Ausnahmen von den Regeln hinzufügen möchten:

i. Klicken Sie im Abschnitt Ausnahmen von der Regel auf **Hinzufügen**.

Es öffnet sich das Fenster Ausnahme von der Regel.

ii. Geben Sie im Feld Name den Namen der Ausnahme ein.

iii. Geben Sie die Einstellungen für die Ausnahme von Programmdateien von den Regeln für die Kontrolle des Programmstarts an. Sie können die Felder mit den Parametern aus den Dateieigenschaften über die Schaltfläche Ausnahme auf Grundlage der Dateieigenschaften festlegen ausfüllen.

- Digitales Zertifikat

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. Anschließend erlaubt das Programm den Start von Programmen mithilfe von 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.

Diese Variante gilt als Standard.

- Header verwenden

  Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers digitaler Zertifikate als Auslösekriterium für die Regel.

  Ist das Kontrollkästchen aktiviert, wird der angegebene Header des digitalen Zertifikats als Auslösekriterium für die Regel verwendet. Die erstellte Regel kontrolliert den Start von Programmen dann lediglich für den im Header genannten Hersteller.

  Ist das Kontrollkästchen deaktiviert, verwendet das Programm den Header des digitalen Zertifikats nicht als Auslösekriterium für die Regel. Ist das Kriterium Digitales Zertifikat ausgewählt, kontrolliert die erstellte Regel Starts von Programmen, die mit einem digitalen Zertifikat mit beliebigem Header signiert sind.

  Den Header des digitalen Zertifikats, mit dem die Datei signiert ist, können Sie nur aus den Eigenschaften der ausgewählten Datei mithilfe der Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben oberhalb des Abschnitts Auslösekriterien für Regeln auswählen.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

- Fingerabdruck verwenden

  Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Fingerabdrucks digitaler Zertifikate als Auslösekriterium für die Regel.

  Ist das Kontrollkästchen aktiviert, wird der angegebene Fingerabdruck des digitalen Zertifikats als Auslösekriterium für die Regel verwendet. Die erstellte Regel kontrolliert dann den Start von Programmen, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.

  Ist das Kontrollkästchen deaktiviert, verwendet das Programm den Fingerabdruck des digitalen Zertifikats nicht als Auslösekriterium für die Regel. Ist das Kriterium Digitales Zertifikat ausgewählt, kontrolliert das Programm Starts von Programmen, die mit einem digitalen Zertifikat mit beliebigem Fingerabdruck signiert sind.

  Den Fingerabdruck des digitalen Zertifikats, mit dem die Datei signiert ist, können Sie nur aus den Eigenschaften der ausgewählten Datei mithilfe der Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben oberhalb des Abschnitts Auslösekriterien für Regeln auswählen.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

- SHA256-Hash

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. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.

Diese Option wird für Fälle empfohlen, in denen die generierten Regeln die höchste Sicherheitsstufe erreichen müssen: als eindeutige Datei-ID kann eine SHA256-Prüfsumme verwendet werden. Die Verwendung einer SHA256-Prüfsumme als Auslösekriterium für die Regel beschränkt den Gültigkeitsbereich der Regel auf eine Datei.

Diese Option ist standardmäßig deaktiviert.

- Dateipfad

  Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den vollständigen Ordnerpfad, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

  Wenn diese Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

i. Klicken Sie auf OK.

ii. Wiederholen Sie die Schritte (i)-(iv), wenn Sie zusätzliche Ausnahmen hinzufügen möchten.

1. Klicken Sie im Fenster Einstellungen der Regel auf OK.

Die erstellte Regel wird in der Liste im Fenster Regeln für die Kontrolle des Programmstarts angezeigt.

Standarderlaubnismodus aktivieren

Der Standarderlaubnismodus erlaubt den Start aller Programme, sofern diese nicht durch Regeln, oder durch eine KSN-Einstufung als "nicht vertrauenswürdig", blockiert sind. Der Standarderlaubnismodus kann durch Hinzufügen bestimmter Erlaubnisregeln aktiviert werden. Sie können den Standarderlaubnismodus nur für Skripte oder für alle ausführbaren Dateien aktivieren.

► *Um eine Standarderlaubnisregel hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Kontrolle des Programmstarts (siehe Abschnitt "**Regelliste für die Kontrolle des Programmstarts öffnen**" auf Seite 319).
2. Klicken Sie auf die Schaltfläche Hinzufügen und wählen Sie aus dem Kontextmenü der Schaltfläche die Option Eine Regel hinzufügen.

   Es öffnet sich das Fenster Einstellungen der Regel.
3. Geben Sie im Feld Name den Namen der Regel an.
4. Wählen Sie in der Dropdown-Liste Typ den Regel-Typ Erlaubnis aus.
5. Wählen Sie in der Dropdown-Liste Gültigkeitsbereich den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:
   - Ausführbare Dateien, wenn Sie möchten, dass die Regel den Start ausführbarer Programmdateien kontrolliert.
   - Skripte und MSI-Pakete, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.
6. Wählen Sie im Abschnitt Auslösekriterien für Regeln die Option Dateipfad aus.
7. Geben Sie die folgende Maske ein: `?:\`
8. Klicken Sie im Fenster Einstellungen der Regel auf OK.

Kaspersky Embedded Systems Security übernimmt den Standarderlaubnismodus.

Erlaubnisregeln aus Ereignissen in Kaspersky Security Center erstellen

► *Um Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center in der Kontrolle des Programmstarts zu erzeugen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Kontrolle des Programmstarts (siehe Abschnitt "**Regelliste für die Kontrolle des Programmstarts öffnen**" auf Seite 319).
2. Klicken Sie auf die Schaltfläche Hinzufügen und wählen Sie im Kontextmenü der Schaltfläche die Option Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center erstellen.
3. Wählen Sie das Prinzip aus, nach dem Regeln zur Liste der bereits festgelegten 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.
   - Mit bestehenden 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.
4. Passen Sie die folgenden Einstellungen für Anfragen an:
   - Adresse des Administrationsservers
   - Port
   - Benutzer
   - Kennwort
5. Wählen Sie den Typ von Ereignissen aus, die von der Aufgabe zum Erstellen von Regeln verwendet werden sollen:
   - Modus "Nur Statistik" Programmstart verboten
   - Programmstart verboten
6. Wählen Sie den Zeitraum aus der Dropdown-Liste In diesem Zeitraum erstellte Ereignisse anfordern.
7. Klicken Sie auf die Schaltfläche Regeln erstellen.
8. Klicken Sie auf die Schaltfläche Speichern im Fenster Regeln für die Kontrolle des Programmstarts.

   Die Regelliste in der Aufgabe zur Kontrolle des Programmstarts wird mit neuen Regeln geladen, basierend auf den Systemdaten des Computers mit der installierten Verwaltungskonsole von Kaspersky Security Center.

   Wenn die Liste der Regeln für die Kontrolle des Programmstarts bereits in der Richtlinie festgelegt ist, fügt Kaspersky Embedded Systems Security die ausgewählten Regeln aus den Blockierungsereignissen zu den schon angegebenen Regeln hinzu. Regeln mit demselben Hash werden nicht hinzugefügt, da alle Regeln in der Liste eindeutig sein müssen.

Regeln aus einem Bericht von Kaspersky Security Center über blockierte Programme importieren

Sie können Daten über blockierte Programmstarts aus einem Bericht importieren, der in Kaspersky Security Center nach der Ausführung der Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik erstellt wurde, und diese Daten zur Erstellung einer Liste von Erlaubnisregeln für die Kontrolle des Programmstarts in der konfigurierten Richtlinie verwenden.

Bei der Berichterstellung über Ereignisse, die während der Ausführung der Aufgabe zur Kontrolle des Programmstarts eintreten, können Sie verfolgen, für welche Programme der Start blockiert wird.

Vergewissern Sie sich beim Import von Daten aus einem Bericht über blockierte Programme in die Richtlinieneinstellungen davon, dass die verwendete Liste nur diejenigen Programme beinhaltet, deren Start Sie erlauben möchten.

► *Um für eine Gruppe von Computern Erlaubnisregeln zur Kontrolle des Programmstarts auf der Grundlage eines Berichts über blockierte Programme aus Kaspersky Security Center festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Kontrolle des Programmstarts (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zur Kontrolle des Programmstarts öffnen" auf Seite 318).
2. Wählen Sie im Abschnitt Aufgabenmodus den Modus Nur Statistik aus.
3. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisbenachrichtigungen**, dass:
   - Für **Kritische Ereignisse** die Speicherdauer des Protokolls der Aufgabenausführung für Programmstart verboten-Ereignisse die geplante Zeitspanne für die Ausführung der Aufgabe im Modus Nur Statistik übersteigt (der Standardwert beträgt 30 Tage).
   - Für Ereignisse mit einer Prioritätsstufe von **Warnung** die Speicherdauer des Protokolls der Aufgabenausführung für Nur Statistik: Programmstart verboten-Ereignisse die geplante Zeitspanne für die Ausführung der Aufgabe im Modus Nur Statistik übersteigt (der Standardwert beträgt 30 Tage).

     Nach Ablauf der Speicherdauer für Ereignisse werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in der Protokolldatei aufgeführt. Vergewissern Sie sich vor dem Start der Aufgabe Kontrolle des Programmstarts im Modus Nur Statistik, dass die Ausführungsdauer der Aufgabe die festgelegte Zeitspanne für die angegebenen Ereignisse nicht überschreitet.
4. Exportieren Sie nach Abschluss der Aufgabe die protokollierten Ereignisse in eine TXT-Datei:
   a. Wählen Sie im Arbeitsbereich des Knotens **Administrationsserver** in Kaspersky Security Center die Registerkarte **Ereignisse** aus.
   b. Erstellen Sie im untergeordneten Knoten **Auswahl erstellen** eine Auswahl von Ereignissen anhand der Eigenschaft *Blockiert*, um zu sehen, welche Programmstarts durch die Aufgabe zur Kontrolle des Programmstarts blockiert werden.
   c. Klicken Sie im Ergebnisbereich der Auswahl auf den Link **Ereignisse in Dateiliste exportieren**, um einen Bericht über die blockierten Programmstarts in einer txt-Datei zu speichern.

Vergewissern Sie sich vor dem Import und der Verwendung des erstellten Berichts in einer Richtlinie, dass der Bericht nur Daten derjenigen Programme enthält, deren Start Sie erlauben möchten.

5. Importieren Sie die Daten über blockierte Programmstarts in die Aufgabe zur Kontrolle des Programmstarts. Gehen Sie dazu in den Eigenschaften der Richtlinie in den Einstellungen der Aufgabe Kontrolle des Programmstarts wie folgt vor:

   a. Klicken Sie auf der Registerkarte Allgemein auf Regelliste.

      Das Fenster Regeln für die Kontrolle des Programmstarts wird geöffnet.

   b. Klicken Sie auf die Schaltfläche Hinzufügen und wählen Sie im Kontextmenü der Schaltfläche den Punkt Importieren der Daten über blockierte Programme aus dem Bericht von Kaspersky Security Center.

   c. Wählen Sie das Prinzip aus, nach dem die Regeln aus der auf Grundlage des Berichts von Kaspersky Security Center erstellten Liste zur Liste der bereits bestehenden Regeln für die Kontrolle des Programmstarts hinzugefügt werden:

      - 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.
      - Mit bestehenden 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.

   d. Wählen Sie folgenden Windows-Standardfenster die txt-Datei aus, in die Ereignisse aus dem Bericht über den gesperrten Programmstart exportiert wurden.

   e. Klicken Sie auf die Schaltfläche **OK** im Fenster Regeln für die Kontrolle des Programmstarts und im Fenster **Aufgabeneinstellungen**.

Die auf Grundlage des Berichts von Kaspersky Security Center über die blockierten Programme erstellten Regeln werden zur Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt.

Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren

Sie können Berichte, die von der Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" erstellt wurden, importieren und als Liste mit Erlaubnisregeln in der konfigurierten Richtlinie verwenden.

Nach Abschluss der Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" exportiert das Programm die erstellten Erlaubnisregeln in Form von XML-Dateien in den freigegebenen Ordner. Jede Datei mit einer Regelliste wird durch eine Analyse des Starts der Dateien und Programme auf jedem einzelnen Computer des Unternehmensnetzwerks erstellt. Die Listen enthalten Erlaubnisregeln für den Start von Dateien und Programmen, deren Typ den in den Einstellungen der Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" gemachten Angaben entspricht.

► *Um Erlaubnisregeln zur Kontrolle des Programmstarts für eine Gruppe von Computern auf der Grundlage automatisch erstellter Liste von Erlaubnisregeln festzulegen, gehen Sie wie folgt vor:*

1. Erstellen Sie auf der Registerkarte **Aufgaben** in der Systemsteuerung der Gruppe von Computern, die Sie konfigurieren, eine Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" oder wählen Sie eine bestehende Aufgabe aus (siehe Abschnitt "Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen" auf Seite 319).
2. Konfigurieren Sie in den Eigenschaften der erstellten Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" oder im Assistenten für neue Aufgaben die folgenden Einstellungen:
   - Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für die Speicherung des Berichts über die Aufgabenausführung.

     Eine ausführliche Anleitung zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
   - Legen Sie im Abschnitt **Einstellungen** die Programmtypen fest, deren Start durch die erstellten Regeln erlaubt werden soll. Sie können auch die Zusammensetzung der Ordner ändern, aus denen ein Programmstart erlaubt ist: Standard-Ordner aus dem Gültigkeitsbereich der Aufgabe ausschließen und neue Ordner manuell hinzufügen.
   - Legen Sie im Abschnitt **Einstellungen** die Vorgänge fest, die von der Aufgabe während ihrer Ausführung und nach ihrem Abschluss durchgeführt werden sollen. Legen Sie das Regelerzeugungskriterium und den Namen der Datei fest, in die die erzeugten Regeln exportiert werden.
   - Passen Sie im Abschnitt **Zeitplan** die Zeitplan-Einstellungen für den Aufgabenstart.
   - Geben Sie im Abschnitt **Benutzerkonto** das Benutzerkonto an, mit dessen Rechten die Aufgabe ausgeführt werden soll.
   - Geben Sie im Abschnitt **Ausnahmen vom Gültigkeitsbereich der Aufgabe** diejenigen Computergruppen an, die aus dem Gültigkeitsbereich der Aufgabe ausgeschlossen werden sollen.

     Kaspersky Embedded Systems Security erstellt keine Erlaubnisregeln für Programme, die auf ausgeschlossenen Computern gestartet werden.
3. Wählen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Computergruppe in der Liste der Gruppenaufgaben die erstellte Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" aus und klicken Sie auf die Schaltfläche **Starten**, um die Aufgabe zu starten.

   Wenn die Aufgabe abgeschlossen ist, werden die automatisch generierten Listen von Erlaubnisregeln in XML-Dateien in einem freigegebenen Ordner gespeichert.

Stellen Sie vor der Verwendung der Aufgabe Kontrolle des Programmstarts im Netzwerk sicher, dass alle geschützten Computer Zugriff auf einen freigegebenen Ordner haben. Falls die Verwendung eines freigegebenen Ordners im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" auf einem Computer in der Test-Computergruppe oder auf einem Referenzcomputer zu starten.

4. Um die erstellten Listen mit Erlaubnisregeln zur Aufgabe zur Kontrolle des Programmstarts hinzuzufügen, gehen Sie wie folgt vor:
   a. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts** (siehe Abschnitt "Regelliste für die Kontrolle des Programmstarts öffnen" auf Seite 319).
   b. Klicken Sie auf **Hinzufügen** und wählen Sie in der folgenden Liste den Punkt **Regeln aus XML-Datei importieren** aus.
   c. Wählen Sie das Prinzip aus, nach dem automatisch erstellte Erlaubnisregeln der Liste der bereits festgelegten 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.
      - Mit bestehenden 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.
   d. Wählen Sie im erscheinenden Standardfenster von Windows die XML-Dateien aus, die nach Abschluss der Gruppenaufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" erstellt wurden.
   e. Klicken Sie auf die Schaltfläche **OK** im Fenster **Regeln für die Kontrolle des Programmstarts** und im Fenster **Aufgabeneinstellungen**.
5. Wenn Sie die erstellten Kontrollregeln für den Start von Programmen übernehmen möchten, wählen Sie in den Eigenschaften der Aufgabe "Kontrolle des Programmstarts" in der Richtlinie den Modus **Aktiv** für die Aufgabe aus.

Automatisch auf Grundlage der Aufgabenstarts auf jedem einzelnen Computer erstellte Erlaubnisregeln werden für alle Computer im Netzwerk, auf denen die konfigurierte Richtlinie übernommen wird, übernommen. Auf diesen Computern erlaubt das Programm nur den Start derjenigen Programme, für die Erlaubnisregeln erstellt wurden.

Programmstarts testen

Bevor Sie die konfigurierten Regeln für die Kontrolle des Programmstarts übernehmen, können Sie ein beliebiges Programm testen, um zu bestimmen, welche Regeln für die Kontrolle des Programmstarts durch dieses Programm ausgelöst werden.

Standardmäßig verbietet Kaspersky Embedded Systems Security den Start von Programmen, deren Start nicht durch eine einzelne Regel erlaubt wird. Um das Verbot des Starts wichtiger Programme zu vermeiden, müssen Sie entsprechende Erlaubnisregeln für solche Programme erstellen.

Wenn der Start eines Programms durch mehrere Regeln verschiedener Typen kontrolliert wird, erhalten Verbotsregeln Priorität: Der Start eines Programms wird verboten, wenn es auch nur unter eine Verbotsregel fällt.

► *Um Regeln für die Kontrolle des Programmstarts zu testen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Kontrolle des Programmstarts (siehe Abschnitt "Regelliste für die Kontrolle des Programmstarts öffnen" auf Seite 319).
2. Klicken Sie im nächsten Fenster auf Regeln für die Datei anzeigen.

   Das Microsoft-Windows-Standardfenster wird geöffnet.
3. Wählen Sie die Datei aus, für die Sie die Kontrolle des Starts testen möchten.

In der Suchzeile wird der Pfad zur angegebenen Datei angezeigt. Die Liste enthält alle Regeln, die ausgelöst werden, wenn die ausgewählte Datei gestartet wird.

Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" erstellen

► *Um die Einstellungen der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu erstellen und zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Einstellungen** im Assistenten für neue Aufgabe (siehe Abschnitt "Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen" auf Seite 319).
2. Passen Sie Folgendes an:
   - Geben Sie ein Präfix für Regelnamen an.

     Dies ist der erste Teil eines Regelnamens. Der zweite Teil des Regelnamens wird aus dem Namen des Objekts gebildet, dessen Start erlaubt wird.

     Das Standardpräfix ist der Name des Computers, auf dem Kaspersky Embedded Systems Security installiert ist. Sie können das Präfix für die Namen von Erlaubnisregeln ändern.
   - Gültigkeitsbereich der Erlaubnisregeln konfigurieren (siehe Abschnitt "Gültigkeitsbereich der Aufgabe einschränken" auf Seite 358).
3. Klicken Sie auf **Weiter**.
4. Geben Sie die Aktionen an, die Kaspersky Embedded Systems Security ausführen soll:
   - Bei der Erstellung von Erlaubnisregeln (siehe Abschnitt "Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln" auf Seite 358).
   - Nach Abschluss der Aufgabe (siehe Abschnitt "Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln" auf Seite 360).
5. Legen Sie im Fenster Zeitplan die Einstellungen für den Zeitplan für den Aufgabenstart fest.
6. Klicken Sie auf **Weiter**.
7. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, das Sie verwenden möchten.
8. Klicken Sie auf **Weiter**.

9. Geben Sie einen Aufgabennamen an.
10. Klicken Sie auf **Weiter**.

    Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

    Daraufhin wird das Fenster **Erstellung der Aufgabe abschließen** geöffnet.
11. Sie können die Aufgabe optional ausführen, nachdem der Assistent abgeschlossen wurde, indem Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** aktivieren.
12. Klicken Sie auf Fertig stellen, um die Erstellung der Aufgabe fertig zu stellen.

► *Um eine bestehende Regel in Kaspersky Security Center zu konfigurieren, gehen Sie wie folgt vor:*

Öffnen Sie das Fenster **Eigenschaften: Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** und passen Sie die oben beschriebenen Einstellungen 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.

In diesem Abschnitt

Gültigkeitsbereich der Aufgabe einschränken

► *Um den Gültigkeitsbereich der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu beschränken, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** (siehe Abschnitt "Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen" auf Seite 319).
2. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Erlaubnisregeln auf Grundlage gestarteter Programme erstellen.

     Dieses Kontrollkästchen aktiviert oder deaktiviert das Generieren von Regeln für die Kontrolle des Programmstarts für Programme, die bereits ausgeführt werden. Diese Option wird empfohlen, wenn auf dem Computer ein Referenzpaket an Programmen gestartet ist, anhand dessen Sie die Erlaubnisregeln erstellen möchten.

     Ist das Kontrollkästchen aktiviert, werden die Erlaubnisregeln zur Kontrolle des Programmstarts auf der Grundlage von gestarteten Programmen erstellt.

     Ist das Kontrollkästchen deaktiviert, so werden gestartete Programme bei der Erstellung der Erlaubnisregeln nicht berücksichtigt.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Das Kontrollkästchen kann nicht deaktiviert werden, wenn in der Tabelle Erlaubnisregeln für Programme aus folgenden Ordnern erstellen kein Ordner ausgewählt ist.

- Erlaubnisregeln für Programme aus folgenden Ordnern erstellen.

  Sie können die Tabelle verwenden, um Ordner für die Aufgab und die Arten der ausführbaren Dateien auswählen, die bei der Erstellung der Regeln für die Kontrolle des Programmstarts berücksichtigt werden sollen, auszuwählen oder anzugeben. Die Aufgabe erstellt dann Erlaubnisregeln für Dateien der ausgewählten Typen, die sich in den angegebenen Ordnern befinden.

3. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln

► *Um die Aktionen anzupassen, die Kaspersky Embedded Systems Security ausführen soll, während Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" ausgeführt wird, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** (siehe Abschnitt "**Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen**" auf Seite 319).
2. Öffnen Sie die Registerkarte Optionen.
3. Konfigurieren Sie im Abschnitt Bei der Erstellung von Erlaubnisregeln die folgenden Parameter:
   - 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. Anschließend erlaubt das Programm den Start von Programmen mithilfe von 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.

Diese Variante gilt als Standard.

- Header und Fingerabdruck des digitalen Zertifikats verwenden

  Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers und des Fingerabdrucks des digitalen Zertifikats der Datei als ein Auslösekriterium für die Erlaubnisregeln für die Kontrolle des Programmstarts. Die Aktivierung dieses Kontrollkästchens ermöglicht die Festlegung strengerer Bedingungen für die Untersuchung digitaler Zertifikate.

  Ist das Kontrollkästchen aktiviert, werden die Werte des Headers und des Fingerabdrucks des digitalen Zertifikats der Dateien, für welche die Regeln erstellt werden, als ein Kriterium für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts festgelegt. Kaspersky Embedded Systems Security erlaubt Programme, die mithilfe von Dateien mit dem angegebenen Fingerabdruck digitalem Zertifikat gestartet werden.

  Die Verwendung dieses Kontrollkästchens stellt eine starke Einschränkung für das Auslösen von Erlaubnisregeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles fälschungssicheres Identifikationsmerkmal eines digitalen Zertifikats handelt.

Ist das Kontrollkästchen deaktiviert, so wird als ein Kriterium für das Auslösen der Erlaubnisregeln zur Kontrolle des Programmstarts das Vorliegen eines beliebigen digitalen Zertifikats festgelegt, das im Betriebssystem als vertrauenswürdig eingestuft ist.

Das Kontrollkästchen ist aktiv, wenn die Option Digitales Zertifikat verwenden ausgewählt ist.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Falls kein Zertifikat vorhanden, Folgendes verwenden

  Es handelt sich um eine Dropdown-Liste, welche die Auswahl der Kriterien für das Auslösen einer Erlaubnisregel für die Kontrolle des Programmstarts für den Fall erlaubt, dass die Datei, auf deren Grundlage die Regel erstellt wird, über kein digitales Zertifikat verfügt.

  - SHA256-Hash. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.
  - Dateipfad. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm keinen Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle Erlaubnisregeln für Programme aus folgenden Ordnern erstellen im Abschnitt Einstellungen angegeben wurden.

- 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. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.

Diese Option wird für Fälle empfohlen, in denen die generierten Regeln die höchste Sicherheitsstufe erreichen müssen: als eindeutige Datei-ID kann eine SHA256-Prüfsumme verwendet werden. Die Verwendung einer SHA256-Prüfsumme als Auslösekriterium für die Regel beschränkt den Gültigkeitsbereich der Regel auf eine Datei.

Diese Option ist standardmäßig deaktiviert.

- Regeln für Benutzer oder Benutzergruppe erstellen

  Es handelt sich um ein Feld, in dem der Benutzer oder die Benutzergruppe angegeben sind. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer oder die angegebene Benutzergruppe.

  Standardmäßig ist die Gruppe **Alle** eingestellt.

1. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln

► *Gehen Sie wie folgt vor, um festzulegen, wie sich Kaspersky Embedded Systems Security nach Abschluss der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" verhalten soll:*

1. Öffnen Sie das Fenster **Eigenschaften: Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** (siehe Abschnitt "Assistent und Eigenschaften für die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen" auf Seite 319).
2. Öffnen Sie die Registerkarte Optionen.
3. Konfigurieren Sie im Abschnitt Nach Abschluss der Aufgabe die folgenden Einstellungen:
   - Erlaubnisregeln in die Liste der Regeln für die Kontrolle des Programmstarts aufnehmen

     Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen neu erstellter Erlaubnisregeln zur Liste der Regeln für die Kontrolle des Programmstarts. Die Liste der Regeln für die Kontrolle des Programmstarts wird angezeigt, wenn Sie im Detailbereich des Knotens "Kontrolle des Programmstarts" auf den Link Regeln für die Kontrolle des Programmstarts klicken.

     Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die bei der Ausführung der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" erstellten Regeln gemäß dem ausgewählten Prinzip zum Hinzufügen von Regeln zur Liste der Regeln für die Kontrolle des Programmstarts hinzu.

     Ist das Kontrollkästchen nicht aktiviert, so fügt Kaspersky Embedded Systems Security die erstellten Erlaubnisregeln nicht zur Liste der Regeln für die Kontrolle des Programmstarts hinzu. Die erstellten Regeln werden lediglich in eine Datei exportiert.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Prinzip für das Hinzufügen.

     Diese Dropdown-Liste wird verwendet, um die Methode für das Hinzufügen der neu erstellten Erlaubnisregeln zur Liste der Regeln für die Kontrolle des Programmstarts festzulegen.

     - Zu den bestehenden Regeln hinzufügen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden dupliziert.
     - Bestehende Regeln ersetzen. Die Regeln werden anstatt der bestehenden Regeln hinzugefügt.
     - Mit bestehenden Regeln zusammenführen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

     Standardmäßig ist die Option Mit bestehenden Regeln zusammenführen aktiviert.

   - Erlaubnisregeln in Datei exportieren

- Computerinformationen zum Dateinamen hinzufügen

  Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen von Informationen über den geschützten Computer zum Namen der Datei, in welche die Erlaubnisregeln exportiert werden.

  Ist das Kontrollkästchen aktiviert, so fügt das Programm zum Namen der Exportdatei den Namen des geschützten Computers sowie das Datum und die Uhrzeit der Dateierstellung hinzu.

  Ist das Kontrollkästchen deaktiviert, fügt das Programm keine Informationen über den geschützten Computer zum Namen der Exportdatei hinzu.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Kontrolle des Programmstarts über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem lokalen Computer konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen

► *Um die allgemeinen Einstellungen der Aufgabe zur Kontrolle des Programmstarts über*

die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten Kontrolle des Programmstarts aus.
3. Klicken Sie im Detailbereich des untergeordneten Knotens Kontrolle des Programmstarts auf den Link Eigenschaften.

   Das Fenster Aufgabeneinstellungen wird geöffnet.

Fenster "Regel für die Kontrolle des Programmstarts" öffnen

► *Um die Regelliste für die Kontrolle des Programmstarts über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten Kontrolle des Programmstarts aus.
3. Klicken Sie im Ergebnisfenster des Knotens Kontrolle des Programmstarts auf den Link Regeln für die Kontrolle des Programmstarts.

   Das Fenster Regeln für die Kontrolle des Programmstarts wird geöffnet.
4. Konfigurieren Sie die Regelliste nach Bedarf.

Einstellungen der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen

► *Um die Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten Automatisches Erstellen von Regeln.
2. Wählen Sie den untergeordneten Knoten **Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts**.
3. Klicken Sie im Detailbereich des untergeordneten Knotens **Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts** auf den Link Eigenschaften.

   Das Fenster Aufgabeneinstellungen wird geöffnet.
4. Konfigurieren Sie die Aufgabe nach Bedarf.

Aufgabeneinstellungen für Kontrolle des Programmstarts konfigurieren

► *Um die allgemeinen Aufgabeneinstellungen für die Kontrolle des Programmstarts zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen" auf Seite 343).
2. Konfigurieren Sie folgende Aufgabeneinstellungen:

- Auf der Registerkarte Allgemein:
  - Modus der Aufgabe zur Kontrolle des Programmstarts (siehe Abschnitt "Modus der Aufgabe zur Kontrolle des Programmstarts auswählen" auf Seite 345).
  - Gültigkeitsbereich der Regeln in der Aufgabe (siehe Abschnitt "Gültigkeitsbereich für die Aufgabe zur Kontrolle des Programmstarts festlegen" auf Seite 347).
  - Verwendung von KSN (siehe Abschnitt "Verwendung von KSN konfigurieren" auf Seite 348).
- Einstellungen der Kontrolle für Installationspakete (siehe Abschnitt "Kontrolle für Installationspakete" auf Seite 349) auf der Registerkarte Kontrolle für Installationspakete.
- Einstellungen für den Zeitplan für den Aufgabenstart (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160) auf den Registerkarten ZeitplanErweitertund Erweitert.

3. Klicken Sie im Fenster Aufgabeneinstellungen auf **OK**.

   Die Änderung der Einstellungen wird gespeichert.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

In diesem Abschnitt

Modus der Aufgabe zur Kontrolle des Programmstarts auswählen

► *Gehen Sie wie folgt vor, um den Modus der Aufgabe zur Kontrolle des Programmstarts zu konfigurieren:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "**Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen**" auf Seite 343).
2. Geben Sie auf der Registerkarte Allgemein in der Dropdown-Liste Aufgabenmodus den Modus der Aufgabe an.

   In dieser Dropdown-Liste können Sie einen Ausführungsmodus für die Aufgabe zur Kontrolle des Programmstarts auswählen:

   - Aktiv. Kaspersky Embedded Systems Security verwendet die festgelegten Regeln, um alle Programme zu kontrollieren, die gestartet werden.
   - Nur Statistik. Kaspersky Embedded Systems Security verwendet die festgelegten Regeln nicht, um den Start von Programmen zu kontrollieren. Stattdessen werden Informationen über diese Starts im Protokoll der Aufgabenausführung aufgezeichnet. 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 Aufgabenausführung enthaltenen Informationen über die Blockierung verwenden.

   Standardmäßig wird die Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik gestartet.

3. Deaktivieren oder aktivieren Sie das Kontrollkästchen Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten.

   Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle wiederholter Programmstarts auf Basis von Einträgen des Caches für Ereignisinformationen.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security nachfolgende Starts eines Programms auf der Grundlage der Einstufung der Aufgabe in Bezug auf den ersten Start des Programms. 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.

   Ist das Kontrollkästchen deaktiviert, so analysiert Kaspersky Embedded Systems Security ein Programm bei jedem versuchten Programmstart von neuem.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

> Kaspersky Embedded Systems Security legt bei jeder Änderung der Einstellungen der Aufgabe zur Kontrolle des Programmstarts eine neue Liste mit Ereignissen im Cache an. Das bedeutet, dass die Kontrolle des Programmstarts gemäß den aktuellen Sicherheitseinstellungen ausgeführt wird.

4. Deaktivieren oder aktivieren Sie Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten.

   Wenn das Kontrollkästchen aktiviert ist, verbietet Kaspersky Embedded Systems Security den Start des Kommandozeileninterpreters auch dann, wenn der Start von Interpretern erlaubt ist. Ein Kommandozeileninterpreter kann ohne Befehl nur dann gestartet werden, wenn beide der folgenden Bedingungen erfüllt sind:

   - Der Start des Kommandozeileninterpreters ist erlaubt.
   - Der auszuführende Befehl ist erlaubt.

   Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security nur Erlaubnisregeln, wenn ein Kommandozeileninterpreter gestartet wird. Der Start wird verboten, wenn keine Erlaubnisregel übernommen wurde oder der ausführbare Prozess laut KSN nicht vertrauenswürdig ist. Wenn eine Erlaubnisregel übernommen wird oder der Prozess laut KSN vertrauenswürdig ist, kann ein Kommandozeileninterpreter mit oder ohne auszuführenden Befehl gestartet werden.

   Kaspersky Embedded Systems Security erkennt
   die folgenden Kommandozeileninterpreter:

   - cmd.exe
   - powershell.exe
   - python.exe
   - perl.exe

   Das Kontrollkästchen ist standardmäßig deaktiviert.

5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

> Alle Versuche, Programme zu starten, werden im Protokoll der Aufgabenausführung festgehalten.

Modus der Aufgabe zur Kontrolle des Programmstarts konfigurieren

► *Gehen Sie wie folgt vor, um den Modus der Aufgabe zur Kontrolle des Programmstarts zu definieren:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "**Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen**" auf Seite 343).
2. Geben Sie auf der Registerkarte Allgemein im Abschnitt Gültigkeitsbereich der Regeln die folgenden Einstellungen an:
   - Regeln für ausführbare Dateien verwenden

     Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von ausführbaren Dateien.

     Ist dieses Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security den Start ausführbarer Dateien mithilfe vorgegebener Regeln, in deren Einstellungen Ausführbare Dateien als Geltungsbereich angegeben ist.

     Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Starts ausführbarer Dateien mithilfe vorgegebener Regeln. Der Start ausführbarer Dateien ist erlaubt.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
   - Laden von DLL-Modulen überwachen

     Dieses Kontrollkästchen aktiviert oder deaktiviert die Überwachung des Ladens von DLL-Modulen.

     Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security das Laden von DLL-Modulen mithilfe vorgegebener Regeln, in deren Einstellungen Ausführbare Dateien als Geltungsbereich angegeben sind.

     Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Ladens von DLL-Modulen mithilfe vorgegebener Regeln. Laden von DLL-Modulen ist erlaubt.

     Das Kontrollkästchen ist aktiv, wenn das Kontrollkästchen Regeln für ausführbare Dateien verwenden aktiviert ist.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

     Das Überwachen des Ladens von DLL-Modulen kann sich auf die Leistung des Betriebssystems auswirken.
   - Regeln für Skripte und MSI-Pakete verwenden

     Dieses Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von Skripten und MSI-Paketen.

     Wenn dieses Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security den Start von Skripten und MSI-Paketen mithilfe vorgegebener Regeln, in deren Einstellungen Skripte und MSI-Pakete als Geltungsbereich angegeben sind.

     Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Starts von Skripten und MSI-Paketen mithilfe vorgegebener Regeln. Das Ausführen von Skripten und MSI-Paketen ist gestattet.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
3. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Verwendung von KSN konfigurieren

► *Gehen Sie wie folgt vor, um die Verwendung der KSN-Dienste für die Aufgabe zur Kontrolle des Programmstarts einzurichten:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "**Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen**" auf Seite 343).
2. Geben Sie auf der Registerkarte Allgemein im Abschnitt Verwendung von KSN die Einstellungen für die Verwendung von KSN-Diensten an.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten.

     Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß der Programmreputation in KSN.

     Ist das Kontrollkästchen aktiviert, blockiert Kaspersky Embedded Systems Security den Start aller Programme, die laut KSN nicht vertrauenswürdig sind. Erlaubnisregeln zur Kontrolle des Programmstarts, die für Programme gelten, die laut KSN nicht vertrauenswürdig sind, werden nicht ausgelöst. Die Aktivierung des Kontrollkästchens gewährleistet zusätzlichen Schutz vor Schadsoftware.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security die Reputation von Programmen, die laut KSN nicht vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die für diese Programme gelten.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben.

     Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß der Programmreputation in KSN.

     Ist das Kontrollkästchen aktiviert, erlaubt Kaspersky Embedded Systems Security den Start von Programmen, wenn sie laut KSN vertrauenswürdig sind. Dabei haben die Verbotsregeln für die Kontrolle des Programmstarts, die für die im KSN vertrauenswürdigen Programme gelten, eine höhere Priorität: wenn ein Programm laut den KSN-Diensten vertrauenswürdig ist, wird der Programmstart verboten.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security die Reputation von Programmen, die laut KSN vertrauenswürdig sind, nicht und erlaubt oder verbietet den Start in Übereinstimmung mit den Regeln, die für solche Programme gelten.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Wenn das Kontrollkästchen Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben aktiviert ist, geben Sie die Benutzer und/oder Benutzergruppen an, denen der Start von laut KSN vertrauenswürdigen Programmen erlaubt ist. Gehen Sie hierzu wie folgt vor:

     a. Klicken Sie auf die Schaltfläche Ändern.

        Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** wird geöffnet.

     b. Geben Sie die Liste der Benutzer und/oder Benutzergruppen an.

     c. Klicken Sie auf **OK**.
3. Klicken Sie im Fenster Aufgabeneinstellungen auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Kontrolle für Installationspakete

► *Um ein vertrauenswürdiges Installationspaket hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "**Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen**" auf Seite 343).
2. Aktivieren Sie auf der Registerkarte Kontrolle für Installationspakete das Kontrollkästchen Verteilung der unten gelisteten Programme und Installationspakete automatisch erlauben.

   Dieses Kontrollkästchen aktiviert/deaktiviert die Möglichkeit, automatisch Ausnahmen für alle Dateien zu erstellen, die mithilfe der in der Liste angegebenen Programme und Installationspakete gestartet werden.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt das Programm automatisch den Start von Dateien, die von vertrauenswürdigen Installationspaketen gestartet wurden. Die Liste der für den Start freigegebenen Programme und Installationspakete kann bearbeitet werden.

   Wenn das Kontrollkästchen deaktiviert ist, verwendet das Programm die in der Liste angegebenen Ausnahmen nicht.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

   Sie können das Kontrollkästchen Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben aktivieren, wenn das Kontrollkästchen Regeln für ausführbare Dateien verwenden auf der Registerkarte Allgemein in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts aktiviert ist.

3. Deaktivieren Sie bei Bedarf das Kontrollkästchen Verteilung von Programmen mithilfe von Windows Installer immer erlauben.

   Dieses Kontrollkästchen aktiviert/deaktiviert die Möglichkeit, Ausnahmen für alle Dateien, die mithilfe von Windows Installer gestartet werden, automatisch zu erstellen.

   Wenn das Kontrollkästchen aktiviert ist, ist der Start von Dateien, die mithilfe von Windows Installer installiert wurden, immer erlaubt.

   Ist das Kontrollkästchen deaktiviert, dürfen Dateien nicht bedingungslos gestartet werden, selbst wenn Sie über Windows Installer gestartet werden.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Dieses Kontrollkästchen kann nicht bearbeitet werden, wenn das Kontrollkästchen Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben nicht aktiviert ist.

   Das Kontrollkästchen Verteilung von Programmen mithilfe von Windows Installer immer erlauben sollte nur deaktiviert werden, wenn dies absolut notwendig ist. 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.

4. Aktivieren Sie bei Bedarf das Kontrollkästchen Verteilung von Programmen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben.

   Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Erlauben der Verteilung von Software mithilfe der Softwarelösung System Center

Configuration Manager.

Wenn das Kontrollkästchen aktiviert ist, erlaubt Kaspersky Embedded Systems Security automatisch die Verteilung von Microsoft Windows mithilfe von System Center Configuration Manager. Das Programm erlaubt die Verteilung von Software nur mithilfe des intelligenten Hintergrundübertragungsdienstes (Background Intelligent Transfer Service).

Das System überwacht den Start von Objekten mit folgenden Erweiterungen:

- .exe
- .msi

Das Kontrollkästchen ist standardmäßig deaktiviert.

Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an den Computer bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation des Systems auf dem Computer ausgeführt wurde.

5. Um die Liste der vertrauenswürdigen Installationspakete zu bearbeiten, klicken Sie auf die Schaltfläche Liste der Pakete bearbeiten und wählen Sie im nächsten Fenster eine der verfügbaren Methoden aus:

   - Ein Installationspaket hinzufügen.

     a. Klicken Sie auf die Schaltfläche Durchsuchen und wählen Sie die ausführbare Datei oder das Installationspaket aus.

        Im Abschnitt Kriterien für Vertrauenswürdigkeit werden die Daten zur ausgewählten Datei automatisch angezeigt.

     b. Aktivieren oder deaktivieren Sie das Kontrollkästchen Den Start von Dateien in allen Ebenen dieses Installationspakets erlauben.

     c. Wählen Sie eine der beiden verfügbaren Varianten der Kriterien für die Vertrauenswürdigkeit aus, auf deren Grundlage die Datei oder das Installationspaket als vertrauenswürdig gelten:

        - Digitales Zertifikat verwenden
        - SHA256-Hash verwenden.

   - Mehrere Pakete anhand von Hash hinzufügen.

     Sie können eine unbegrenzte Anzahl an ausführbaren Dateien und Installationspaketen auswählen und gleichzeitig zur Liste hinzufügen. Kaspersky Embedded Systems Security untersucht den Hash und erlaubt dem Betriebssystem den Start der angegebenen Dateien.

   - Ausgewähltes Paket bearbeiten.

     Verwenden Sie diese Variante, um eine andere ausführbare Datei oder ein anderes Installationspaket auszuwählen sowie die Kriterien für die Vertrauenswürdigkeit zu ändern.

- Liste mit Paketen aus Datei importieren.

  Sie können die Liste der vertrauenswürdigen Installationspakete aus einer Konfigurationsdatei importieren. Damit eine solche Datei von Kaspersky Embedded Systems Security erkannt wird, muss sie folgende Voraussetzungen erfüllen:

  - Die Dateierweiterung lautet TXT.
  - Die Datei muss Informationen in Form einer Liste mit Zeilen enthalten, von denen jede die Daten einer einzigen vertrauenswürdigen Datei enthält.
  - Die Datei muss eine Liste enthalten, die einem von zwei Formaten entspricht:
    - <Dateiname>:<SHA256-Hash>.
    - <SHA256-Hash>*<Dateiname>.

  Geben Sie im Fenster **Öffnen** die Konfigurationsdatei mit der Liste der vertrauenswürdigen Installationspakete an.

6. Wenn Sie ein früher hinzugefügtes Programm oder Installationspaket aus der Liste der vertrauenswürdigen Installationspakete löschen möchten, klicken Sie auf die Schaltfläche Installationspakete löschen. Der Start extrahierter Dateien wird erlaubt.

   Um den Start extrahierter Dateien zu verbieten, deinstallieren Sie das Programm vollständig vom geschützten Computer oder erstellen Sie eine Verbotsregel in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts.

7. Klicken Sie auf **OK**.

Ihre neu konfigurierten Einstellungen werden gespeichert.

Regeln für die Kontrolle des Programmstarts konfigurieren

Erfahren Sie, wie Sie eine Liste von Regeln erzeugen, importieren und exportieren oder mithilfe der Aufgabe zur Kontrolle des Programmstarts manuell Erlaubnis- oder Verbotsregeln erstellen können.

In diesem Abschnitt

Regel für die Kontrolle des Programmstarts hinzufügen

► *Um eine Regel für die Kontrolle des Programmstarts hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regel für die Kontrolle des Programmstarts.
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt Eine Regel hinzufügen aus.

   Es öffnet sich das Fenster Einstellungen der Regel.
4. Geben Sie die folgenden Einstellungen an:
   a. Geben Sie im Feld Name den Namen der Regel an.
   b. Wählen Sie in der Dropdown-Liste Typ den Typ der Regel:
      - Erlaubnis, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien erlaubt.
      - Verbot, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien verbietet.
   c. Wählen Sie in der Dropdown-Liste Gültigkeitsbereich 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.
   d. Geben Sie im Feld Benutzer und/oder Benutzergruppe die Benutzer an, denen der Programmstart in Übereinstimmung mit dem Regeltyp erlaubt oder verboten werden soll. Gehen Sie hierzu wie folgt vor:
      i. Klicken Sie auf die Schaltfläche Durchsuchen.
      ii. Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** wird geöffnet.
      iii. Geben Sie die Liste der Benutzer und/oder Benutzergruppen an.
      iv. Klicken Sie auf **OK**.
   e. Gehen Sie wie folgt vor, wenn Sie die Werte für die im Abschnitt Auslösekriterien für Regeln genannten Auslösekriterien der Regel aus einer Datei entnehmen möchten:
      i. Klicken Sie auf die Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben.

         Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.
      ii. Wählen Sie die Datei aus.
      iii. Klicken Sie auf **Öffnen**.

         Die Werte der Kriterien in der Dateien werden in den Feldern im Abschnitt Auslösekriterien für Regeln angezeigt. Standardmäßig wird das erste Kriterium der Liste ausgewählt, dessen Daten in den Dateieigenschaften enthalten sind.

f. Wählen Sie im Abschnitt Auslösekriterien für Regeln eine der folgenden Optionen aus:

- Digitales Zertifikat, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, welche mit einem digitalen Zertifikat signiert sind:
  - Aktivieren Sie das Kontrollkästchen Header verwenden, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit dem angegebenen Header signiert sind.
  - Aktivieren Sie das Kontrollkästchen Fingerabdruck verwenden, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.
- SHA256-Hash, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, deren Prüfsumme dem angegebenen Wert entspricht.
- Dateipfad, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, die sich unter dem angegebenen Dateipfad befinden.

  Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie den Backslash ("\"), um den Pfad korrekt einzutragen.

g. Gehen Sie wie folgt vor, wenn Sie Ausnahmen von den Regeln hinzufügen möchten:

i. Klicken Sie im Abschnitt Ausnahmen von der Regel auf **Hinzufügen**.

Es öffnet sich das Fenster Ausnahme von der Regel.

ii. Geben Sie im Feld Name den Namen der Ausnahme ein.

iii. Geben Sie die Einstellungen für die Ausnahme von Programmdateien von den Regeln für die Kontrolle des Programmstarts an. Sie können die Felder mit den Parametern aus den Dateieigenschaften über die Schaltfläche Ausnahme auf Grundlage der Dateieigenschaften festlegen ausfüllen.

- Digitales Zertifikat

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. Anschließend erlaubt das Programm den Start von Programmen mithilfe von 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.

Diese Variante gilt als Standard.

- Header verwenden

  Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers digitaler Zertifikate als Auslösekriterium für die Regel.

  Ist das Kontrollkästchen aktiviert, wird der angegebene Header des digitalen Zertifikats als Auslösekriterium für die Regel verwendet. Die erstellte Regel kontrolliert den Start von Programmen dann lediglich für den im Header genannten Hersteller.

  Ist das Kontrollkästchen deaktiviert, verwendet das Programm den Header des digitalen Zertifikats nicht als Auslösekriterium für die Regel. Ist das Kriterium Digitales Zertifikat ausgewählt, kontrolliert die erstellte Regel Starts von Programmen, die mit einem digitalen Zertifikat mit beliebigem Header signiert sind.

Den Header des digitalen Zertifikats, mit dem die Datei signiert ist, können Sie nur aus den Eigenschaften der ausgewählten Datei mithilfe der Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben oberhalb des Abschnitts Auslösekriterien für Regeln auswählen.

Das Kontrollkästchen ist standardmäßig deaktiviert.

- Fingerabdruck verwenden

  Das Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Fingerabdrucks digitaler Zertifikate als Auslösekriterium für die Regel.

  Ist das Kontrollkästchen aktiviert, wird der angegebene Fingerabdruck des digitalen Zertifikats als Auslösekriterium für die Regel verwendet. Die erstellte Regel kontrolliert dann den Start von Programmen, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.

  Ist das Kontrollkästchen deaktiviert, verwendet das Programm den Fingerabdruck des digitalen Zertifikats nicht als Auslösekriterium für die Regel. Ist das Kriterium Digitales Zertifikat ausgewählt, kontrolliert das Programm Starts von Programmen, die mit einem digitalen Zertifikat mit beliebigem Fingerabdruck signiert sind.

  Den Fingerabdruck des digitalen Zertifikats, mit dem die Datei signiert ist, können Sie nur aus den Eigenschaften der ausgewählten Datei mithilfe der Schaltfläche Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben oberhalb des Abschnitts Auslösekriterien für Regeln auswählen.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

- SHA256-Hash

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. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.

Diese Option wird für Fälle empfohlen, in denen die generierten Regeln die höchste Sicherheitsstufe erreichen müssen: als eindeutige Datei-ID kann eine SHA256-Prüfsumme verwendet werden. Die Verwendung einer SHA256-Prüfsumme als Auslösekriterium für die Regel beschränkt den Gültigkeitsbereich der Regel auf eine Datei.

Diese Option ist standardmäßig deaktiviert.

- Dateipfad

  Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den vollständigen Ordnerpfad, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

  Wenn diese Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

i. Klicken Sie auf OK.

ii. Wiederholen Sie die Schritte (i)-(iv), wenn Sie zusätzliche Ausnahmen hinzufügen möchten.

1. Klicken Sie im Fenster Einstellungen der Regel auf OK.

Die erstellte Regel wird in der Liste im Fenster Regeln für die Kontrolle des Programmstarts angezeigt.

Standarderlaubnismodus aktivieren

Der Standarderlaubnismodus erlaubt den Start aller Programme, sofern diese nicht durch Regeln, oder durch eine KSN-Einstufung als "nicht vertrauenswürdig", blockiert sind. Der Standarderlaubnismodus kann durch Hinzufügen bestimmter Erlaubnisregeln aktiviert werden. Sie können den Standarderlaubnismodus nur für Skripte oder für alle ausführbaren Dateien aktivieren.

► *Um eine Standarderlaubnisregel hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regel für die Kontrolle des Programmstarts.
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt Eine Regel hinzufügen aus.

   Es öffnet sich das Fenster Einstellungen der Regel.
4. Geben Sie im Feld Name den Namen der Regel an.
5. Wählen Sie in der Dropdown-Liste Typ den Regel-Typ Erlaubnis aus.
6. Wählen Sie in der Dropdown-Liste Gültigkeitsbereich den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:
   - Ausführbare Dateien, wenn Sie möchten, dass die Regel den Start ausführbarer Programmdateien kontrolliert.
   - Skripte und MSI-Pakete, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.
7. Wählen Sie im Abschnitt Auslösekriterien für Regeln die Option Dateipfad aus.
8. Geben Sie die folgende Maske ein: `?:\`
9. Klicken Sie im Fenster Einstellungen der Regel auf OK.

Kaspersky Embedded Systems Security übernimmt den Standarderlaubnismodus.

Erlaubnisregeln aus Ereignissen der Aufgabe zur Kontrolle des Programmstarts erstellen

► *Um eine Konfigurationsdatei mit Erlaubnisregeln zu erstellen, die aus Aufgabenereignissen der Kontrolle des Programmstarts erzeugt wurden, gehen Sie wie folgt vor:*

1. Führen Sie die Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik aus (s. Abschnitt "Modus der Aufgabe zur Kontrolle des Programmstarts auswählen" auf S. 345), um Informationen über alle verarbeiteten Programmstarts auf einem geschützten Computer im Protokoll der Aufgabenausführung aufzuzeichnen.
2. Nach Abschluss der Aufgabe im Modus Nur Statistik öffnen Sie das Protokoll der Aufgabenausführung über die Schaltfläche Protokoll der Aufgabenausführung öffnen im Abschnitt Verwaltung im Detailbereich des Knotens Kontrolle des Programmstarts.
3. Klicken Sie im Fenster Protokolle auf die Schaltfläche Regeln anhand von Ereignissen erstellen.

Kaspersky Embedded Systems Security erstellt eine Konfigurationsdatei im xml-Format mit einer Liste der Regeln, die anhand der Ereignisse der Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik erstellt wurden. In der Aufgabe zur Kontrolle des Programmstarts können Sie diese Regelliste übernehmen (siehe Abschnitt "Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren" auf Seite 356)

Bevor Sie die aus den protokollierten Aufgabenereignissen erzeugte Regelliste übernehmen, wird empfohlen, die Liste zu überprüfen und manuell zu verarbeiten, um sicher zu gehen, dass der Start von kritischen Dateien (beispielsweise Systemdateien) durch die angegebene Regel erlaubt wird.

Unabhängig vom Aufgabenmodus werden alle Aufgabenereignisse im Protokoll der Aufgabenausführung aufgezeichnet. Sie können eine Konfigurationsdatei mit der Regelliste anhand des Protokolls erstellen, das erstellt wurde, während die Aufgabe im Modus Aktiv ausgeführt wurde. Dieses Szenario wird mit Ausnahme von wichtigen Fällen nicht empfohlen, da eine endgültige Regelliste erzeugt werden muss, bevor die Aufgabe im Modus Aktiv ausgeführt wird, damit sie effektiv wird.

Regeln für die Kontrolle des Programmstarts exportieren

► *Um Regeln für die Kontrolle des Programmstarts in eine Konfigurationsdatei zu exportieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regel für die Kontrolle des Programmstarts.
2. Klicken Sie auf In Datei exportieren.

   Das Microsoft-Windows-Standardfenster wird geöffnet.
3. Geben Sie im erscheinenden Fenster die Datei an, in die Sie die Regeln exportieren möchten. Existiert die angegebene Datei nicht, so wird sie erstellt. Existiert bereits eine Datei mit dem angegebenen Namen, so wird ihr Inhalt nach überschrieben, wenn die Regeln exportiert werden.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Regeleinstellungen werden in die angegebene Datei exportiert.

Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren

► *Um Regeln für die Kontrolle des Programmstarts zu importieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regel für die Kontrolle des Programmstarts.
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt Regeln aus XML-Datei importieren aus.
4. Geben Sie an, auf welche Weise die zu importierenden Regeln hinzugefügt werden sollen. Wählen Sie hierzu einen der Punkte des Kontextmenüs der Schaltfläche Regeln aus XML-Datei importieren aus:
   - 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.
   - Mit bestehenden 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.

   Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.
5. Wählen Sie im Microsoft-Windows-Fenster **Öffnen** die XML-Datei aus, welche die Regeln für die Kontrolle des Programmstarts enthält.
6. Klicken Sie auf **Öffnen**.

Die importierten Regeln werden in der Liste im Fenster Regeln für die Kontrolle des Programmstarts angezeigt.

Regeln für die Kontrolle des Programmstarts löschen

► *Um Regeln für die Kontrolle des Programmstarts zu entfernen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regel für die Kontrolle des Programmstarts.
2. Wählen Sie in der Liste der Regeln eine oder mehrere Regeln aus, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche Auswahl entfernen.
4. Klicken Sie auf die Schaltfläche Speichern.

Die ausgewählten Regeln für die Kontrolle des Programmstarts werden gelöscht.

Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren

► *Um die Einstellungen der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (s. Abschnitt "Einstellungen der Aufgabe "**Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen**" auf S. 344) der Aufgabe Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts.
2. Passen Sie die folgenden Einstellungen an:
   - Auf der Registerkarte **Allgemein**:
     - Geben Sie ein Präfix für Regelnamen an.

       Dies ist der erste Teil eines Regelnamens. Der zweite Teil des Regelnamens wird aus dem Namen des Objekts gebildet, dessen Start erlaubt wird.

       Das Standardpräfix ist der Name des Computers, auf dem Kaspersky Embedded Systems Security installiert ist. Sie können das Präfix für die Namen von Erlaubnisregeln ändern.
     - Gültigkeitsbereich der Erlaubnisregeln konfigurieren (siehe Abschnitt "Gültigkeitsbereich der Aufgabe einschränken" auf Seite 358).
   - Geben Sie auf der Registerkarte **Aktion** die Aktionen an, die Kaspersky Embedded Systems Security ausführen soll:
     - Bei der Erstellung von Erlaubnisregeln (siehe Abschnitt "Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln" auf Seite 358).
     - Nach Abschluss der Aufgabe (siehe Abschnitt "Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln" auf Seite 360).
   - Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** die Einstellungen des Zeitplans für den Aufgabenstart an (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160).
   - Passen Sie auf der Registerkarte **Mit folgenden Rechten starten** die Einstellungen für den Aufgabenstart mit Benutzerrechten an (siehe Abschnitt "Festlegen eines Benutzerkontos für den Aufgabenstart" auf Seite 163).
3. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung.

In diesem Abschnitt

Gültigkeitsbereich der Aufgabe einschränken

► *Um den Gültigkeitsbereich der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" zu beschränken, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (s. Abschnitt "Einstellungen der Aufgabe "**Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen**" auf S. 344) der Aufgabe Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts.
2. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Erlaubnisregeln auf Grundlage gestarteter Programme erstellen.

     Dieses Kontrollkästchen aktiviert oder deaktiviert das Generieren von Regeln für die Kontrolle des Programmstarts für Programme, die bereits ausgeführt werden. Diese Option wird empfohlen, wenn auf dem Computer ein Referenzpaket an Programmen gestartet ist, anhand dessen Sie die Erlaubnisregeln erstellen möchten.

     Ist das Kontrollkästchen aktiviert, werden die Erlaubnisregeln zur Kontrolle des Programmstarts auf der Grundlage von gestarteten Programmen erstellt.

     Ist das Kontrollkästchen deaktiviert, so werden gestartete Programme bei der Erstellung der Erlaubnisregeln nicht berücksichtigt.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     Das Kontrollkästchen kann nicht deaktiviert werden, wenn in der Tabelle Erlaubnisregeln für Programme aus folgenden Ordnern erstellen kein Ordner ausgewählt ist.

   - Erlaubnisregeln für Programme aus folgenden Ordnern erstellen.

     Sie können die Tabelle verwenden, um Ordner für die Aufgab und die Arten der ausführbaren Dateien auswählen, die bei der Erstellung der Regeln für die Kontrolle des Programmstarts berücksichtigt werden sollen, auszuwählen oder anzugeben. Die Aufgabe erstellt dann Erlaubnisregeln für Dateien der ausgewählten Typen, die sich in den angegebenen Ordnern befinden.
3. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln

► *Um die Aktionen anzupassen, die Kaspersky Embedded Systems Security ausführen soll, während Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" ausgeführt wird, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (s. Abschnitt "Einstellungen der Aufgabe "**Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen**" auf S. 344) der Aufgabe Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts.
2. Öffnen Sie die Registerkarte Aktionen.
3. Konfigurieren Sie im Abschnitt Bei der Erstellung von Erlaubnisregeln die folgenden Parameter:
   - 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. Anschließend erlaubt das Programm den Start von Programmen mithilfe von 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.

Diese Variante gilt als Standard.

- Header und Fingerabdruck des digitalen Zertifikats verwenden

  Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers und des Fingerabdrucks des digitalen Zertifikats der Datei als ein Auslösekriterium für die Erlaubnisregeln für die Kontrolle des Programmstarts. Die Aktivierung dieses Kontrollkästchens ermöglicht die Festlegung strengerer Bedingungen für die Untersuchung digitaler Zertifikate.

  Ist das Kontrollkästchen aktiviert, werden die Werte des Headers und des Fingerabdrucks des digitalen Zertifikats der Dateien, für welche die Regeln erstellt werden, als ein Kriterium für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts festgelegt. Kaspersky Embedded Systems Security erlaubt Programme, die mithilfe von Dateien mit dem angegebenen Fingerabdruck digitalem Zertifikat gestartet werden.

  Die Verwendung dieses Kontrollkästchens stellt eine starke Einschränkung für das Auslösen von Erlaubnisregeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles fälschungssicheres Identifikationsmerkmal eines digitalen Zertifikats handelt.

  Ist das Kontrollkästchen deaktiviert, so wird als ein Kriterium für das Auslösen der Erlaubnisregeln zur Kontrolle des Programmstarts das Vorliegen eines beliebigen digitalen Zertifikats festgelegt, das im Betriebssystem als vertrauenswürdig eingestuft ist.

  Das Kontrollkästchen ist aktiv, wenn die Option Digitales Zertifikat verwenden ausgewählt ist.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Falls kein Zertifikat vorhanden, Folgendes verwenden

  Es handelt sich um eine Dropdown-Liste, welche die Auswahl der Kriterien für das Auslösen einer Erlaubnisregel für die Kontrolle des Programmstarts für den Fall erlaubt, dass die Datei, auf deren Grundlage die Regel erstellt wird, über kein digitales Zertifikat verfügt.

- SHA256-Hash. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.
- Dateipfad. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm keinen Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle Erlaubnisregeln für Programme aus folgenden Ordnern erstellen im Abschnitt Einstellungen angegeben wurden.

- 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. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.

Diese Option wird für Fälle empfohlen, in denen die generierten Regeln die höchste Sicherheitsstufe erreichen müssen: als eindeutige Datei-ID kann eine SHA256-Prüfsumme verwendet werden. Die Verwendung einer SHA256-Prüfsumme als Auslösekriterium für die Regel beschränkt den Gültigkeitsbereich der Regel auf eine Datei.

Diese Option ist standardmäßig deaktiviert.

- Regeln für Benutzer oder Benutzergruppe erstellen

  Es handelt sich um ein Feld, in dem der Benutzer oder die Benutzergruppe angegeben sind. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer oder die angegebene Benutzergruppe.

  Standardmäßig ist die Gruppe **Alle** eingestellt.

1. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln

► *Gehen Sie wie folgt vor, um festzulegen, wie sich Kaspersky Embedded Systems Security nach Abschluss der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" verhalten soll:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (s. Abschnitt "**Einstellungen der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen**" auf S. 344) der Aufgabe Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts.
2. Öffnen Sie die Registerkarte Aktionen.
3. Konfigurieren Sie im Abschnitt Nach Abschluss der Aufgabe die folgenden Einstellungen:
   - Erlaubnisregeln in die Liste der Regeln für die Kontrolle des Programmstarts aufnehmen

     Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen neu erstellter Erlaubnisregeln zur Liste der Regeln für die Kontrolle des Programmstarts. Die Liste der Regeln für die Kontrolle des Programmstarts wird angezeigt, wenn Sie im Detailbereich des Knotens "Kontrolle des Programmstarts" auf den Link Regeln für die Kontrolle des Programmstarts klicken.

Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die bei der Ausführung der Aufgabe "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts" erstellten Regeln gemäß dem ausgewählten Prinzip zum Hinzufügen von Regeln zur Liste der Regeln für die Kontrolle des Programmstarts hinzu.

Ist das Kontrollkästchen nicht aktiviert, so fügt Kaspersky Embedded Systems Security die erstellten Erlaubnisregeln nicht zur Liste der Regeln für die Kontrolle des Programmstarts hinzu. Die erstellten Regeln werden lediglich in eine Datei exportiert.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Prinzip für das Hinzufügen.

  Diese Dropdown-Liste wird verwendet, um die Methode für das Hinzufügen der neu erstellten Erlaubnisregeln zur Liste der Regeln für die Kontrolle des Programmstarts festzulegen.

  - Zu den bestehenden Regeln hinzufügen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden dupliziert.
  - Bestehende Regeln ersetzen. Die Regeln werden anstatt der bestehenden Regeln hinzugefügt.
  - Mit bestehenden Regeln zusammenführen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

  Standardmäßig ist die Option Mit bestehenden Regeln zusammenführen aktiviert.

- Erlaubnisregeln in Datei exportieren
- Computerinformationen zum Dateinamen hinzufügen

  Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen von Informationen über den geschützten Computer zum Namen der Datei, in welche die Erlaubnisregeln exportiert werden.

  Ist das Kontrollkästchen aktiviert, so fügt das Programm zum Namen der Exportdatei den Namen des geschützten Computers sowie das Datum und die Uhrzeit der Dateierstellung hinzu.

  Ist das Kontrollkästchen deaktiviert, fügt das Programm keine Informationen über den geschützten Computer zum Namen der Exportdatei hinzu.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Gerätekontrolle

Dieser Abschnitt informiert über die Aufgabe Gerätekontrolle und enthält Anweisungen für die Einrichtung ihrer Einstellungen.

In diesem Kapitel

Über die Aufgabe Gerätekontrolle

Kaspersky Embedded Systems Security kontrolliert die Registrierung und die Verwendung von Massenspeichergeräten und CD-/DVD-Geräten, um den Computer vor Gefahren zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können. Ein Massenspeichergerät ist ein externes Gerät, das zum Zweck des Kopieren und Speicherns von Daten mit einem Computer verbunden werden kann.

Kaspersky Embedded Systems Security kontrolliert die folgenden Verbindungen zu externen USB-Geräten:

- USB-Flash-Laufwerke
- CD-/DVD-ROM-Laufwerke
- USB-Diskettenlaufwerke
- über USB angeschlossene mobile MTP-Geräte

Kaspersky Embedded Systems Security informiert Sie mithilfe eines entsprechenden Ereignisses in den Aufgabenprotokollen und Ereignisprotokollen über alle Geräte, die über USB angeschlossen werden. Das Ereignis enthält den Gerätetyp und den Verbindungspfad. Wenn die Aufgabe zur Gerätekontrolle gestartet wurde, prüft Kaspersky Embedded Systems Security alle USB-Geräte und listet sie auf. Sie können die Benachrichtigungen im Abschnitt "Benachrichtigungen anpassen" in Kaspersky Security Center anpassen.

Die Aufgabe zur Gerätekontrolle überwacht die Verbindungsversuche der externen Geräte mit dem geschützten Computer über USB und blockiert die Verbindung, wenn für diese Geräte keine Erlaubnisregeln gefunden werden. Wenn die Verbindung blockiert wird, ist das Gerät nicht verfügbar.

Das Programm weist jedem angeschlossenen Massenspeicher einen der folgenden Status zu:

- *Vertrauenswürdig*. Gerät, mit dem der Datenaustausch erlaubt ist. Der *Geräteinstanzpfad* eines solchen Geräts fällt unter den Anwendungsbereich zumindest einer Erlaubnisregel.
- *Nicht vertrauenswürdig*. Gerät, mit dem der Datenaustausch verboten ist. Der Geräteinstanzpfad eines solchen Geräts fällt nicht unter den Anwendungsbereich von Erlaubnisregeln.

Sie können mithilfe der Aufgabe Erstellen von Regeln für die Gerätekontrolle Erlaubnisregeln für externe Geräte erstellen, mit denen Sie einen Datenaustausch erlauben wollen. Sie können den Gültigkeitsbereich von bereits erstellten Erlaubnisregeln auch erweitern. Sie können keine Erlaubnisregeln manuell erstellen.

Kaspersky Embedded Systems Security identifiziert im System registrierte Massenspeicher anhand des Wertes des Geräteinstanzpfads. Der Geräteinstanzpfad ist ein eindeutiges Merkmal für jedes externe Gerät. Die Informationen zum Geräteinstanzpfad sind in den Eigenschaften des externen Geräts im Windows-System enthalten und werden von Kaspersky Embedded Systems Security während der Erstellung von Regeln automatisch bestimmt.

Die Aufgabe Gerätekontrolle kann in einem der folgenden beiden Modi ausgeführt werden:

- Aktiv. Kaspersky Embedded Systems Security kontrolliert mithilfe der Regeln den Anschluss von Flash-Laufwerken und anderen externen Geräten und verbietet oder erlaubt die Verwendung aller Geräte gemäß dem Prinzip des standardmäßigen Verbots (Default Deny) und den festgelegten Erlaubnisregeln. Die Verwendung von vertrauenswürdigen externen Geräten wird erlaubt. Die Verwendung von nicht vertrauenswürdigen externen Geräten wird standardmäßig verboten.

  Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, vor dem Start der Aufgabe zur Gerätekontrolle im Modus Aktiv an den geschützten Computer angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder den Computer neu zu starten. Anderenfalls wird das Prinzip "Standardmäßig verboten" für das Gerät nicht übernommen.

- Nur Statistik. Kaspersky Embedded Systems Security kontrolliert das Anschließen von Flash-Laufwerken und anderen externen Geräten nicht, sondern speichert lediglich die Informationen zu Anschluss und Registrierung von externen Geräten auf dem geschützten Computer sowie zu den Erlaubnisregeln zur Gerätekontrolle, denen die angeschlossenen Geräte unterliegen, im Protokoll der Aufgabenausführung. Die Verwendung aller externen Geräte wird erlaubt. Dieser Modus ist standardmäßig eingestellt.

  Sie können diesen Modus für die Erstellung von Regeln aufgrund von Informationen über Blockierung, die während der Aufgabenausführung aufgezeichnet wurden, verwenden (siehe Abschnitt "Liste der Regeln nach den Ereignissen der Aufgabe Gerätekontrolle erstellen" auf Seite 384).

Über die Regeln für die Gerätekontrolle

Die Regeln werden für jedes Gerät, das in diesen Moment oder zuvor an den geschützten Computer angeschlossen wurde, individuell erstellt, wenn über dieses Gerät Daten im System gespeichert wurden.

Für das Erstellen von Erlaubnisregeln zur Gerätekontrolle können Sie folgenden Aktionen ausführen:

- Die Aufgabe zum Erstellen von Erlaubnisregeln übernehmen (siehe Abschnitt "Über die Aufgabe Erstellen von Regeln für die Gerätekontrolle" auf Seite 367)
- Den Modus "Nur Statistik" in der Aufgabe zur Gerätekontrolle verwenden (siehe Abschnitt "Liste der Regeln nach den Ereignissen der Aufgabe zur Gerätekontrolle ergänzen" auf Seite 384)

- Die Systemdaten über angeschlossene Geräte übernehmen (siehe Abschnitt "Erlaubnisregel für ein oder mehrere externe Geräte hinzufügen" auf Seite 385)
- Den Gültigkeitsbereich von bereits erstellen Regeln erweitern (siehe Abschnitt "Gültigkeitsbereich der Regeln zur Gerätekontrolle erweitern" auf Seite 387).

Die maximale Anzahl der Regeln zur Gerätekontrolle, die Kaspersky Embedded Systems Security unterstützt, beträgt 3072.

Die Regeln für die Gerätekontrolle werden nachfolgend beschrieben.

Regeltyp

Typ der Regel – immer *Erlaubnis*. Die Aufgabe zur Gerätekontrolle sperrt die Verbindung aller Flash-Laufwerke und anderer externer Geräte standardmäßig, wenn sie nicht in den Gültigkeitsbereich von mindestens einer Erlaubnisregel fallen.

Auslösekriterium und Gültigkeitsbereich der Regel

Die Regeln für die Gerätekontrolle identifizieren die angeschlossenen Flash-Laufwerke und andere externe Geräte anhand des Wertes des *Pfads der Geräteexemplarklasse*. Der Geräteinstanzpfad ist ein eindeutiger Identifikator, der dem Gerät vom System zum Zeitpunkt seines Anschlusses und seiner Registrierung als Massenspeicher (Mass Storage) oder CD-/DVD-Laufwerk (z. B. IDE oder SCSI) zugewiesen wird.

Kaspersky Embedded Systems Security kontrolliert den Anschluss externer CD-/DVD-Laufwerke unabhängig von der Schnittstelle des Anschlusses. Beim Montieren solcher Geräte über USB registriert das Betriebssystem zwei Werte für den Geräteinstanzpfad: für den Massenspeicher (Mass Storage), sowie für das CD/DVD-Gerät (beispielsweise IDE oder SCSI). Für einen korrekten Anschluss solcher Geräte sind Erlaubnisregeln für jeden Wert des Geräteinstanzpfades erforderlich.

Kaspersky Embedded Systems Security bestimmt den Geräteinstanzpfad und schlüsselt den gefundenen Wert auf die folgenden Elemente auf:

- Hersteller (VID) des Geräts
- Controller-Typ (PID) des Geräts
- Seriennummer des Geräts

Sie können den Geräteinstanzpfad nicht manuell festlegen. Die in den Eigenschaften der Erlaubnisregel festgelegten Auslösekriterien für die Regel bestimmen den Gültigkeitsbereich dieser Regel. Standardmäßig beinhaltet der Gültigkeitsbereich einer gerade erstellten Erlaubnisregel ein Gerät, auf der Grundlage von dessen Eigenschaften Kaspersky Embedded Systems Security die Erlaubnisregel erstellt hat. Sie können die angegebenen Werte mithilfe der Maske in den Eigenschaften der erstellten Regel bearbeiten, um den Gültigkeitsbereich der Regel auszudehnen (siehe Abschnitt "Gültigkeitsbereich der Regeln zur Gerätekontrolle erweitern" auf Seite 387).

Daten des Ausgangsgeräts

Die Daten des Geräts, aufgrund von dessen Eigenschaften Kaspersky Embedded Systems Security die Erlaubnisregel gebildet hat, werden in den Eigenschaften der einzelnen Regeln angezeigt.

Die Daten des Ausgangsgeräts enthalten die folgenden Informationen:

- Pfad der Geräteexemplarklasse. Aufgrund dieses Wertes bestimmt Kaspersky Embedded Systems Security die Auslösekriterien für die Regel und füllt die Felder Hersteller (VID), Controller-Typ (PID), Seriennummer im Abschnitt Gültigkeitsbereich der Regel im Fenster Einstellungen der Regel aus.
- Anzeigename. Name, der vom Hersteller in den Eigenschaften des Geräts angegeben ist.

Kaspersky Embedded Systems Security bestimmt die Daten des Ausgangsgeräts zum Zeitpunkt des Erstellens der Regel automatisch. Im Folgenden können Sie diese Werte verwenden, um zu bestimmen, aufgrund der Daten welchen Geräts die Regel erstellt wurde. Die Daten des Ausgangsgeräts können nicht bearbeitet werden.

Beschreibung

Sie können die Zusatzinformationen für jede erstellte Regel für die Gerätekontrolle im Feld Kommentar hinzufügen, beispielsweise, den Namen des angeschlossenen Flash-Laufwerkes oder den Namen seines Inhabers. Der Kommentar wird in der entsprechenden Tabellenspalte im Fenster Regeln für die Gerätekontrolle angezeigt.

Der Kommentar und die Daten des Ausgangsgeräts werden bei der Ausführung der Regel nicht berücksichtigt und dienen nur zur Vereinfachung der Kennzeichnung der Geräte und Regeln für den Benutzer.

Über die Erstellung der Liste mit Regeln für die Gerätekontrolle

Sie können Listen von Erlaubnisregeln zur Gerätekontrolle aus einer XML-Datei importieren, die im Zuge Ausführung der Aufgabe zur Gerätekontrolle oder der Aufgabe Erstellen von Regeln für die Gerätekontrolle automatisch erstellt wird.

Standardmäßig schränkt Kaspersky Embedded Systems Security den Anschluss aller Flash-Laufwerke und anderer externer Geräte ein, die nicht in den Geltungsbereich der festgelegten Regeln für die Gerätekontrolle fallen.

Tabelle 49. Ziele und Szenarien zur Erstellung von Listen mit Regeln zur Gerätekontrolle

Szenarium zur Erstellung der Regelliste	Lösungsaufgabe
Aufgabe Erstellen von Regeln für die Gerätekontrolle	• Erlaubnisregeln für bereits verwendete vertrauenswürdige Geräte müssen vor dem ersten Start der Aufgabe zur Gerätekontrolle erstellt werden. • Die Regelliste für die vertrauenswürdigen Geräte muss im Netzwerk der geschützten Computer erstellt werden.
Erstellen von Regeln aufgrund der Systemdaten	Die Erlaubnisregeln für ein oder mehrere neue angeschlossene Geräte müssen hinzugefügt werden.
Modus Nur Statistik der Aufgabe zur Gerätekontrolle	Erlaubnisregeln für eine große Anzahl von vertrauenswürdigen Geräten müssen erstellt werden.

Verwendung der Aufgabe Erstellen von Regeln für die Gerätekontrolle

Die xml-Datei, die nach Abschluss der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle erstellt wird,

enthält die Erlaubnisregeln für Flash-Laufwerke und andere externe Geräte, über deren Anschluss Daten im System gespeichert wurden.

Bei der Aufgabenausführung empfängt Kaspersky Embedded Systems Security die Systeminformationen zu allen Massenspeichergeräten, die zuvor oder zu diesem Zeitpunkt an den geschützten Computer angeschlossen sind, und erstellt aufgrund dieser Daten eine Liste mit Erlaubnisregeln für die gefundenen Geräte. Nach den Abschluss der Aufgabe erstellt das Programm eine XML-Datei im Ordner nach dem Pfad, der in den Einstellungen der Aufgabe angegeben ist. Sie können den automatischen Import erstellter Regeln in die Liste der Regeln für die Aufgabe Gerätekontrolle konfigurieren.

Es wird empfohlen, dieses Szenario zur Erstellung der Liste mit Erlaubnisregeln vor dem ersten Aufgabenstart die Gerätekontrolle zu verwenden, damit die erstellten Erlaubnisregeln alle externen Geräte berücksichtigen, die auf dem geschützten Computer verwendet werden.

Verwendung der Systemdaten über alle angeschlossenen Geräte

Im Verlauf der Aufgabenausführung erhält Kaspersky Embedded Systems Security Systemdaten über alle externen Geräte, die früher angeschlossen waren und zum gegenwärtigen Zeitpunkt an den geschützten Computer angeschlossen sind, und zeigt die gefundenen Geräte im Fenster Regel auf Grundlage der folgenden Systemdaten erstellen in der Liste der gefundenen Geräte an.

Kaspersky Embedded Systems Security bestimmt für jedes gefundene Gerät den Hersteller (VID), den Controller-Typ (PID), den Anzeigenamen, die Seriennummer und den Geräteinstanzpfad. Sie können die Erlaubnisregeln für einen beliebigen Massenspeicher erstellen, für das Daten gefunden wurden, und die neuen Regeln sofort zur Liste der festgelegten Regeln zur Gerätekontrolle hinzufügen.

Es wird empfohlen, dieses Szenario für das Update der Regelliste zu verwenden, wenn die Verwendung einer kleinen Anzahl von Massenspeichern erlaubt werden soll.

Kaspersky Embedded Systems Security erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Es können keine Erlaubnisregeln für MTP-Mobilgeräte erstellt werden.

Verwendung der Aufgabe zur Gerätekontrolle im Modus "Nur Statistik"

xml-Datei, die nach Abschluss der Aufgabe zur Gerätekontrolle im Modus Nur Statistik auf der Grundlage des Protokolls der Ausgabenausführung erstellt wurde.

Während der Aufgabenausführung protokolliert Kaspersky Embedded Systems Security alle Verbindungen von Flash-Laufwerken und anderen Massenspeichern zum geschützten Computer im Protokoll der Aufgabenausführung. Sie können Erlaubnisregeln anhand von Ereignissen der Aufgabe erstellen und sie in eine XML-Datei exportieren. Vor dem Aufgabenstart im Modus Nur Statistik wird empfohlen, den Zeitraum der Aufgabenausführung so anzupassen, dass alle möglichen Verbindungen von externen Geräten mit dem geschützten Computer im angegebenen Zeitraum ausgeführt wurden.

Es wird empfohlen, dieses Szenario für das Update einer bereits erstellten Regelliste zu verwenden, wenn eine große Anzahl an neuen externen Geräten erlaubt werden soll.

Wenn das Erstellen einer Regelliste nach diesem Szenario auf einem Referenzcomputer ausgeführt wird, können Sie die angelegte Liste mit Erlaubnisregeln für die Einstellungen der Aufgabe "Gerätekontrolle" in Kaspersky Security Center verwenden. Auf diese Weise können Sie die Verwendung von externen Geräten, die an den Referenzcomputer angeschlossen sind, auf allen Computern des geschützten Netzwerks erlauben.

Über die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle

Mithilfe der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle können Sie automatisch eine Liste der Erlaubnisregeln für den Anschluss von Flash-Laufwerken und anderen Massenspeichern auf Basis der Systemdaten der Geräte erstellen, die zuvor an den geschützten Computer angeschlossen wurden.

Kaspersky Embedded Systems Security erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Es können keine Erlaubnisregeln für MTP-Mobilgeräte erstellt werden.

Nach Abschluss der Ausführung der Aufgabe erstellt Kaspersky Embedded Systems Security eine Konfigurationsdatei im XML-Format mit der Liste der Erlaubnisregeln für die gefundenen externen Geräte bzw. fügt die erstellten Regeln abhängig von den festgelegten Aufgabeneinstellungen sofort zur Aufgabe zum Erstellen von Regeln für die Gerätekontrolle hinzu. Daraufhin erlaubt das Programm Geräte, für die Erlaubnisregeln automatisch erstellt wurden.

Erzeugte und zur Aufgabe hinzugefügte Regeln werden im Fenster Regeln für die Gerätekontrolle angezeigt.

Szenarien für die Erzeugung von Regeln für die Gerätekontrolle

Sie können auf der Grundlage von Windows-Daten für alle Massenspeicher Regeln erstellen (siehe Abschnitt Erstellen von Regeln für die Gerätekontrolle aller Computer durch Kaspersky Security Center auf Seite 372), die jemals oder derzeit über drei Szenarien verbunden waren:

- Mithilfe der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle". Verwenden Sie diese Methode, wenn Sie möchten, dass beim Erstellen der Erlaubnisregeln die Daten über die jemals angeschlossenen Massenspeicher, die in den Systemen aller Computer im Netzwerk registriert wurden, berücksichtigt werden.
- Mithilfe der Option Regeln auf Grundlage von Systemdaten erstellen. Verwenden Sie diese Methode, wenn Sie möchten, dass beim Erstellen der Erlaubnisregeln die Daten über alle jemals angeschlossenen Massenspeicher, die im System des Computers mit der installierten Verwaltungskonsole von Kaspersky Security Center registriert wurden, berücksichtigt werden.
- Mithilfe der Option Regeln auf Grundlage verbundener Geräte erstellen im Fenster Regeln für die Gerätekontrolle und den Einstellungen der Aufgabe "Erstellen von Regeln für die Gerätekontrolle". Verwenden Sie diese Methode, wenn Sie möchten, dass nur Daten über Geräte berücksichtigt werden, die momentan an den geschützten Computer angeschlossen sind, wenn Sie Erlaubnisregeln erstellen.

Kaspersky Embedded Systems Security erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Sie können Erlaubnisregeln für vertrauenswürdige mobile Geräte, die über das MTP-Protokoll angeschlossen werden nicht mithilfe von Szenarien zur Ergänzung von Regellisten zur Gerätekontrolle erstellen, die auf der Anwendung der Systemdaten über alle Geräte basieren.

Standardeinstellungen der Aufgabe zur Gerätekontrolle

Die Aufgabe zur Gerätekontrolle weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 50. Standardaufgabeneinstellungen für die Gerätekontrolle

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	Nur Statistik	Die Aufgabe speichert das Erlauben und Verbieten des Anschlusses von externen Geräten gemäß den festgelegten Regeln im Protokoll der Aufgabenausführung. Eine tatsächliche Blockierung der Verwendung von externen Geräten findet nicht statt. Sie können zum Schutz des Computers den Modus Aktiv auswählen, damit eine tatsächliche Blockierung der Verwendung von externen Geräten stattfindet.
Verwendung aller Massenspeicher erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird	Wird nicht verwendet	Kaspersky Embedded Systems Security verbietet die Verwendung von externen Geräten unabhängig vom Ausführungsstatus der Aufgabe zur Gerätekontrolle. Dies gewährleistet die maximale Sicherheit des Computers vor Bedrohungen, die beim Dateiaustausch mit externen Geräten entstehen. Sie können die Einstellung so anpassen, dass Kaspersky Embedded Systems Security die Verwendung aller externen Geräte erlaubt, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Gerätekontrolle wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können den Zeitplan für den Aufgabenstart konfigurieren.

Tabelle 51. Standardeinstellungen der Aufgabe Erstellen von Regeln für die Gerätekontrolle

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	Systemdaten über alle jemals angeschlossenen Massenspeicher berücksichtigen	Der Ausführungsmodus der Aufgabe. Sie können den Aufgabenmodus **Nur Systemdaten zu den momentan angeschlossenen Massenspeichern berücksichtigen** auswählen.
Aktionen nach Abschluss der Aufgabe	Die Erlaubnisregeln werden der Liste der Regeln zur Gerätekontrolle hinzugefügt; die neuen Regeln werden mit den bestehenden Regeln zusammengeführt; doppelte Regeln werden gelöscht.	Sie können die Regeln den bereits existierenden Regeln hinzufügen, ohne dabei doppelte Regeln zusammenzuführen oder zu löschen oder bestehende Regeln durch neue Erlaubnisregeln zu ersetzen, sowie die Einstellungen für den Export der Erlaubnisregeln in eine Datei konfigurieren.

Einstellung	Standardwert	Beschreibung
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle wird nicht automatisch beim Hochfahren von Kaspersky Embedded Systems Security ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Gerätekontrolle über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie durch die Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Verbindungen von beliebigen Massenspeichern mit allen Computern im Netzwerk verwalten, indem Sie Regellisten für die Gruppen von Computern über das Kaspersky Security Center erstellen.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Richtlinieneinstellungen für die Aufgabe zur Gerätekontrolle öffnen

► *Um die Aufgabeneinstellungen für die Gerätekontrolle über die Richtlinie von Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt Überwachung der Desktop-Aktivitäten.
6. Klicken Sie auf die Schaltfläche Einstellungen im Unterabschnitt Gerätekontrolle.

   Das Fenster Gerätekontrolle wird geöffnet.
7. Konfigurieren Sie die Richtlinie nach Bedarf.

Regelliste für die Gerätekontrolle öffnen

► *Um die Regelliste für die Gerätekontrolle über das Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt Überwachung der Desktop-Aktivitäten.
6. Klicken Sie auf die Schaltfläche Einstellungen im Unterabschnitt Gerätekontrolle.

   Das Fenster Gerätekontrolle wird geöffnet.
7. Klicken Sie auf der Registerkarte Allgemein auf Regelliste.

   Das Fenster Regeln für die Gerätekontrolle wird geöffnet.
8. Konfigurieren Sie die Richtlinie nach Bedarf.

Assistent und Eigenschaften für die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle öffnen

► *Um die Erstellung einer Aufgabe zum Erstellen von Regeln für die Gerätekontrolle auszulösen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe**geöffnet.
5. Wählen Sie die Aufgabe Erstellen von Regeln für die Gerätekontrolle aus.
6. Klicken Sie auf **Weiter**.

   Das Fenster Einstellungen wird geöffnet.

► *Um die bestehende Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben von Kaspersky Security Center.

   Daraufhin wird das Fenster **Eigenschaften: Erstellen von Regeln für die Gerätekontrolle** geöffnet.

Details darüber, wie Sie die Aufgabe konfigurieren, finden Sie im Abschnitt Aufgabe zum Erstellen von Regeln für die Gerätekontrolle konfigurieren.

Aufgabe zur Gerätekontrolle konfigurieren

► *Um die Einstellungen der Aufgabe zur Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Gerätekontrolle (siehe Abschnitt "Richtlinieneinstellungen für die Aufgabe zur Gerätekontrolle öffnen" auf Seite 369).
2. Passen Sie auf der Registerkarte Allgemein folgende Aufgabenparameter an:
   - Wählen Sie im Abschnitt Aufgabenmodus einen Aufgabenmodus aus:
     - Aktiv.

       Kaspersky Embedded Systems Security kontrolliert mithilfe der Regeln den Anschluss von Flash-Laufwerken und anderen externen Geräten und verbietet oder erlaubt die Verwendung aller Geräte gemäß dem Prinzip "standardmäßig verboten" (Default Deny) und den festgelegten Erlaubnisregeln. Die Verwendung von vertrauenswürdigen externen Geräten wird erlaubt. Die Verwendung von nicht vertrauenswürdigen externen Geräten wird standardmäßig verboten.

Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, vor dem Start der Aufgabe zur Gerätekontrolle im Modus "Aktiv" an den geschützten Server angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder den Computer neu zu starten. Anderenfalls wird das Prinzip "Standardmäßig verboten" für das Gerät nicht übernommen.

- Nur Statistik.

  Kaspersky Embedded Systems Security kontrolliert das Anschließen von Flash-Laufwerken und anderen externen Geräten nicht, sondern speichert lediglich die Informationen zu Anschluss und Registrierung von externen Geräten auf dem geschützten Computer sowie zu den Erlaubnisregeln zur Gerätekontrolle, denen die angeschlossenen Geräte unterliegen, im Protokoll der Aufgabenausführung. Die Verwendung aller externen Geräte wird erlaubt. Dieser Modus ist standardmäßig eingestellt.

- Deaktivieren oder aktivieren Sie das Kontrollkästchen Verwendung aller Massenspeicher erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.

  Das Kontrollkästchen erlaubt oder verbietet die Verwendung von Massenspeichern, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.

  Wenn das Kontrollkästchen aktiviert ist und die Aufgabe zur Gerätekontrolle nicht ausgeführt wird, erlaubt Kaspersky Embedded Systems Security die Verwendung beliebiger Massenspeichergeräte auf dem geschützten Computer.

  Wenn das Kontrollkästchen deaktiviert ist, verbietet das Programm die Verwendung von nicht vertrauenswürdigen Massenspeichern auf dem geschützten Computer in den folgenden Fällen: wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird oder wenn Kaspersky Security Service angehalten ist. Es wird empfohlen, zur Gewährleistung maximaler Sicherheit des Computers vor Bedrohungen, die beim Dateiaustausch mit den externen Geräten entstehen, diese Variante zu verwenden.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

3. Klicken Sie auf die Schaltfläche der Liste Regeln, um die Liste der Regeln für die Gerätekontrolle zu bearbeiten (siehe Abschnitt "Regeln für die Gerätekontrolle über das Kaspersky Security Center konfigurieren" auf Seite 375).
4. Passen Sie bei Bedarf die Einstellungen des Zeitplans für den Aufgabenstart auf der Registerkarte Aufgabenverwaltung an.
5. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Protokoll der Aufgabenausführung gespeichert.

Erstellen von Regeln für die Gerätekontrolle aller Computer durch Kaspersky Security Center

Sie können mithilfe der Aufgaben von Kaspersky Security Center für alle Computer und Computergruppen im Netzwerk des Unternehmens gleichzeitig Listen mit Regeln für die Gerätekontrolle erstellen.

Sie können Listen mit Regeln für die Gerätekontrolle auf der Seite von Kaspersky Security Center auf folgende Arten erstellen:

- Mithilfe der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle".

  Bei Verwendung dieses Szenarios erstellt die Gruppenaufgabe die Regellisten aufgrund der Systemdaten jedes Computers über alle irgendwann angeschlossenen Flash-Laufwerke und anderen Massenspeichergeräten. Die Aufgabe berücksichtigt auch alle Massenspeichergeräte, die während der Ausführung der Gruppenaufgabe angeschlossen wurden. Nach der Ausführung der Gruppenaufgabe erstellt Kaspersky Embedded Systems Security Listen mit Erlaubnisregeln für alle registrierten Massenspeichergeräte des Netzwerks und speichert diese Listen in einer xml-Datei im angegebenen allgemeinen Ordner. Im Weiteren können Sie die erstellten Listen mit Regeln manuell in die Einstellungen der Aufgabe "Gerätekontrolle" importieren. Im Gegensatz zur Aufgabe auf einem lokalen Computer können Sie in der Richtlinie auf Seiten von Kaspersky Security Center kein automatisches Hinzufügen erstellter Regeln in die Liste der Regeln für die Gerätekontrolle nach Abschluss der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" einrichten.

  Es wird empfohlen, diese Option für die Erstellung einer Liste mit Erlaubnisregeln vor dem ersten Start der Aufgabe "Gerätekontrolle" im Modus **Aktiv** der Regelanwendung zu verwenden.

  > Stellen Sie bei der Übernahme der Richtlinie für Gerätekontrolle im Netzwerk sicher, dass für alle geschützten Computer der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Verwendung einer Netzwerkfreigabe im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" für Regeln zur Computer-Kontrolle auf der Test-Computergruppe oder einem Referenzcomputer zu starten.

- Auf Grundlage des in Kaspersky Security Center erstellten Berichts über Ereignisse bei der Ausführung der Aufgabe "Gerätekontrolle" im Modus Nur Statistik.

  Bei Verwendung dieses Szenarios blockiert Kaspersky Embedded Systems Security den Anschluss der Massenspeichergeräte nicht, protokolliert aber alle Verbindungs- und Registrierungsversuche von Massenspeichergeräten auf allen Netzwerkcomputern während der Ausführung der Aufgabe "Gerätekontrolle" im Modus Nur Statistik. Die protokollierten Informationen können auf der Registerkarte **Ereignisse** im Arbeitsbereich des Knotens **Administrationsserver** von Kaspersky Security Center eingesehen werden. Daraufhin erstellt Kaspersky Security Center auf Grundlage des Protokolls der Aufgabenausführung eine einheitliche Liste von Massenspeichern, die Ereignisse beschränken und erlauben.

  Sie müssen den Zeitraum der Aufgabenausführung so anpassen, dass für den angegebenen Zeitraum alle Verbindungen von Massenspeichergeräten ausgeführt werden. Danach können Sie beim Hinzufügen von Regeln zur Aufgabe zur Gerätekontrolle Daten über Geräteverbindungen aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (im Format TXT) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle der betreffenden Geräte erstellen. Die Art der Ereignisse, auf denen ein importiertes Protokoll basiert, hat keinen Einfluss auf den generierten Regeltyp - es werden nur Erlaubnisregeln generiert.

  Es wird empfohlen, dieses Szenario zu verwenden, wenn Erlaubnisregeln für eine große Menge neuer

Massenspeicher erstellt werden sollen, sowie für das Erstellen von Erlaubnisregeln für über das MTP-Protokoll angeschlossene vertrauenswürdige mobile Geräte.

- Auf Grundlage der Daten der System-Registry über die angeschlossenen Massenspeicher (mithilfe der Option Regel auf Grundlage von Systemdaten erstellen in den Einstellungen der Aufgabe "Gerätekontrolle").

  Bei Verwendung dieses Szenarios erstellt Kaspersky Embedded Systems Security Erlaubnisregeln für Massenspeicher, die in diesem Moment oder zuvor an den Computer angeschlossen wurden, auf dem Kaspersky Security Center installiert ist.

  Es wird empfohlen, dieses Szenario zu verwenden, wenn Regeln für eine geringe Anzahl neuer Massenspeichergeräte erstellt werden sollen, deren Verwendung Sie auf allen Computern im Netzwerk erlauben möchten.

- Auf Grundlage der Daten über die Geräte, die momentan angeschlossen sind (mithilfe der Option Regeln basierend auf verbundenen Geräte erstellen)

  Bei Verwendung dieses Szenarios erstellt Kaspersky Embedded Systems Security Erlaubnisregeln nur für Geräte, die momentan angeschlossen sind. Sie können ein oder mehrere Geräte auswählen, für die Sie die Erlaubnisregeln erstellen möchten.

> Kaspersky Embedded Systems Security erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Sie können Erlaubnisregeln für vertrauenswürdige mobile Geräte, die über das MTP-Protokoll angeschlossen werden nicht mithilfe von Szenarien zur Ergänzung von Regellisten zur Gerätekontrolle erstellen, die auf der Anwendung der Systemdaten über alle Geräte basieren.

Aufgabe zum Erstellen von Regeln für die Gerätekontrolle konfigurieren

► *Um die Einstellungen der Aufgabe Erstellen von Regeln für die Gerätekontrolle anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Erstellen von Regeln für die Gerätekontrolle** (siehe Abschnitt "**Assistent und Eigenschaften für die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle öffnen**" auf Seite 370).
2. 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*.

3. Im Abschnitt **Einstellungen** können Sie die folgenden Einstellungen konfigurieren:
   - Betriebsmodus auswählen: Systemdaten über alle jemals angeschlossenen Massenspeicher berücksichtigen oder nur derzeit angeschlossene Massenspeicher berücksichtigen.
   - Passen Sie die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln an, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.
4. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).

5. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
6. 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 Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center*

7. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**.

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Regeln für die Gerätekontrolle über das Kaspersky Security Center konfigurieren

Erfahren Sie, wie Sie auf der Grundlage von verschiedenen Kriterien eine Liste von Regeln erzeugen oder mithilfe der Aufgabe zur Gerätekontrolle manuell Erlaubnis- oder Verbotsregeln erstellen können.

In diesem Abschnitt

Erlaubnisregeln auf Grundlage von Systemdaten des Systems in einer Richtlinie von Kaspersky Security Center erstellen

► *Um die Erlaubnisregeln mithilfe der Option Regel auf Grundlage von Systemdaten erstellen in den Einstellungen der Aufgabe "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Schließen Sie an den Computer mit der installierten Verwaltungskonsole von Kaspersky Security Center erforderlichenfalls einen neuen Massenspeicher an, den Sie vertrauenswürdig machen möchten.
2. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "Regelliste für die Gerätekontrolle öffnen" auf Seite 370).
3. Klicken Sie auf Hinzufügen und wählen Sie im Kontextmenü der Schaltfläche den Punkt Regel auf Grundlage der folgenden Systemdaten erstellen.

4. Wählen Sie das Prinzip aus, nach dem Erlaubnisregeln zur Liste der bereits festgelegten Regeln für die Gerätekontrolle hinzugefügt werden sollen.
   - Wählen Sie ein Gerät in der Liste der Geräte im Fenster Regel auf Grundlage der folgenden Systemdaten erstellen aus.
   - Klicken Sie auf Regel für ausgewählte Geräte hinzufügen.
5. Klicken Sie auf die Schaltfläche Speichern im Fenster Gerätekontrolle**.**

Die Liste der Regeln in der Aufgabe Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des Computers mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Regeln für angeschlossene Geräte erstellen

► *Um die Erlaubnisregeln mithilfe der Option Regeln auf Grundlage verbundener Geräte erstellen in den Einstellungen der Aufgabe "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "**Regelliste für die Gerätekontrolle öffnen**" auf Seite 370).
2. Klicken Sie auf die Schaltfläche Hinzufügen und wählen Sie im Kontextmenü den Punkt Regeln für momentan angeschlossene Geräte berücksichtigen aus.

   Das Fenster Regeln auf Grundlage der Systemdaten erstellen wird geöffnet.
3. Wählen Sie in der Liste der gefundenen Geräte, die an den geschützten Computer angeschlossen sind, die Geräte aus, für die Sie Erlaubnisregeln erstellen möchten.
4. Klicken Sie auf die Schaltfläche Regel für ausgewählte Geräte hinzufügen.
5. Klicken Sie auf die Schaltfläche Speichern im Fenster Gerätekontrolle**.**

Die Liste der Regeln in der Aufgabe Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des Computers mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Regeln aus dem Bericht von Kaspersky Security Center über blockierte Geräte importieren

Sie können Daten über blockierte Geräteverbindungen aus dem Bericht importieren, der in Kaspersky Security Center nach der Ausführung der Aufgabe zur Gerätekontrolle im Modus Nur Statistik erstellt wurde (siehe Abschnitt "Aufgabe zur Gerätekontrolle konfigurieren" auf Seite 371), und diese Daten für die Erstellung einer Liste von Erlaubnisregeln für die Gerätekontrolle in der konfigurierten Richtlinie verwenden.

Bei der Berichterstellung über Ereignisse, die während der Ausführung der Aufgabe zur Gerätekontrolle eintreten, können Sie verfolgen, für welche Programme die Verbindung blockiert wird.

► *Gehen Sie wie folgt vor, um auf Grundlage eines Berichts aus Kaspersky Security Center über blockierten Geräte Erlaubnisregeln für Geräteverbindungen für eine Gruppe von Computern festzulegen:*

1. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisbenachrichtigungen**, dass:
   - Für die Prioritätsstufe Kritische Ereignisse die Zeitspanne zum Speichern des Protokolls der Aufgabenausführung für das Ereignis *Massenspeicher eingeschränkt* die geplante Betriebsdauer im Modus Nur Statistik übersteigt (der Standardwert beträgt 30 Tage).

- Für die Prioritätsstufe **Warnung** die Zeitspanne zum Speichern des Protokolls der Aufgabenausführung für das Ereignis *Nur Statistik: nicht vertrauenswürdiges Gerät gefunden* die geplante Betriebsdauer der Aufgabe im Modus Nur Statistik übersteigt (der Standardwert beträgt 30 Tage).

  Nach Ablauf der Zeitspanne für das Speichern von Ereignissen werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in die Protokolldatei aufgenommen. Vergewissern Sie sich vor dem Start der Aufgabe "Gerätekontrolle" im Modus Nur Statistik, dass die Ausführungsdauer der Aufgabe die eingestellte Speicherzeit für die angegebenen Ereignisse nicht überschreitet.

2. Starten Sie die Aufgabe zur Gerätekontrolle im Modus Nur Statistik. Wählen Sie im Arbeitsbereich des Knotens **Administrationsserver** in Kaspersky Security Center die Registerkarte **Ereignisse** aus. Klicken Sie auf die Schaltfläche **Auswahl erstellen** und erstellen Sie eine Auswahl von Ereignissen auf der Grundlage des Kriteriums *Nicht vertrauenswürdiger Massenspeicher gefunden*, um die Geräte anzuzeigen, deren Verbindungen durch die Aufgabe zur Gerätekontrolle eingeschränkt werden. Klicken Sie im Detailbereich der Auswahl auf den Link **Ereignisse in Datei exportieren**, um den Bericht über eingeschränkte Verbindungen in einer TXT-Datei zu speichern.

   Vergewissern Sie sich vor dem Import und der Verwendung des erstellten Berichts in der Richtlinie, dass der Bericht nur Daten derjenigen Geräte enthält, deren Verbindung Sie erlauben möchten.

3. Importieren Sie die Daten über die Verbindungen eingeschränkter Geräte in die Aufgabe "Gerätekontrolle":

   a. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "Regelliste für die Gerätekontrolle öffnen" auf Seite 370).

   b. Klicken Sie auf Hinzufügen und wählen Sie im Kontextmenü der Schaltfläche den Punkt Regeln aus Datei des Kaspersky Security Center-Berichts über blockierte Geräte importieren.

   c. Wählen Sie das Prinzip aus, nach dem die Regeln aus der auf Grundlage des Berichts von Kaspersky Security Center erstellten Liste zur Liste der bereits bestehenden Regeln zur Gerätekontrolle hinzugefügt werden.

      - 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.
      - Mit bestehenden 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.

   d. Wählen Sie im erscheinenden Windows-Standardfenster die TXT-Datei aus, in welche die Ereignisse aus dem Bericht über die blockierten Geräte exportiert wurden.

   e. Klicken Sie auf die Schaltfläche Speichern im Fenster Gerätekontrolle**.**

4. Klicken Sie im Fenster Gerätekontrolle auf **OK**.

Die auf Grundlage des Berichts von Kaspersky Security Center über die blockierten Geräte erstellten Regeln werden der Liste der Regeln in der Richtlinie zur Gerätekontrolle hinzugefügt.

Regeln mithilfe der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen

► *Um Erlaubnisregeln für die Gerätekontrolle für eine Gruppe von Computern mithilfe der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" festzulegen, gehen Sie wie folgt vor.*

1. Öffnen Sie das Fenster Einstellungen im **Assistenten für neue Aufgabe** (siehe Abschnitt "**Assistent und Eigenschaften für die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle öffnen**" auf Seite 370).
2. Passen Sie Folgendes an:
   - Im Abschnitt Modus:
     - Systemdaten über alle jemals angeschlossenen Massenspeicher berücksichtigen.
     - Nur Systemdaten zu den momentan angeschlossenen Massenspeichern berücksichtigen.
   - Im Abschnitt Nach Abschluss der Aufgabe:
     - Erlaubnisregeln in die Liste der Regeln für die Gerätekontrolle aufnehmen.

       Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen erstellter Erlaubnisregeln zur Liste der Regeln für die Gerätekontrolle. Die Liste der Regeln für die Gerätekontrolle wird angezeigt, wenn Sie im Detailbereich des Knotens "Gerätekontrolle" auf den Link Regeln für die Gerätekontrolle klicken.

       Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die bei der Ausführung der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle erstellten Regeln gemäß dem ausgewählten Prinzip zum Hinzufügen von Regeln zur Liste der Regeln für die Gerätekontrolle hinzu.

       Ist das Kontrollkästchen nicht aktiviert, so fügt Kaspersky Embedded Systems Security die erstellten Erlaubnisregeln nicht zur Liste der Regeln für die Gerätekontrolle hinzu. Die erstellten Regeln werden lediglich in eine Datei exportiert.

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

       Das Kontrollkästchen kann nicht deaktiviert werden, wenn das Kontrollkästchen Erlaubnisregeln in Datei exportieren nicht aktiviert ist.

     - Prinzip für das Hinzufügen.

       Diese Dropdown-Liste wird verwendet, um die Methode für das Hinzufügen der neu erstellten Erlaubnisregeln zur Liste der Regeln für die Kontrolle des Programmstarts festzulegen.

       - Zu den bestehenden Regeln hinzufügen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden dupliziert.
       - Bestehende Regeln ersetzen. Die Regeln werden anstatt der bestehenden Regeln hinzugefügt.
       - Mit bestehenden Regeln zusammenführen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

       Standardmäßig ist die Option Mit bestehenden Regeln zusammenführen aktiviert.

- Erlaubnisregeln in Datei exportieren

  Dieses Kontrollkästchen aktiviert oder deaktiviert den Export von Erlaubnisregeln für die Gerätekontrolle in eine Datei.

  Ist das Kontrollkästchen aktiviert, exportiert Kaspersky Embedded Systems Security die Erlaubnisregeln nach Abschluss der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" in die im darunter angeordneten Feld angegebene Datei.

  Wenn dieses Kontrollkästchen deaktiviert ist, exportiert das Programm die erzeugten Erlaubnisregeln nicht in eine Datei, wenn die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" abgeschlossen ist. Stattdessen werden sie nur zur Liste der Regeln für die Gerätekontrolle hinzugefügt.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

  Das Kontrollkästchen kann nicht deaktiviert werden, wenn das Kontrollkästchen **Erlaubnisregeln in die Liste der Regeln für die Gerätekontrolle aufnehmen** nicht aktiviert ist.

- Computerinformationen zum Dateinamen hinzufügen

  Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen von Informationen über den geschützten Computer zum Namen der Datei, in welche die Erlaubnisregeln exportiert werden.

  Ist das Kontrollkästchen aktiviert, so fügt das Programm zum Namen der Exportdatei den Namen des geschützten Computers sowie das Datum und die Uhrzeit der Dateierstellung hinzu.

  Ist das Kontrollkästchen deaktiviert, fügt das Programm keine Informationen über den geschützten Computer zum Namen der Exportdatei hinzu.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

3. Klicken Sie auf **Weiter**.
4. Legen Sie im Fenster Zeitplan die Einstellungen für den Zeitplan für den Aufgabenstart fest.
5. Klicken Sie auf **Weiter**.
6. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, das Sie verwenden möchten.
7. Klicken Sie auf **Weiter**.
8. Geben Sie einen Aufgabennamen an.
9. Klicken Sie auf **Weiter**.

   Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

   Daraufhin wird das Fenster **Erstellung der Aufgabe abschließen** geöffnet.
10. Sie können die Aufgabe optional ausführen, nachdem der Assistent abgeschlossen wurde, indem Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** aktivieren.
11. Klicken Sie auf Fertig stellen, um die Erstellung der Aufgabe fertig zu stellen.
12. Wählen Sie auf der Registerkarte **Aufgaben** im Arbeitsbereich der konfigurierten Computergruppe in der Liste der Gruppenaufgaben die erstellte Aufgabe zum Erstellen von Regeln für die Gerätekontrolle aus.
13. Klicken Sie auf die Schaltfläche **Starten**, um die Aufgabe zu starten.

Nach Abschluss der Aufgabe werden die automatisch erstellten Listen mit Erlaubnisregeln in Form von XML-Dateien in einem freigegebenen Ordner gespeichert.

Stellen Sie bei der Übernahme der Richtlinie für Gerätekontrolle im Netzwerk sicher, dass für alle geschützten Computer der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Verwendung einer Netzwerkfreigabe im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" für Regeln zur Computer-Kontrolle auf der Test-Computergruppe oder einem Referenzcomputer zu starten.

Erzeugte Regeln in die Regelliste für die Gerätekontrolle aufnehmen

► *Um die erzeugten Listen mit Erlaubnisregeln zur Aufgabe zur Gerätekontrolle hinzuzufügen, gehen Sie wie folgt vor.*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "Regelliste für die Gerätekontrolle öffnen" auf Seite 370).
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü der Schaltfläche "Hinzufügen" die Option Regeln aus XML-Datei importieren aus.
4. Wählen Sie das Prinzip aus, nach dem automatisch erstellte Erlaubnisregeln der Liste der bereits festgelegten Regeln zur Gerätekontrolle 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.
   - Mit bestehenden 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.
5. Wählen Sie im erscheinenden Standardfenster von Windows die XML-Dateien aus, die nach Abschluss der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellt wurden.
6. Klicken Sie auf **Öffnen**.

   Alle erzeugten Regeln aus der XML-Datei werden entsprechend dem ausgewählten Prinzip zur Liste hinzugefügt.
7. Klicken Sie auf die Schaltfläche Speichern im Fenster Gerätekontrolle**.**
8. Wenn Sie die erstellten Regeln für die Gerätekontrolle verwenden möchten, wählen Sie in den Eigenschaften der Richtlinie zur Gerätekontrolle den Aufgabenmodus Aktiv.

Automatisch auf Grundlage der Systemdaten auf jedem einzelnen Computer erstellte Erlaubnisregeln werden für alle Computer im Netzwerk, auf denen die konfigurierte Richtlinie übernommen wird, übernommen. Für diese Computer erlaubt das Programm nur die Verbindung von Geräten, für die Erlaubnisregeln erstellt wurden.

Gerätekontrolle über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem lokalen Computer konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Einstellungen der Aufgabe zur Gerätekontrolle öffnen

► *Um die Einstellungen der Aufgabe zur Gerätekontrolle über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten Gerätekontrolle aus.
3. Klicken Sie im Detailbereich des untergeordneten Knotens Gerätekontrolle auf den Link Eigenschaften.

   Das Fenster Aufgabeneinstellungen wird geöffnet.
4. Konfigurieren Sie die Aufgabe nach Bedarf.

Fenster "Regeln für die Gerätekontrolle" öffnen

► *Um die Regelliste für die Gerätekontrolle über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten Gerätekontrolle aus.

3. Klicken Sie im Detailbereich des Knotens Gerätekontrolle auf den Link Regeln für die Gerätekontrolle.

   Das Fenster Regeln für die Gerätekontrolle wird geöffnet.

4. Konfigurieren Sie die Regelliste nach Bedarf.

Einstellungen für das Erstellen von Regeln für die Gerätekontrolle öffnen

► *Um die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten Automatisches Erstellen von Regeln.
2. Wählen Sie den untergeordneten Knoten Erstellen von Regeln für die Gerätekontrolle.
3. Klicken Sie im Detailbereich des untergeordneten Knotens Erstellen von Regeln für die Gerätekontrolle auf den Link Eigenschaften.

   Das Fenster Aufgabeneinstellungen wird geöffnet.

4. Konfigurieren Sie die Aufgabe nach Bedarf.

Einstellungen der Aufgabe Gerätekontrolle anpassen

► *Um die Einstellungen der Aufgabe zur Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Aufgabeneinstellungen (siehe Abschnitt "Einstellungen der Aufgabe zur Gerätekontrolle öffnen" auf Seite 381).
2. Passen Sie auf der Registerkarte Allgemein folgende Aufgabenparameter an:
   - Wählen Sie im Abschnitt Aufgabenmodus einen Aufgabenmodus aus:
     - Aktiv.

       Kaspersky Embedded Systems Security kontrolliert mithilfe der Regeln den Anschluss von Flash-Laufwerken und anderen externen Geräten und verbietet oder erlaubt die Verwendung aller Geräte gemäß dem Prinzip "standardmäßig verboten" (Default Deny) und den festgelegten Erlaubnisregeln. Die Verwendung von vertrauenswürdigen externen Geräten wird erlaubt. Die Verwendung von nicht vertrauenswürdigen externen Geräten wird standardmäßig verboten.

       Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, vor dem Start der Aufgabe zur Gerätekontrolle im Modus "Aktiv" an den geschützten Server angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder den Computer neu zu starten. Anderenfalls wird das Prinzip "Standardmäßig verboten" für das Gerät nicht übernommen.

     - Nur Statistik.

       Kaspersky Embedded Systems Security kontrolliert das Anschließen von Flash-Laufwerken und anderen externen Geräten nicht, sondern speichert lediglich die Informationen zu Anschluss und Registrierung von externen Geräten auf dem geschützten Computer sowie zu den Erlaubnisregeln zur Gerätekontrolle, denen die angeschlossenen Geräte unterliegen, im Protokoll der Aufgabenausführung. Die Verwendung aller externen Geräte wird erlaubt. Dieser Modus ist standardmäßig eingestellt.

- Deaktivieren oder aktivieren Sie das Kontrollkästchen Verwendung aller Massenspeicher erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.

  Das Kontrollkästchen erlaubt oder verbietet die Verwendung von Massenspeichern, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.

  Wenn das Kontrollkästchen aktiviert ist und die Aufgabe zur Gerätekontrolle nicht ausgeführt wird, erlaubt Kaspersky Embedded Systems Security die Verwendung beliebiger Massenspeichergeräte auf dem geschützten Computer.

  Wenn das Kontrollkästchen deaktiviert ist, verbietet das Programm die Verwendung von nicht vertrauenswürdigen Massenspeichern auf dem geschützten Computer in den folgenden Fällen: wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird oder wenn Kaspersky Security Service angehalten ist. Es wird empfohlen, zur Gewährleistung maximaler Sicherheit des Computers vor Bedrohungen, die beim Dateiaustausch mit den externen Geräten entstehen, diese Variante zu verwenden.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

3. Passen Sie erforderlichenfalls auf den Registerkarten Zeitplan und Erweitert den Zeitplan für den Aufgabenstart an (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160).
4. Um die Regelliste für die Gerätekontrolle zu bearbeiten (siehe Abschnitt "Über die Erstellung der Liste mit Regeln für die Gerätekontrolle" auf Seite 365), klicken Sie auf den Link Regeln für die Gerätekontrolle im unteren Teil des Detailbereichs der Knotens Gerätekontrolle.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Regeln für die Gerätekontrolle konfigurieren

Erfahren Sie, wie Sie eine Liste von Regeln erzeugen, importieren und exportieren oder mithilfe der Aufgabe zur Gerätekontrolle manuell Erlaubnis- oder Verbotsregeln erstellen können.

In diesem Abschnitt

Regeln für die Gerätekontrolle aus einer XML-Datei importieren

► *Um Regeln zur Gerätekontrolle zu importieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "**Fenster "Regeln für die Gerätekontrolle" öffnen**" auf Seite 381).
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt Regeln aus XML-Datei importieren aus.
4. Geben Sie an, auf welche Weise die zu importierenden Regeln hinzugefügt werden sollen. Wählen Sie hierzu einen der Punkte des Kontextmenüs der Schaltfläche Regeln aus XML-Datei importieren aus:
   - 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.
   - Mit bestehenden 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.

   Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.
5. Wählen Sie im Fenster **Öffnen** die XML-Datei aus, in der die Einstellungen der Regeln für die Gerätekontrolle enthalten sind.
6. Klicken Sie auf **Öffnen**.

Die importierten Regeln erscheinen in der Liste im Fenster Regeln für die Gerätekontrolle.

Liste der Regeln nach den Ereignissen der Aufgabe Gerätekontrolle erstellen

► *Um die Konfigurationsdatei mit der Liste der Regeln zur Gerätekontrolle, die anhand von Ereignissen der Aufgabe Gerätekontrolle erstellt wurde, zu erstellen, gehen Sie wie folgt vor:*

1. Führen Sie die Aufgabe zur Gerätekontrolle im Modus Nur Statistik aus (s. Abschnitt "**Einstellungen der Aufgabe Gerätekontrolle anpassen**" auf S. 382), um im Protokoll der Aufgabenausführung alle Ereignisse zu protokollieren, die beim Anschluss von Flash-Laufwerken und anderen externen Geräten an den geschützten Computer auftreten.
2. Nach Abschluss der Aufgabe im Modus Nur Statistik öffnen Sie das Protokol der Aufgabenausführung über die Schaltfläche Protokoll der Aufgabenausführung öffnen im Abschnitt Verwaltung im Ergebnisbereich des Knotens Gerätekontrolle.
3. Klicken Sie im Fenster Protokolle auf die Schaltfläche Regeln anhand von Ereignissen erstellen.

Kaspersky Embedded Systems Security erstellt die Konfigurationsdatei im xml-Format mit der Liste der Regeln, die anhand der Ereignisse der Ausführung der Aufgabe zur Gerätekontrolle im Modus Nur Statistik erstellt wurden. Sie können diese Liste in der Aufgabe zur Gerätekontrolle übernehmen (siehe Abschnitt "Regeln für die Gerätekontrolle aus einer XML-Datei importieren" auf Seite 384).

Vor der Anwendung der Regelliste, die anhand von Ereignissen der Aufgabe erstellt wurde, wird empfohlen, die Liste der Regeln anzuzeigen und manuell zu bearbeiten, um sicherzustellen, dass die Verbindung von nicht vertrauenswürdigen Geräten nicht durch die festgelegten Regeln erlaubt ist.

Beim Konvertieren der XML-Datei mit den Ereignissen der Aufgabenausführung in die Liste der Regeln zur Gerätekontrolle erstellt das Programm Erlaubnisregeln für alle gespeicherten Ereignisse, darunter auch für Ereignisse der Gerätesperre.

In beiden Modi werden alle Ereignisse der Aufgabenausführung im Protokoll der Aufgabenausführung registriert. Sie können eine Konfigurationsdatei mit der Regelliste anhand von Ereignissen der Aufgabe im Modus Aktiv erstellen. Dieses Szenario wird nicht empfohlen, mit Ausnahme von dringlichen Fällen, da für die effektive Ausführung der Aufgabe die Erstellung von Listen bis zum Start der Aufgabe im aktiven Modus erforderlich ist.

Erlaubnisregel für ein oder mehrere externe Geräte hinzufügen

In der Aufgabe zur Gerätekontrolle ist die Funktion des manuellen Hinzufügens einer Regel nicht vorgesehen. Falls Sie jedoch Erlaubnisregeln für einen oder mehrere neue externe Geräte hinzufügen müssen, können Sie die Option **Regel auf Grundlage der folgenden Systemdaten erstellen** verwenden. Bei Verwendung dieses Szenarios zur Ergänzung der Regelliste verwendet das Programm die Windows-Daten über alle angeschlossenen externen Geräte, die jemals im System registriert wurden, und berücksichtigt die externen Geräte, die momentan angeschlossen sind.

Kaspersky Embedded Systems Security erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Es können keine Erlaubnisregeln für MTP-Mobilgeräte erstellt werden.

► *Um eine Erlaubnisregel für ein oder mehrere externe Geräte, die zum aktuellen Zeitpunkt angeschlossen sind, hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle** Regeln für die Gerätekontrolle(siehe Abschnitt "Fenster "Regeln für die Gerätekontrolle" öffnen" auf Seite 381).
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Wählen Sie im Kontextmenü den Punkt Regel auf Grundlage der folgenden Systemdaten erstellen.
4. Wählen Sie im folgenden Fenster in der Liste der gefundenen Geräte ein Gerät oder mehrere Geräte aus, deren Verwendung auf dem geschützten Computer erlaubt werden soll.
5. Klicken Sie auf die Schaltfläche Regel für ausgewählte Geräte hinzufügen.

Die neuen Regeln werden zur Liste der Regeln zur Gerätekontrolle hinzugefügt.

Regeln der Gerätekontrolle löschen

► *Um Regeln für die Gerätekontrolle zu entfernen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "**Fenster "Regeln für die Gerätekontrolle" öffnen**" auf Seite 381).
2. Wählen Sie in der Liste der Regeln eine oder mehrere Regeln aus, die Sie entfernen möchten.
3. Klicken Sie auf die Schaltfläche Auswahl entfernen.
4. Klicken Sie auf die Schaltfläche Speichern.

Die ausgewählten Regeln zur Gerätekontrolle werden gelöscht.

Regeln der Gerätekontrolle exportieren

► *Um Regeln für die Gerätekontrolle in eine Konfigurationsdatei zu exportieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "**Fenster "Regeln für die Gerätekontrolle" öffnen**" auf Seite 381).
2. Klicken Sie auf In Datei exportieren.

   Das Microsoft-Windows-Standardfenster wird geöffnet.
3. Geben Sie im erscheinenden Fenster die Datei an, in die Sie die Regeln exportieren möchten. Existiert die angegebene Datei nicht, so wird sie erstellt. Existiert bereits eine Datei mit dem angegebenen Namen, so wird ihr Inhalt nach Abschluss des Exports der Regeln überschrieben.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Regeln und ihre Einstellungen werden in die angegebene Datei exportiert.

Regeln zur Gerätekontrolle aktivieren und deaktivieren

Sie können die Anwendung der erstellten Erlaubnisregeln zur Gerätekontrolle aktivieren und deaktivieren, ohne sie zu löschen.

► *Um die erstellte Regel für die Gerätekontrolle zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "**Fenster "Regeln für die Gerätekontrolle" öffnen**" auf Seite 381).
2. Öffnen Sie in der Liste der angegebenen Regeln das Fenster Eigenschaften der Regel, indem Sie mit der rechten Maustaste auf die Regel doppelklicken, deren Einstellungen Sie anpassen wollen.

3. Deaktivieren oder aktivieren Sie im folgenden Fenster das Kontrollkästchen Regel übernehmen.

   Das Kontrollkästchen aktiviert oder deaktiviert die Anwendung der Regel für die Gerätekontrolle.

   Wenn das Kontrollkästchen in den Einstellungen der Regel aktiviert ist, ist diese Regel aktiv. Der Anschluss externer Geräte, die in den Gültigkeitsbereich dieser Regel fallen, wird erlaubt.

   Wenn das Kontrollkästchen in den Einstellungen der Regel deaktiviert ist, ist diese Regel inaktiv. Der Anschluss externer Geräte, die in den Gültigkeitsbereich dieser Regel fallen, wird verboten.

   Standardmäßig ist das Kontrollkästchen in den Einstellungen jeder erstellten Regel aktiviert.

4. Klicken Sie auf OK.

Der Status der Anwendung der Regel wird gespeichert und für die angegebene Regel angezeigt.

Gültigkeitsbereich der Regeln zur Gerätekontrolle erweitern

Jede automatisch erstellte Regel für die Gerätekontrolle erlaubt die Verbindung nur eines externen Geräts. Sie können den Gültigkeitsbereich der Regel manuell erweitern, indem Sie die Maske des Pfads der Geräteexemplarklasse in den Eigenschaften einer beliebigen festgelegten Regel für die Gerätekontrolle anwenden.

Die Anwendung der Maske des Pfads der Geräteexemplarklasse verringert die Anzahl der Erlaubnisregeln der Gerätekontrolle und vereinfacht den Prozess ihrer manuellen Verarbeitung. Die Erweiterung des Gültigkeitsbereichs der Regeln kann jedoch die Effektivität der Kontrolle von Massenspeichergeräten verringern.

► *Um eine Maske des Geräteinstanzpfads in den Eigenschaften der Erlaubnisregel für die Gerätekontrolle zu übernehmen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Regeln für die Gerätekontrolle (siehe Abschnitt "**Fenster "Regeln für die Gerätekontrolle" öffnen**" auf Seite 381).
2. Wählen Sie im folgenden Fenster eine Regel aus, deren Eigenschaften Sie für die Maske des Programms verwenden möchten.
3. Öffnen Sie das Fenster Einstellungen der Regel mit einem Doppelklick auf der ausgewählten Regel für die Gerätekontrolle.
4. Im sich öffnenden Fenster gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen Maske verwenden neben dem Feld Controller-Typ (PID), wenn Sie möchten, dass eine ausgewählte Regel die Verbindung aller Massenspeicher nach den festgelegten Daten über den Hersteller und die Seriennummer des Geräts erlaubt.
   - Aktivieren Sie das Kontrollkästchen Maske verwenden neben dem Feld Seriennummer, wenn Sie möchten, dass eine ausgewählte Regel die Verbindung aller Massenspeicher nach den festgelegten Daten über den Hersteller und den Gerätetyp erlaubt.
   - Aktivieren Sie die Kontrollkästchen Maske verwenden neben den Feldern Controller-Typ (PID) und Seriennummer, wenn Sie möchten, dass eine ausgewählte Regel die Verbindung aller Massenspeicher nach den festgelegten Daten über den Hersteller erlaubt.

   Wenn in mindestens einem Feld das Kontrollkästchen Maske verwenden aktiviert ist, werden die Informationen in den Feldern, in denen dieses Kontrollkästchen aktiviert ist, durch das Zeichen * ersetzt und beim Auslösen der Regel nicht berücksichtigt.

5. Geben Sie im Feld Beschreibung bei Bedarf zusätzlich erläuternde Informationen zur Regel an. Geben Sie z. B. an, für welche Geräte die Regel gelten soll.
6. Klicken Sie auf OK.

Die vorgenommenen Regel-Einstellungen werden gespeichert. Der Gültigkeitsbereich der Regel wird entsprechend der angegebenen Maske des Pfads der Geräteexemplarklasse erweitert.

Aufgabe "Erstellen von Regeln für die Gerätekontrolle" konfigurieren

► *Um die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten Automatisches Erstellen von Regeln.
2. Wählen Sie den untergeordneten Knoten Erstellen von Regeln für die Gerätekontrolle.
3. Klicken Sie im Detailbereich des Knotens Erstellen von Regeln für die Gerätekontrolle auf den Link Eigenschaften.

   Das Fenster Aufgabeneinstellungen wird geöffnet.
4. Wählen Sie auf der Registerkarte Allgemein im Abschnitt Aufgabenmodus den Modus der Aufgabenausführung aus:
   - Systemdaten über alle jemals angeschlossenen Massenspeicher berücksichtigen.
   - Nur Systemdaten zu den momentan angeschlossenen Massenspeichern berücksichtigen.
5. Geben Sie im Abschnitt Nach Abschluss der Aufgabe die Aktionen an, die Kaspersky Embedded Systems Security beim Abschluss der Aufgabe ausführen soll:
   - Erlaubnisregeln in die Liste der Regeln für die Gerätekontrolle aufnehmen.

     Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen erstellter Erlaubnisregeln zur Liste der Regeln für die Gerätekontrolle. Die Liste der Regeln für die Gerätekontrolle wird angezeigt, wenn Sie im Detailbereich des Knotens "Gerätekontrolle" auf den Link Regeln für die Gerätekontrolle klicken.

     Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die bei der Ausführung der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle erstellten Regeln gemäß dem ausgewählten Prinzip zum Hinzufügen von Regeln zur Liste der Regeln für die Gerätekontrolle hinzu.

     Ist das Kontrollkästchen nicht aktiviert, so fügt Kaspersky Embedded Systems Security die erstellten Erlaubnisregeln nicht zur Liste der Regeln für die Gerätekontrolle hinzu. Die erstellten Regeln werden lediglich in eine Datei exportiert.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     Das Kontrollkästchen kann nicht deaktiviert werden, wenn das Kontrollkästchen Erlaubnisregeln in Datei exportieren nicht aktiviert ist.

- Prinzip für das Hinzufügen.

  Diese Dropdown-Liste wird verwendet, um die Methode für das Hinzufügen der neu erstellten Erlaubnisregeln zur Liste der Regeln für die Kontrolle des Programmstarts festzulegen.

  - Zu den bestehenden Regeln hinzufügen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden dupliziert.
  - Bestehende Regeln ersetzen. Die Regeln werden anstatt der bestehenden Regeln hinzugefügt.
  - Mit bestehenden Regeln zusammenführen. Die Regeln ergänzen die Liste der bestehenden Regeln. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

  Standardmäßig ist die Option Mit bestehenden Regeln zusammenführen aktiviert.

- Erlaubnisregeln in Datei exportieren

  Dieses Kontrollkästchen aktiviert oder deaktiviert den Export von Erlaubnisregeln für die Gerätekontrolle in eine Datei.

  Ist das Kontrollkästchen aktiviert, exportiert Kaspersky Embedded Systems Security die Erlaubnisregeln nach Abschluss der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" in die im darunter angeordneten Feld angegebene Datei.

  Wenn dieses Kontrollkästchen deaktiviert ist, exportiert das Programm die erzeugten Erlaubnisregeln nicht in eine Datei, wenn die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" abgeschlossen ist. Stattdessen werden sie nur zur Liste der Regeln für die Gerätekontrolle hinzugefügt.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

  Das Kontrollkästchen kann nicht deaktiviert werden, wenn das Kontrollkästchen **Erlaubnisregeln in die Liste der Regeln für die Gerätekontrolle aufnehmen** nicht aktiviert ist.

- Computerinformationen zum Dateinamen hinzufügen

  Dieses Kontrollkästchen aktiviert oder deaktiviert das Hinzufügen von Informationen über den geschützten Computer zum Namen der Datei, in welche die Erlaubnisregeln exportiert werden.

  Ist das Kontrollkästchen aktiviert, so fügt das Programm zum Namen der Exportdatei den Namen des geschützten Computers sowie das Datum und die Uhrzeit der Dateierstellung hinzu.

  Ist das Kontrollkästchen deaktiviert, fügt das Programm keine Informationen über den geschützten Computer zum Namen der Exportdatei hinzu.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Passen Sie auf den Registerkarten Zeitplan und Erweitert die Einstellungen für den Zeitplan für den Aufgabenstart an (siehe Abschnitt "Einstellungen für den Zeitplan für den Aufgabenstart anpassen" auf Seite 160).
7. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Firewall-Verwaltung

Dieser Abschnitt informiert über die Aufgabe zur Firewall-Verwaltung und erläutert die Konfiguration dieser Aufgabe.

In diesem Kapitel

Über die Aufgabe zur Firewall-Verwaltung

Kaspersky Embedded Systems Security stellt eine sichere und ergonomische Lösung für den Schutz von Netzwerkverbindungen mithilfe der Aufgabe zur Firewall-Verwaltung zur Verfügung.

Die Aufgabe zur Firewall-Verwaltung führt keine selbständige Filterung des Datenverkehrs durch, sondern ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Embedded Systems Security zu verwalten. Während der Ausführung der Aufgabe zur Firewall-Verwaltung übernimmt Kaspersky Embedded Systems Security die vollständige Verwaltung der Einstellungen und Regeln der Firewall des Betriebssystems und blockiert jeden Versuch, die Firewall-Einstellungen auf andere Weise anzupassen.

Bei der Programminstallation liest und kopiert die Komponente Firewall-Verwaltung den Status der Windows-Firewall sowie alle festgelegten Regeln. Von diesem Zeitpunkt an kann die Änderung der Regelsätze und Einstellungen sowie das Anhalten oder der Start der Firewall nur über Kaspersky Embedded Systems Security vorgenommen werden.

Wenn die Windows-Firewall bei der Installation von Kaspersky Embedded Systems Security deaktiviert ist, wird die Aufgabe zur Firewall-Verwaltung nach Abschluss der Installation nicht ausgeführt. Wenn die Windows-Firewall bei der Programminstallation aktiviert ist, wird die Aufgabe zur Firewall-Verwaltung nach Abschluss der Installation ausgeführt und blockiert alle Netzwerkverbindungen, die nicht von den festgelegten Regeln erlaubt sind.

Die Komponente Firewall-Verwaltung gehört nicht zu den Komponenten der empfohlenen Installation und wird nicht standardmäßig installiert.

Die Aufgabe zur Firewall-Verwaltung erzwingt das Blockieren aller eingehenden und ausgehenden Verbindungen, wenn sie nicht von den festgelegten Regeln der Aufgabe erlaubt sind.

Die Aufgabe fragt regelmäßig die Windows-Firewall ab und überprüft ihren Zustand. Standardmäßig beträgt das Abfrageintervall 1 Minute und kann nicht geändert werden. Wenn Kaspersky Embedded Systems Security bei der Durchführung der Abfrage feststellt, dass die Einstellungen der Windows-Firewall und der Einstellungen der Aufgabe zur Firewall-Verwaltung nicht übereinstimmen, erzwingt das Programm die Weitergabe der Einstellungen der Aufgabe an die Firewall des Betriebssystems.

Bei der minutengenauen Abfrage der Windows-Firewall prüft Kaspersky Embedded Systems Security Folgendes:

- Status der Funktion der Windows-Firewall.
- Status der Regeln, die nach der Installation von Kaspersky Embedded Systems Security von anderen Programmen oder Tools hinzugefügt wurden (z. B. Hinzufügen einer neuen Regel des Programms für einen Port oder eine App mithilfe von wf.msc)

Wenn Sie die neuen Regeln für die Windows Firewall übernehmen, erstellt Kaspersky Embedded Systems Security einen Satz von Gruppenregeln für Kaspersky Security im **Windows Firewall**-Snap-in. Dieser Regelsatz vereint alle von Kaspersky Embedded Systems Security mithilfe der Aufgabe zur Firewall-Verwaltung erstellten Regeln. Die Regeln, die zur Gruppe Kaspersky Security Group gehören, werden vom Programm bei der minutenweisen Abfrage nicht überprüft und nicht automatisch mit der Liste der Regeln synchronisiert, die in den Einstellungen der Aufgabe zur Firewall-Verwaltung festgelegt wurden. Bei Bedarf können Sie das Update der Regeln von Kaspersky Security Group manuell vornehmen.

► *Um die Regelliste von Kaspersky Security Group manuell zu aktualisieren,*

starten Sie die Aufgabe zur Firewall-Verwaltung in Kaspersky Embedded Systems Security neu.

Außerdem können Sie die Regeln von Kaspersky Security Group manuell über das Snap-In **Windows Firewall** anpassen.

Der Start der Aufgabe zur Firewall-Verwaltung ist nicht möglich, wenn die Windows-Firewall von der Gruppenrichtlinie von Kaspersky Security Center verwaltet wird.

Über Firewall-Regeln

Die Aufgabe "Firewall-Verwaltung" kontrolliert die Filterung des eingehenden und ausgehenden Datenverkehrs mithilfe von Erlaubnisregeln, deren Weitergabe an die Windows-Firewall bei der Aufgabenausführung erzwungen wird.

Beim ersten Aufgabenstart liest Kaspersky Embedded Systems Security alle Erlaubnisregeln für den eingehenden Datenverkehr, die in den Einstellungen der Windows-Firewall festgelegt sind, und kopiert sie in die Einstellungen der Aufgabe "Firewall-Verwaltung". Von diesem Zeitpunkt an wird das Programm nach den folgenden Algorithmen ausgeführt:

- Wenn in den Einstellungen der Windows-Firewall eine neue Regel erstellt wird (manuell oder automatisch bei der Installation einer neuen App), löscht Kaspersky Embedded Systems Security diese Regel.
- Wenn in den Einstellungen der Windows-Firewall eine bereits vorhandene Regel gelöscht wird, stellt Kaspersky Embedded Systems Security diese Regel bei einem Neustart der Aufgabe wieder her.
- Wenn in den Einstellungen der Windows-Firewall die Einstellungen einer vorhandenen Regel geändert

werden, verwirft Kaspersky Embedded Systems Security die Änderungen.

- Wenn in den Einstellungen der Aufgabe "Firewall-Verwaltung" eine neue Regel erstellt wird, erzwingt Kaspersky Embedded Systems Security die Übernahme dieser Regel durch die Windows-Firewall.
- Wenn in den Einstellungen der Aufgabe zur Firewall-Verwaltung eine bereits vorhandene Regel gelöscht wird, erzwingt Kaspersky Embedded Systems Security das Löschen dieser Regel aus den Einstellungen der Windows-Firewall.

Kaspersky Embedded Systems Security funktioniert nicht mit Verbotsregeln sowie mit Regeln, die den ausgehenden Datenverkehr kontrollieren. Zum Zeitpunkt des Starts der Aufgabe "Firewall-Verwaltung" löscht Kaspersky Embedded Systems Security alle Regeln dieser Art aus den Einstellungen der Windows-Firewall.

Zur Filterung des eingehenden Datenverkehrs können Sie Regeln festlegen, löschen und bearbeiten.

Für die Kontrolle des ausgehenden Datenverkehrs können Sie keine neue Regel in den Einstellungen der Aufgabe zur Firewall-Verwaltung festlegen. Alle Firewall-Regeln, die über Kaspersky Embedded Systems Security festgelegt werden, kontrollieren nur den eingehenden Datenverkehr.

Sie können mit Firewall-Regeln folgender Arten arbeiten:

- Regeln für Programme.
- Regeln für Ports

Regeln für Apps

Regeln dieser Art erlauben Netzwerkverbindungen für ausgewählte angegebene Apps. Ein Auslösekriterium für solche Regeln ist der Pfad zur ausführbaren Datei.

Sie können die Regeln für Apps auf folgende Weise verwalten:

- Neue Regeln hinzufügen
- Vorhandene Regeln löschen
- Festgelegte Regeln aktivieren oder deaktivieren
- Einstellungen der festgelegten Regeln ändern: Regelname, Pfad der ausführbaren Datei und Gültigkeitsbereich der Regel angeben

Regeln für Ports

Regeln dieser Art erlauben Netzwerkverbindungen für angegebene Ports und Protokolle (TCP/UDP). Die Auslösekriterien solcher Regeln sind die Portnummer und der Typ des Protokolls.

Sie können Regeln für Ports auf folgende Weise verwalten:

- Neue Regeln hinzufügen
- Vorhandene Regeln löschen
- Festgelegte Regeln aktivieren oder deaktivieren
- Einstellungen der festgelegten Regeln ändern: Regelname, Portnummer, Protokolltyp und Gültigkeitsbereich der Regel festlegen

Die Regeln für Ports sind mit einem größeren Gültigkeitsbereich verbunden als die Regeln für Apps. Indem Sie Verbindungen anhand von Regeln für Ports erlauben, reduzieren Sie die Sicherheitsstufe des geschützten Computers.

Standardeinstellungen der Aufgabe zur Firewall-Verwaltung

Die Aufgabe zur Firewall-Verwaltung weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 52. Standardeinstellungen der Aufgabe zur Firewall-Verwaltung

Einstellung	Standardwert	Beschreibung
Firewall-Regeln für das Programm	Zwei Standardregeln für das Programm aktiviert	Sie können die Standardregeln deaktivieren oder neue Regeln hinzufügen.
Firewall-Regeln für Ports	Sechs Standardregeln für Ports aktiviert	Sie können die Standardregeln deaktivieren oder neue Regeln hinzufügen.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Firewall-Verwaltung wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können den Zeitplan für den Aufgabenstart konfigurieren.

Firewall-Regeln über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie Firewall-Regeln über die Benutzeroberfläche der Programmkonsole hinzufügen und konfigurieren.

In diesem Abschnitt

Firewall-Regeln aktivieren und deaktivieren

► *Um eine bereits vorhandene Regel zur Filterung des eingehenden Datenverkehrs zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   > Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Firewall-Verwaltung**.
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
6. Wählen Sie je nach Art der Regel, deren Status Sie ändern möchten, die Registerkarte **Programme** oder **Ports** aus.
7. 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.
8. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **OK**.
9. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln manuell hinzufügen

Sie können nur Regeln für Apps und Ports hinzufügen und bearbeiten. Sie können für Gruppen keine neuen Regeln hinzufügen oder bereits vorhandene Regeln bearbeiten.

► *Um eine neue Regel zur Filterung des eingehenden Datenverkehrs hinzuzufügen oder eine bereits vorhandene Regel zu ändern, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Firewall-Verwaltung**.
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
6. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus – je nachdem, welche Art der Regel Sie hinzufügen möchten – und führen Sie eine der folgenden Aktionen aus:
   - Um eine bereits vorhandene Regel zu ändern, wählen Sie in der Regelliste die Regel aus, deren Einstellungen Sie anpassen möchten, und klicken Sie auf **Ändern**.
   - Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**.

     Je nach Art der angepassten Regel öffnet sich das Fenster **Regel für Port anpassen** oder das Fenster **Regel für Programm anpassen**.
7. Im sich öffnenden Fenster gehen Sie wie folgt vor:
   - Wenn Sie eine Regel für Apps anpassen, gehen Sie wie folgt vor:
     a. Geben Sie im Feld **Regelname** den Namen der bearbeiteten Regel an.
     b. Geben Sie im Feld **Pfad zum Programm** den Pfad zur ausführbaren Datei des Programms an, für das Sie mithilfe der bearbeiteten Regel Verbindungen erlauben möchten.

        Sie können den Pfad manuell oder über die Schaltfläche **Durchsuchen** angeben.
     c. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

Die Angabe von IP-Adressen ist nur im Format IPv4 zulässig.

- Wenn Sie eine Regel für Ports anpassen, gehen Sie wie folgt vor:
  a. Geben Sie im Feld **Regelname** den Namen der bearbeiteten Regel an.
  b. Geben Sie im Feld **Portnummer** die Portnummer an, für die das Programm Verbindungen erlauben soll.
  c. Wählen Sie den Typ des Protokolls (TCP/UDP) aus, für den das Programm Verbindungen erlauben soll.
  d. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

Die Angabe von IP-Adressen ist nur im Format IPv4 zulässig.

8. Klicken Sie im Fenster **Regel für Programm anpassen** oder **Regel für Port anpassen** auf **OK**.
9. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln löschen

Sie können nur Regeln für Apps und Ports löschen. Sie können bereits vorhandene Regeln für Gruppen nicht löschen.

► *Um eine bereits vorhandene Regel zur Filterung von eingehendem Datenverkehr zu löschen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Firewall-Verwaltung.**
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
6. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
7. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
8. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählte Regel wird gelöscht.
9. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **OK**.
10. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.
11. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Die angegebenen Aufgabeneinstellungen für die Firewall-Verwaltung werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie Firewall-Regeln über die Benutzeroberfläche der Programmkonsole hinzufügen und konfigurieren.

In diesem Abschnitt

Firewall-Regeln aktivieren und deaktivieren

► *Um eine bereits vorhandene Regel zur Filterung des eingehenden Datenverkehrs zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Firewall-Verwaltung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Firewall-Verwaltung** auf den Link **Firewall-Regeln**.

   Das Fenster **Firewall-Regeln** wird geöffnet.

4. Wählen Sie je nach Art der Regel, deren Status Sie ändern möchten, die Registerkarte **Programme** oder **Ports** aus.
5. 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. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln manuell hinzufügen

► *Um eine neue Regel zur Filterung des eingehenden Datenverkehrs hinzuzufügen oder eine bereits vorhandene Regel zu ändern, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Firewall-Verwaltung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Firewall-Verwaltung** auf den Link **Firewall-Regeln**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
4. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus – je nachdem, welche Art der Regel Sie hinzufügen möchten – und führen Sie eine der folgenden Aktionen aus:
   - Um eine bereits vorhandene Regel zu ändern, wählen Sie in der Regelliste die Regel aus, deren Einstellungen Sie anpassen möchten, und klicken Sie auf **Ändern**.
   - Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**.

     Je nach Art der angepassten Regel öffnet sich das Fenster **Regel für Port anpassen** oder das Fenster **Regel für Programm anpassen**.
5. Im sich öffnenden Fenster gehen Sie wie folgt vor:
   - Wenn Sie eine Regel für Apps anpassen, gehen Sie wie folgt vor:
     a. Geben Sie im Feld **Regelname** den Namen der bearbeiteten Regel an.
     b. Geben Sie im Feld **Pfad zum Programm** den Pfad zur ausführbaren Datei des Programms an, für das Sie mithilfe der bearbeiteten Regel Verbindungen erlauben möchten.

        Sie können den Pfad manuell oder über die Schaltfläche **Durchsuchen** angeben.
     c. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

     Die Angabe von IP-Adressen ist nur im Format IPv4 zulässig.

- Wenn Sie eine Regel für Ports anpassen, gehen Sie wie folgt vor:
  a. Geben Sie im Feld **Regelname** den Namen der bearbeiteten Regel an.
  b. Geben Sie im Feld **Portnummer** die Portnummer an, für die das Programm Verbindungen erlauben soll.
  c. Wählen Sie den Typ des Protokolls (TCP/UDP) aus, für den das Programm Verbindungen erlauben soll.
  d. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

  Die Angabe von IP-Adressen ist nur im Format IPv4 zulässig.

6. Klicken Sie im Fenster **Regel für Programm anpassen** oder **Regel für Port anpassen** auf **OK**.
7. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln löschen

Sie können nur Regeln für Apps und Ports löschen. Sie können bereits vorhandene Regeln für Gruppen nicht löschen.

► *Um eine bereits vorhandene Regel zur Filterung von eingehendem Datenverkehr zu löschen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Firewall-Verwaltung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Firewall-Verwaltung** auf den Link **Firewall-Regeln**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
4. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
5. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
6. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählte Regel wird gelöscht.
7. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Überwachung der Datei-Integrität

Dieser Abschnitt enthält Informationen über den Start und das Anpassen der Aufgabe zur Überwachung der Datei-Integrität.

In diesem Kapitel

Über die Aufgabe Überwachung der Datei-Integrität

Die Aufgabe Überwachung der Datei-Integrität überwacht Aktionen, die mit bestimmten Dateien oder Ordnern ausgeführt werden, im Rahmen von Überwachungsbereichen, die in den Einstellungen der Aufgabe festgelegt wurden. Mithilfe der Aufgabe können Sie Änderungen an Dateien erkennen, die eventuell auf eine Verletzung der Sicherheit auf dem geschützten Computer hindeuten. Sie können außerdem Änderungen an Dateien in Zeiträumen nachverfolgen, in denen die Überwachung unterbrochen war.

Eine *Unterbrechung der Überwachung* tritt auf, wenn der Überwachungsbereich vorübergehend aus dem Gültigkeitsbereich der Aufgabe fällt, weil z. B. die Aufgabenausführung angehalten wird oder ein Massenspeichergerät nicht physisch auf einem geschützten Computer vorhanden ist. Kaspersky Embedded Systems Security benachrichtigt Sie über gefundene Dateioperationen im Überwachungsbereich, sobald das Massenspeichergerät wieder angeschlossen ist.

Wenn das Anhalten der Aufgabenausführung im festgelegten Überwachungsbereich durch eine Neuinstallation der Komponente "Überwachung der Datei-Integrität" verursacht wurde, gilt dies nicht als Unterbrechung der Überwachung. In diesem Fall wird die Aufgabe Überwachung der Datei-Integrität nicht ausgeführt.

Umgebungsanforderungen

Für die Ausführung der Aufgabe Überwachung der Datei-Integrität müssen folgende Voraussetzungen erfüllt sein:

- Auf dem geschützten Computer ist ein Massenspeichergerät installiert, der die Dateisysteme ReFS und NTFS unterstützt
- Das Windows USN-Protokoll ist aktiviert. Die Komponente fragt dieses Protokoll ab, um Informationen über Dateioperationen zu erhalten.

Wenn Sie das USN-Protokoll aktiviert haben, nachdem die Regel für das Laufwerk erstellt und die Aufgabe zur Überwachung der Datei-Integrität gestartet wurde, ist es erforderlich, die Aufgabe neu zu starten. Andernfalls wird die Regel bei der Überwachung nicht berücksichtigt.

Ausnahmen für den Überwachungsbereich

Sie können Ausnahmen von Überwachungsbereichen erstellen (siehe Abschnitt "Einstellungen der Überwachungsregeln anpassen" auf Seite 406). Die Ausnahmen werden für jede einzelne Regel angegeben und gelten nur für den angegebenen Überwachungsbereich. Sie können für jede Regel eine unbegrenzte Anzahl an Ausnahmen festlegen.

Ausnahmen haben eine höhere Priorität als der Überwachungsbereich und werden von der Aufgabe nicht überwacht, selbst wenn ein angegebener Ordner oder eine Datei in den Überwachungsbereich fallen sollte. Wenn die Einstellungen für eine der Regeln einen Überwachungsbereich angeben, der sich auf einer niedrigeren Stufe befindet als ein in den Ausnahmen angegebener Ordner, wird der Überwachungsbereich bei der Ausführung der Aufgabe nicht berücksichtigt.

Zur Angabe von Ausnahmen können Sie die gleichen Masken verwenden wie für die Angabe des Überwachungsbereichs.

Über die Regeln zur Überwachung von Datei-Operationen

Die Aufgabe Überwachung der Datei-Integrität wird auf der Grundlage der Regeln zur Überwachung von Datei-Operationen ausgeführt. Sie können mithilfe von Auslösekriterien für Regeln die Bedingungen zum Auslösen der Aufgabe anpassen und die Prioritätsstufe für gefundene Dateioperationen bestimmen, die im Protokoll der Aufgabenausführung gespeichert werden.

Die Regel zur Überwachung von Datei-Operationen wird für jeden festgelegten Überwachungsbereich angegeben.

Sie können folgende Auslösekriterien für Regeln anpassen:

- Vertrauenswürdige Benutzer
- Datei-Operations-Marker

Vertrauenswürdige Benutzer

Standardmäßig stuft das Programm die Aktionen aller Benutzer als potenzielle Verletzungen der Sicherheit ein. Die Liste mit vertrauenswürdigen Benutzern ist leer. Sie können die Prioritätsstufe des Ereignisses anpassen, indem Sie eine Liste mit vertrauenswürdigen Benutzern in den Einstellungen der Regel zur Überwachung von Datei-Operationen erstellen.

Ein *nicht vertrauenswürdiger Benutzer* ist ein beliebiger Benutzer, der nicht zur Liste vertrauenswürdiger Benutzer in den Einstellungen des Überwachungsbereichs hinzugefügt wurde. Wenn Kaspersky Embedded Systems Security eine Dateioperation findet, die von einem nicht vertrauenswürdigen Benutzer ausgeführt wurde, protokolliert die Aufgabe zur Überwachung der Datei-Integrität ein Ereignis mit der Ereigniskategorie "Kritisches Ereignis" im Protokoll der Aufgabenausführung.

Ein vertrauenswürdiger Benutzer ist ein Benutzer oder eine Benutzergruppe, dem/der das Ausführen von Dateioperationen im angegebenen Überwachungsbereich erlaubt ist. Wenn Kaspersky Embedded Systems Security Dateioperationen findet, die von einem vertrauenswürdigen Benutzer ausgeführt wurden, protokolliert

die Aufgabe zur Überwachung der Datei-Integrität ein Informatives Ereignis im Protokoll der Aufgabenausführung.

Kaspersky Embedded Systems Security kann Benutzer nicht bestimmen, die Operationen in einem Zeitraum, in dem die Überwachung unterbrochen war, ausführen. In diesem Fall wird der Status des Benutzers als Unbekannt angegeben.

Unbekannter Benutzer – dieser Status wird einem Benutzer zugewiesen, wenn Kaspersky Embedded Systems Security keine Daten über den Benutzer abrufen kann, da die Aufgabe unterbrochen wurde oder eine Störung in der Synchronisierung der Treiberdaten oder des USN-Protokolls aufgetreten ist. Wenn Kaspersky Embedded Systems Security eine Dateioperation findet, die von einem unbekannten Benutzer ausgeführt wurde, speichert die Aufgabe zur Überwachung der Datei-Integrität das Ereignis mit der Ereigniskategorie *Warnung* im Protokoll der Aufgabenausführung.

Datei-Operations-Marker

Während der Ausführung der Aufgabe zur Überwachung der Datei-Integrität ermittelt Kaspersky Embedded Systems Security mithilfe von Datei-Operations-Markern, ob eine Aktion mit einer Datei ausgeführt wurde.

Der Datei-Operations-Marker ist ein eindeutiges Merkmal, mit dem eine Dateioperation charakterisiert werden kann.

Jede Dateioperation kann eine einzelne Aktion oder eine Kette von Aktionen mit Dateien darstellen. Jede solche Aktion wird einem Datei-Operations-Marker gleichgestellt. Wenn in der Kette der Dateioperationen ein Marker gefunden wird, der von Ihnen als Auslösekriterium für eine Überwachungsregel festgelegt wurde, protokolliert das Programm das Ereignis nach der Durchführung einer solchen Dateioperation.

Die Prioritätsstufe der protokollierten Ereignisse hängt nicht von den ausgewählten Datei-Operations-Markern oder ihrer Anzahl ab.

Standardmäßig werden von Kaspersky Embedded Systems Security alle verfügbaren Datei-Operations-Marker berücksichtigt. Sie können Datei-Operations-Marker manuell in den Einstellungen der Aufgabenregeln auswählen (s. Tabelle unten).

Tabelle 53. Datei-Operations-Marker

ID der Dateioperation	Datei-Operations-Marker	Unterstützte Dateisysteme
BASIC_INFO_CHANGE	Attribute oder Zeitstempel der Datei bzw. des Ordners wurden verändert	NTFS, ReFS
COMPRESSION_CHANGE	Die Komprimierungsrate der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
DATA_EXTEND	Die Größe der Datei bzw. des Ordners hat sich erhöht	NTFS, ReFS
DATA_OVERWRITE	Daten in der Datei bzw. dem Ordner wurden überschrieben	NTFS, ReFS
DATA_TRUNCATION	Die Datei bzw. der Ordner wurde gekürzt	NTFS, ReFS
EA_CHANGE	Erweiterte Attribute von Datei oder Ordner wurden verändert	Nur NTFS

ID der Dateioperation	Datei-Operations-Marker	Unterstützte Dateisysteme
ENCRYPTION_CHANGE	Der Verschlüsselungsstatus der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
FILE_CREATE	Die Datei bzw. der Ordner wurde zum ersten Mal erstellt	NTFS, ReFS
FILE_DELETE	Eine Datei oder ein Ordner wurde mit der Tastenkombination UMSCHALT+ENTF permanent gelöscht.	NTFS, ReFS
HARD_LINK_CHANGE	Für die Datei bzw. den Ordner wurde ein harter Link erstellt oder gelöscht	Nur NTFS
INDEXABLE_CHANGE	Der Indizierungsstatus der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
INTEGRITY_CHANGE	Das Integritätsattribut für den benannten Dateidatenstrom wurde verändert	Nur ReFS
NAMED_DATA_EXTEND	Die Größe des benannten Dateidatenstroms hat sich erhöht	NTFS, ReFS
NAMED_DATA_OVERWRITE	Ein benannter Dateidatenstrom wurde überschrieben	NTFS, ReFS
NAMED_DATA_TRUNCATION	Ein benannter Dateidatenstrom wurde gekürzt	NTFS, ReFS
OBJECT_ID_CHANGE	Die ID der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
RENAME_NEW_NAME	Der Datei bzw. dem Ordner wurde ein neuer Name zugewiesen	NTFS, ReFS
REPARSE_POINT_CHANGE	Für die Datei bzw. den Ordner wurde ein neuer Analysepunkt erstellt oder ein vorhandener Punkt verändert	NTFS, ReFS
SECURITY_CHANGE	Die Zugriffsrechte zur Datei bzw. zum Ordner wurden verändert	NTFS, ReFS
STREAM_CHANGE	Ein neuer benannter Dateidatenstrom wurde erstellt oder ein vorhandener verändert	NTFS, ReFS
TRANSACTED_CHANGE	Ein benannter Dateidatenstrom wurde durch die TxF-Transaktion verändert	Nur ReFS

Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Die Aufgabe "Überwachung der Datei-Integrität" weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 54. Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Standardwert	Beschreibung
Überwachungsbereich	Nicht festgelegt.	Sie können Ordner und Dateien angeben, deren Aktionen überwacht werden sollen. Für die Ordner und Dateien des angegebenen Überwachungsbereichs werden Überwachungsereignisse erstellt.
Liste mit vertrauenswürdigen Benutzern	Nicht festgelegt.	Sie können Benutzer und\oder Benutzergruppen festlegen, deren Aktionen in den angegebenen Ordnern von der Komponente als sicher bewertet werden sollen.
Dateioperationen in Leerlaufperioden der Aufgabe kontrollieren	Wird verwendet	Sie können die Protokollierung von Dateioperationen aktivieren oder deaktivieren, die in den angegebenen Überwachungsbereichen in Leerlaufperioden der Aufgabe ausgeführt wurden.
Folgende Ordner aus der Überwachung ausschließen	Wird nicht verwendet	Sie können die Anwendung von Ausnahmen für Ordner regeln, in denen keine Dateioperationen überwacht werden müssen. Bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität überspringt Kaspersky Embedded Systems Security Überwachungsbereiche, die als Ausnahmen festgelegt wurden.
Berechnung der Prüfsumme	Wird nicht verwendet	Sie können festlegen, dass die Berechnung der Prüfsumme der Datei nach deren Bearbeitung durchgeführt wird.
Datei-Operations-Marker berücksichtigen	Es werden alle verfügbaren Datei-Operations-Marker berücksichtigt.	Sie können eine Reihe von Markern angeben, die Dateioperationen kennzeichnen. Wenn eine im Überwachungsbereich ausgeführte Dateioperation mit einem oder mehreren angegebenen Marker gekennzeichnet ist, erstellt Kaspersky Embedded Systems Security ein Systemaudit-Ereignis.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Überwachung der Datei-Integrität über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung der Datei-Integrität über das Verwaltungs-Plug-in konfigurieren.

In diesem Abschnitt

Einstellungen der Aufgabe "Überwachung der Datei-Integrität" anpassen

Gehen Sie wie folgt vor, um die Einstellungen der Aufgabe zur Überwachung der Datei-Integrität anzupassen:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **System-Diagnose** im Block **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung der Datei-Integrität** wird geöffnet.
5. Passen Sie im folgenden Fenster auf der Registerkarte **Einstellungen zur Überwachung von Dateioperationen** die Einstellungen des Überwachungsbereichs an:

   a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden**.

      Das Kontrollkästchen aktiviert oder deaktiviert die Überwachung der Dateioperationen, die in den Einstellungen der Aufgabe Überwachung der Datei-Integrität ausgewählt sind, auch in Zeiträumen, in denen die Aufgabenausführung aus irgendeinem Grund unterbrochen ist (Entfernung der Festplatte, Beenden der Aufgabe durch Benutzer, Funktionsstörung der Software).

      Wenn das Kontrollkästchen aktiviert ist, protokolliert Kaspersky Embedded Systems

Security die Ereignisse in allen Überwachungsbereichen während der Unterbrechung der Aufgabe zur Überwachung der Datei-Integrität.

Wenn das Kontrollkästchen deaktiviert ist, werden die Dateioperationen in den Überwachungsbereichen bei einer Unterbrechung der Aufgabe nicht vom Programm protokolliert.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

b. Fügen Sie die Überwachungsbereiche (siehe Abschnitt "Einstellungen der Überwachungsregeln anpassen" auf Seite 406) hinzu, die von der Aufgabe überwacht werden sollen.

6. Konfigurieren Sie auf der Registerkarte **Aufgabenverwaltung** die Aufgabe auf der Grundlage eines Zeitplans (siehe Abschnitt "Arbeit mit dem Aufgabenzeitplan" auf Seite 139).

7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Einstellungen der Überwachungsregeln anpassen

Sie können die Standard-Einstellungen der Aufgabe Überwachung der Datei-Integrität anpassen (s. Tabelle unten).

Tabelle 55. Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Standardwert	Beschreibung
Überwachungsbereich	Nicht festgelegt.	Sie können Ordner und Dateien angeben, deren Aktionen überwacht werden sollen. Für die Ordner und Dateien des angegebenen Überwachungsbereichs werden Überwachungsereignisse erstellt.
Liste mit vertrauenswürdigen Benutzern	Nicht festgelegt.	Sie können Benutzer und\oder Benutzergruppen festlegen, deren Aktionen in den angegebenen Ordnern von der Komponente als sicher bewertet werden sollen.
Dateioperationen in Leerlaufperioden der Aufgabe kontrollieren	Wird verwendet	Sie können die Protokollierung von Dateioperationen aktivieren oder deaktivieren, die in den angegebenen Überwachungsbereichen in Leerlaufperioden der Aufgabe ausgeführt wurden.
Folgende Ordner aus der Überwachung ausschließen	Wird nicht verwendet	Sie können die Anwendung von Ausnahmen für Ordner regeln, in denen keine Dateioperationen überwacht werden müssen. Bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität überspringt Kaspersky Embedded Systems Security Überwachungsbereiche, die als Ausnahmen festgelegt wurden.
Berechnung der Prüfsumme	Wird nicht verwendet	Sie können festlegen, dass die Berechnung der Prüfsumme der Datei nach deren Bearbeitung durchgeführt wird.

Einstellung	Standardwert	Beschreibung
Datei-Operations-Marker berücksichtigen	Es werden alle verfügbaren Datei-Operations-Marker berücksichtigt.	Sie können eine Reihe von Markern angeben, die Dateioperationen kennzeichnen. Wenn eine im Überwachungsbereich ausgeführte Dateioperation mit einem oder mehreren angegebenen Marker gekennzeichnet ist, erstellt Kaspersky Embedded Systems Security ein Systemaudit-Ereignis.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

► *Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

     Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **System-Diagnose** im Block **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Eigenschaften: Überwachung der Datei-Integrität** wird geöffnet.
5. Klicken Sie im Block **Überwachungsbereich** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Überwachungsbereich** wird geöffnet.
6. Fügen Sie den Überwachungsbereich auf eine der folgenden Arten hinzu:
   - Wenn Sie im Standarddialog von Microsoft Windows Ordner auswählen möchten:
     a. Klicken Sie auf die Schaltfläche **Durchsuchen**.

        Das Microsoft-Windows-Standardfenster "Ordner suchen" wird geöffnet.

     b. Wählen Sie im nächsten Fenster den Ordner aus, dessen Dateioperationen Sie überwachen möchten, und klicken Sie auf **OK**.
   - Um den Überwachungsbereich manuell festzulegen, fügen Sie mithilfe einer der unterstützten Masken einen Pfad hinzu:
     - <*.ext> – alle Dateien mit der Erweiterung <ext> unabhängig von ihrem Speicherort

- <*\name.ext> – alle Dateien mit dem Namen <name> und der Erweiterung <ext> unabhängig von ihrem Speicherort
- <\dir*> – alle Dateien im Ordner <\dir>
- <\dir*\name.ext> – alle Dateien mit dem Namen <name> und der Erweiterung <ext> im Ordner <\dir> und allen Unterordnern

Stellen Sie bei der manuellen Angabe des Überwachungsbereichs sicher, dass der Pfad dem folgenden Format entspricht: <Laufwerksbuchstabe>:\<Maske>. Wenn der Laufwerksbuchstabe fehlt, fügt Kaspersky Embedded Systems Security den angegebenen Überwachungsbereich nicht hinzu.

7. Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

   Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** wird geöffnet.

8. Wählen Sie die Benutzer oder Benutzergruppen aus, die Dateioperationen in den ausgewählten Überwachungsbereichen ausführen dürfen, und klicken Sie auf **OK**.

Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 401) und erstellt für sie kritische Ereignisse.

9. Wählen Sie die Registerkarte **Datei-Operations-Marker** aus.
10. Gehen Sie wie folgt vor, um bei Bedarf mehrere Datei-Operations-Marker auszuwählen:
    a. Wählen Sie die Option **Dateioperationen anhand der folgenden Marker erkennen** aus.
    b. Aktivieren Sie in der Liste der verfügbaren Dateioperationen (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 401) die Kontrollkästchen aller Operationen, die Sie überwachen möchten.

Standardmäßig überwacht Kaspersky Embedded Systems Security alle verfügbaren Dateioperationen, wenn die Option **Dateioperationen anhand von allen identifizierbaren Markern erkennen** ausgewählt ist.

11. Wenn Sie möchten, dass Kaspersky Embedded Systems Security die Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:
    a. Aktivieren Sie das Kontrollkästchen **Prüfsumme der Datei berechnen, wenn möglich. Die Prüfsumme wird im Aufgabenbericht angezeigt.**

       Wenn das Kontrollkästchen aktiviert ist, ermittelt Kaspersky Embedded Systems Security die Prüfsumme der geänderten Datei, in der eine Dateioperation gefunden wurde, die mindestens einem Datei-Operations-Marker entspricht.

       Wenn die Dateioperation anhand mehrerer Marker gleichzeitig gefunden wird, so wird nur die endgültige Prüfsumme der Datei nach allen Änderungen ermittelt.

       Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security keine Prüfsumme für geänderte 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.

b. Wählen Sie in der Dropdown-Liste **Prüfsumme anhand von Algorithmus berechnen** eine der folgenden Optionen aus:

- **MD5-Hash**
- **SHA256-Hash**

12. Wenn Sie nicht alle Dateioperationen überwachen möchten, aktivieren Sie in der Liste der verfügbaren Dateioperationen (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 401) die Kontrollkästchen neben den Operationen, die Sie überwachen möchten.
13. Gehen Sie wie folgt vor, um bei Bedarf Ausnahmen für den Überwachungsbereich hinzuzufügen:
    a. Wählen Sie die Registerkarte **Ausnahmen** aus.
    b. Aktivieren Sie das Kontrollkästchen **Folgende Ordner aus der Überwachung ausschließen**.

       Das Kontrollkästchen aktiviert oder deaktiviert die Anwendung von Ausnahmen für Ordner, in denen keine Dateioperationen überwacht werden müssen.

       Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität die Überwachungsbereiche, die zur Liste mit Ausnahmen hinzugefügt wurden.

       Wenn das Kontrollkästchen deaktiviert ist, protokolliert Kaspersky Embedded Systems Security Ereignisse für alle angegebenen Überwachungsbereiche.

       Standardmäßig ist das Kontrollkästchen deaktiviert und die Ausnahmeliste leer.

    c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

       Das Fenster **Ordner zum Hinzufügen auswählen** wird geöffnet.

    d. Wählen Sie im geöffneten Fenster den Ordner aus, den Sie aus dem Überwachungsbereich ausschließen möchten.

    e. Klicken Sie auf **OK**.

       Der angegebene Ordner wird zur Liste der ausgeschlossenen Bereiche hinzugefügt.

14. Klicken Sie im Fenster **Regel zur Überwachung von Datei-Operationen** auf **OK**.

    Die angegebenen Einstellungen der Regeln werden im ausgewählten Überwachungsbereich der Aufgabe "Überwachung der Datei-Integrität" gelten.

Überwachung der Datei-Integrität über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung der Datei-Integrität über die Programmkonsole konfigurieren.

In diesem Abschnitt

Einstellungen der Aufgabe "Überwachung der Datei-Integrität" anpassen

► *Gehen Sie wie folgt vor, um die Einstellungen der Aufgabe zur Überwachung der Datei-Integrität anzupassen:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Überwachung der Datei-Integrität** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Überwachung der Datei-Integrität** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Deaktivieren oder aktivieren Sie im nächsten Fenster auf der Registerkarte **Allgemein** das Kontrollkästchen **Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden**.

   Das Kontrollkästchen aktiviert oder deaktiviert die Überwachung der Dateioperationen, die in den Einstellungen der Aufgabe Überwachung der Datei-Integrität ausgewählt sind, auch in Zeiträumen, in denen die Aufgabenausführung aus irgendeinem Grund unterbrochen ist (Entfernung der Festplatte, Beenden der Aufgabe durch Benutzer, Funktionsstörung der Software).

   Wenn das Kontrollkästchen aktiviert ist, protokolliert Kaspersky Embedded Systems Security die Ereignisse in allen Überwachungsbereichen während der Unterbrechung der Aufgabe zur Überwachung der Datei-Integrität.

   Wenn das Kontrollkästchen deaktiviert ist, werden die Dateioperationen in den Überwachungsbereichen bei einer Unterbrechung der Aufgabe nicht vom Programm protokolliert.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
5. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan an (siehe Abschnitt "Arbeit mit dem Aufgabenzeitplan" auf Seite 139).
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Einstellungen der Überwachungsregeln anpassen

Sie können die Standard-Einstellungen der Aufgabe Überwachung der Datei-Integrität anpassen (s. Tabelle unten).

Tabelle 56. Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Standardwert	Beschreibung
Überwachungsbereich	Nicht festgelegt.	Sie können Ordner und Dateien angeben, deren Aktionen überwacht werden sollen. Für die Ordner und Dateien des angegebenen Überwachungsbereichs werden Überwachungsereignisse erstellt.
Liste mit vertrauenswürdigen Benutzern	Nicht festgelegt.	Sie können Benutzer und\oder Benutzergruppen festlegen, deren Aktionen in den angegebenen Ordnern von der Komponente als sicher bewertet werden sollen.
Dateioperationen in Leerlaufperioden der Aufgabe kontrollieren	Wird verwendet	Sie können die Protokollierung von Dateioperationen aktivieren oder deaktivieren, die in den angegebenen Überwachungsbereichen in Leerlaufperioden der Aufgabe ausgeführt wurden.
Folgende Ordner aus der Überwachung ausschließen	Wird nicht verwendet	Sie können die Anwendung von Ausnahmen für Ordner regeln, in denen keine Dateioperationen überwacht werden müssen. Bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität überspringt Kaspersky Embedded Systems Security Überwachungsbereiche, die als Ausnahmen festgelegt wurden.
Berechnung der Prüfsumme	Wird nicht verwendet	Sie können festlegen, dass die Berechnung der Prüfsumme der Datei nach deren Bearbeitung durchgeführt wird.
Datei-Operations-Marker berücksichtigen	Es werden alle verfügbaren Datei-Operations-Marker berücksichtigt.	Sie können eine Reihe von Markern angeben, die Dateioperationen kennzeichnen. Wenn eine im Überwachungsbereich ausgeführte Dateioperation mit einem oder mehreren angegebenen Marker gekennzeichnet ist, erstellt Kaspersky Embedded Systems Security ein Systemaudit-Ereignis.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

► *Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Überwachung der Datei-Integrität** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Überwachung der Datei-Integrität** auf den Link **Regel zur Überwachung von Datei-Operationen**.

Das Fenster **Überwachung von Dateioperationen** wird geöffnet.

4. Fügen Sie den Überwachungsbereich auf eine der folgenden Arten hinzu:
   - Wenn Sie im Standarddialog von Microsoft Windows Ordner auswählen möchten:
     a. Klicken Sie im linken Bereich des Fensters auf die Schaltfläche **Durchsuchen**.

        Das Microsoft-Windows-Standardfenster **Ordner suchen** wird geöffnet.

     b. Wählen Sie im nächsten Fenster den Ordner aus, dessen Dateioperationen Sie überwachen möchten, und klicken Sie auf **OK**.

     c. Klicken Sie auf **Hinzufügen**, Kaspersky Embedded Systems Security damit beginnt, Dateioperationen im angegebenen Überwachungsbereich zu überwachen.
   - Um den Überwachungsbereich manuell festzulegen, fügen Sie mithilfe einer der unterstützten Masken einen Pfad hinzu:
     - <*.ext> – alle Dateien mit der Erweiterung <ext> unabhängig von ihrem Speicherort
     - <*\name.ext> – alle Dateien mit dem Namen <name> und der Erweiterung <ext> unabhängig von ihrem Speicherort
     - <\dir*> – alle Dateien im Ordner <\dir>
     - <\dir*\name.ext> – alle Dateien mit dem Namen <name> und der Erweiterung <ext> im Ordner <\dir> und allen Unterordnern

   Stellen Sie bei der manuellen Angabe des Überwachungsbereichs sicher, dass der Pfad dem folgenden Format entspricht: <Laufwerksbuchstabe>:\<Maske>. Wenn der Laufwerksbuchstabe fehlt, fügt Kaspersky Embedded Systems Security den angegebenen Überwachungsbereich nicht hinzu.

   Im rechten Fensterbereich auf der Registerkarte **Regelbeschreibung** werden vertrauenswürdige Benutzer und Marker für Datei-Operationen angezeigt, die für diesen Überwachungsbereich gewählt wurden.

5. Wählen Sie in der Liste der hinzugefügten Überwachungsbereiche den Bereich aus, für den Sie andere Einstellungen anpassen möchten.
6. Wählen Sie die Registerkarte **Vertrauenswürdige Benutzer** aus.
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** wird geöffnet.
8. Wählen Sie die Benutzer oder Benutzergruppen aus, die Kaspersky Embedded Systems Security für den ausgewählten Überwachungsbereich als vertrauenswürdig einstufen soll.
9. Klicken Sie auf **OK**.

   Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 401) und erstellt für sie kritische Ereignisse.
10. Wählen Sie die Registerkarte **Marker für Datei-Operationen einstellen** aus.
11. Gehen Sie wie folgt vor, um bei Bedarf mehrere Datei-Operations-Marker auszuwählen:

a. Wählen Sie die Option **Dateioperationen anhand der folgenden Marker erkennen** aus.

b. Aktivieren Sie in der Liste der verfügbaren Dateioperationen (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 401) die Kontrollkästchen aller Operationen, die Sie überwachen möchten.

> Standardmäßig überwacht Kaspersky Embedded Systems Security alle verfügbaren Dateioperationen, wenn die Option **Dateioperationen anhand von allen identifizierbaren Markern erkennen** ausgewählt ist.

12. Wenn Sie möchten, dass Kaspersky Embedded Systems Security die Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:

    a. Aktivieren Sie im Abschnitt **Berechnung der Prüfsumme** das Kontrollkästchen **Prüfsumme der geänderten Datei berechnen, wenn möglich**.

       Wenn das Kontrollkästchen aktiviert ist, ermittelt Kaspersky Embedded Systems Security die Prüfsumme der geänderten Datei, in der eine Dateioperation gefunden wurde, die mindestens einem Datei-Operations-Marker entspricht.

       Wenn die Dateioperation anhand mehrerer Marker gleichzeitig gefunden wird, so wird nur die endgültige Prüfsumme der Datei nach allen Änderungen ermittelt.

       Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security keine Prüfsumme für geänderte 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.

    b. Wählen Sie in der Dropdown-Liste **Prüfsumme anhand von Algorithmus berechnen** eine der folgenden Optionen aus:

       - **MD5-Hash**.
       - **SHA256-Hash**.

13. Gehen Sie wie folgt vor, um bei Bedarf Ausnahmen für den Überwachungsbereich hinzuzufügen:

    a. Wählen Sie die Registerkarte **Eingestellte Ausnahmen** aus.

    b. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene Überwachungsbereiche berücksichtigen**.

       Das Kontrollkästchen aktiviert oder deaktiviert die Anwendung von Ausnahmen für Ordner, in denen keine Dateioperationen überwacht werden müssen.

       Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität die Überwachungsbereiche, die zur Liste mit Ausnahmen hinzugefügt wurden.

       Wenn das Kontrollkästchen deaktiviert ist, protokolliert Kaspersky Embedded Systems Security Ereignisse für alle angegebenen Überwachungsbereiche.

       Standardmäßig ist das Kontrollkästchen deaktiviert und die Ausnahmeliste leer.

    c. Klicken Sie auf die Schaltfläche **Durchsuchen**.

       Das Microsoft-Windows-Standardfenster **Ordner suchen** wird geöffnet.

d. Wählen Sie im geöffneten Fenster den Ordner aus, den Sie aus dem Überwachungsbereich ausschließen möchten.

e. Klicken Sie auf **OK**.

f. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Der angegebene Ordner wird zur Liste der ausgeschlossenen Bereiche hinzugefügt.

> Sie können Ausnahmen für Überwachungsbereiche auch manuell hinzufügen, indem Sie die gleichen Masken verwenden wie für die Angabe des Überwachungsbereichs.

14. Klicken Sie auf die Schaltfläche **Speichern**, um die neue Konfigurationsdatei der Regel zu übernehmen.

Protokollanalyse

Dieser Abschnitt enthält Informationen über die Aufgabe zur Protokollanalyse und die Aufgabeneinstellungen.

In diesem Kapitel

Über die Aufgabe Protokollanalyse

Während der Ausführung der Aufgabe zur Protokollanalyse überwacht Kaspersky Embedded Systems Security die Integrität der geschützten Umgebung auf Basis der Ergebnisse der Analyse der Windows-Ereignisprotokolle. Das Programm informiert den Administrator, wenn Anzeichen für untypisches Verhalten im System gefunden werden; solche Anzeichen können auf Angriffsversuche auf den Computer hindeuten.

Kaspersky Embedded Systems Security liest die Daten der Windows-Ereignisprotokolle aus und ermittelt Verstöße entsprechend den vom Benutzer festgelegten Regeln oder den Einstellungen der heuristischen Analyse, die von der Aufgabe zur Protokollanalyse verwendet wird.

Vordefinierte Regeln und heuristische Analyse.

Mit der Aufgabe Protokollanalyse können Sie den Status des geschützten Systems überwachen, indem Sie die vordefinierten Regeln anwenden, die auf bestehenden Heuristiken basieren. Die heuristische Analyse ermittelt das Vorhandensein von anomaler Aktivität auf dem geschützten Computer, die ein Merkmal von versuchten Angriffen sein kann. Die Vorlagen für die Ermittlung von anomaler Aktivität finden Sie in den verfügbaren Heuristiken in den vordefinierten Regeleinstellungen.

In der Regelliste sind sieben Heuristiken für die Protokollanalyse verfügbar. Sie können die Verwendung jeder Regel aktivieren und deaktivieren. Sie können vorhandene Regeln nicht löschen und keine neuen Regeln erstellen.

Sie können die auslösenden Kriterien für Regeln, die Ereignisse überwachen, für die folgenden Operationen konfigurieren:

- Verarbeitung von Brute-Force
- Netzwerk-Anmeldungserkennung

In den Einstellungen der Aufgabe können Sie auch Ausnahmen anpassen. Die heuristische Analyse wird nicht ausgelöst, wenn die Anmeldung von einem vertrauenswürdigen Benutzer oder von einer vertrauenswürdigen IP-Adresse durchgeführt wurde.

Kaspersky Embedded Systems Security verwendet keine Heuristiken für die Analyse von Windows-Protokollen, wenn die heuristische Analyse nicht von der Aufgabe verwendet wird. Standardmäßig ist die heuristische Analyse aktiviert.

Beim Anwenden der Regeln protokolliert das Programm ein *Kritisches Ereignis* im Protokoll der Aufgabenausführung der Aufgabe zur Protokollanalyse.

Benutzerdefinierte Regeln der Aufgabe Protokollanalyse

Mithilfe der Einstellungen der Aufgabenregeln können Sie Auslösekriterien für Regeln beim Fund bestimmter Ereignisse im angegebenen Windows-Protokoll angeben und bearbeiten. Standardmäßig enthält die Regelliste der Aufgabe zur Protokollanalyse vier Regeln. Sie können die Verwendung dieser Regeln aktivieren und deaktivieren, Regeln löschen und ihre Einstellungen bearbeiten.

Sie können für jede Regel folgende Auslösekriterien anpassen:

- Liste der IDs der Einträge im Windows-Ereignisprotokoll

  Die Regel wird ausgelöst, sobald ein neuer Eintrag im Windows-Ereignisprotokoll gefunden wird, dessen Parameter die für diese Regel angegebene Ereignis-ID enthalten. Sie können IDs für jede angegebene Regel hinzufügen und löschen.

- Ereignisquelle

  Sie können für jede Regel ein Unterprotokoll des Windows-Ereignisprotokolls festlegen. Das Programm wird nur in diesem Unterprotokoll nach Einträgen mit den angegebenen Ereignis-IDs suchen. Sie können eines der Standard-Unterprotokolle (Programm, Sicherheit oder System) auswählen, oder ein benutzerdefiniertes Unterprotokoll angeben, in dem Sie den Namen im Feld zur Auswahl der Quelle angeben.

  Das Programm prüft nicht, ob das angegebene Unterprotokoll tatsächlich im Windows-Ereignisprotokoll vorhanden ist.

Wenn die Regel ausgelöst wird, protokolliert Kaspersky Embedded Systems Security ein "Kritisches Ereignis" im Protokoll der Aufgabenausführung der Protokollanalyse.

Standardmäßig übernimmt die Aufgabe zur Protokollanalyse benutzerdefinierte Regeln.

Bevor Sie die Aufgabe zur Protokollanalyse starten, vergewissern Sie sich, dass die Systemaudit-Richtlinie korrekt eingerichtet ist. Weitere Informationen finden Sie im Microsoft-Artikel https://technet.microsoft.com/en-us/library/cc952128.aspx.

Standardeinstellungen der Aufgabe "Protokollanalyse"

Die Aufgabe zur Protokollanalyse weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 57. Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Standardwert	Beschreibung
Benutzerdefinierte Regeln zur Protokollanalyse anwenden	Wird verwendet	Sie können die benutzerdefinierten Regeln aktivieren, deaktivieren, hinzufügen oder ändern.
Vordefinierte Regeln zur Protokollanalyse anwenden	Wird verwendet	Sie können die heuristische Analyse zur Erkennung von anomaler Aktivität auf dem geschützten Server aktivieren oder deaktivieren.
Verarbeitung von Brute-Force	10 Anmeldefehler pro 300 Sekunden.	Sie können die Anzahl der Versuche sowie den Zeitraum angeben, in dem die Versuche ausgeführt wurden, die als Auslösekriterien der heuristischen Analyse dienen sollen.
Netzwerkanmeldung	12:00:00 Uhr.	Sie können den Anfang und das Ende der Zeitspanne angeben, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.
Ausnahmen	Wird nicht verwendet.	Sie können Benutzer und IP-Adressen angeben, die keine heuristische Analyse auslösen.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Regeln für die Protokollanalyse über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie Regeln für die Protokollanalyse über das Verwaltungs-Plug-in hinzufügen und konfigurieren.

In diesem Abschnitt

Vordefinierte Aufgabenregeln über das Verwaltungs-Plug-in verwalten

► *Um die vorkonfigurierten Regeln für die Aufgabe zur Protokollanalyse anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Computergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

   Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **System-Diagnose** im Block **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.
5. Wählen Sie die Registerkarte **Vorkonfigurierte Regeln** aus.
6. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die heuristische Analyse zum Erkennen anomaler Aktivität auf dem geschützten Computer.

   Ist dieses Kontrollkästchen nicht aktiviert, ist die heuristische Analyse deaktiviert und Kaspersky Embedded Systems Security verwendet zum Erkennen anomaler Aktivität die vorinstallierten oder benutzerdefinierte Regeln.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Für die Ausführung der Aufgabe muss zumindest eine Regel für die Protokollanalyse ausgewählt sein.
7. Wählen Sie aus der Liste der vorkonfigurierten Regeln jene Regeln aus, die Sie für die Protokollanalyse verwenden möchten:
   - Ein möglicher Versuch, das Kennwort anhand von Brute-Force zu knacken, wurde entdeckt
   - Anzeichen für eine Gefährdung der Windows-Protokolle wurden gefunden
   - Verdächtige Aktivitäten des neu installierten Dienstes wurden gefunden
   - Eine verdächtige Authentifizierung mit eindeutiger Angabe von Anmeldedaten wurde gefunden

- Anzeichen für den Angriff Kerberos forged PAC (MS14-068) wurden gefunden
- Verdächtige Veränderungen in der privilegierten Gruppe Administratoren wurden gefunden
- Verdächtige Aktivitäten während der Anmeldesitzung im Netzwerk wurden gefunden

8. Um die ausgewählten Regeln anzupassen, klicken Sie auf die Schaltfläche **Erweiterte Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

9. Geben Sie im Abschnitt **Verarbeitung von Brute-Force** die Anzahl der Versuche sowie den Zeitraum an, in dem die Versuche ausgeführt wurden, die als Auslösekriterien der heuristischen Analyse dienen sollen.
10. Geben Sie im Abschnitt **Netzwerk-Anmeldungserkennung** den Anfang und das Ende der Zeitspanne an, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.
11. Wählen Sie die Registerkarte **Ausnahmen** aus.
12. Um Benutzer hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Klicken Sie auf die Schaltfläche **Durchsuchen**.
    b. Wählen Sie einen Benutzer aus.
    c. Klicken Sie auf **OK**.

       Der angegebene Benutzer wird zur Liste der vertrauenswürdigen Benutzer hinzugefügt.
13. Um IP-Adressen hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Geben Sie die IP-Adresse ein.
    b. Klicken Sie auf die Schaltfläche **Hinzufügen**.
14. Die angegebene IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.
15. Passen Sie auf der Registerkarte **Aufgabenverwaltung** den Zeitplan für den Aufgabenstart an (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 139).
16. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe zur Protokollanalyse werden gespeichert.

Regeln für die Protokollanalyse über das Verwaltungs-Plug-in hinzufügen

► *Um eine neue benutzerdefinierte Regel für die Protokollanalyse hinzuzufügen und anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "Richtlinie anpassen" auf S. 121).
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster Programmeinstellungen (siehe Abschnitt Lokale Aufgaben im

Fenster Programmeinstellungen von Kaspersky Security Center anpassen auf Seite 126).

> Wenn für ein Gerät eine aktive Richtlinie von Kaspersky Security Center übernommen wird und diese Richtlinie Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster Programmeinstellungen nicht bearbeitet werden.

4. Klicken Sie im Abschnitt **System-Diagnose** im Block **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

5. Deaktivieren oder aktivieren Sie auf der Registerkarte **Benutzerdefinierte Regeln** das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die benutzerdefinierten Regeln für die Protokollanalyse entsprechend den eingestellten Einstellungen der jeweiligen Regel. Sie können Regeln für die Protokollanalyse hinzufügen, entfernen oder anpassen.

   Wenn das Kontrollkästchen deaktiviert ist, können benutzerdefinierte Regeln weder hinzugefügt noch geändert werden. Kaspersky Embedded Systems Security übernimmt die Standard-Regeleinstellungen.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert. Lediglich die Regel "Ein Pop-up-Fenster einer App wurde gefunden" ist aktiv.

> Sie können kontrollieren, ob die vordefinierten Regeln für die Protokollanalyse übernommen werden. Aktivieren Sie die Kontrollkästchen neben den Regeln, die Sie für die Protokollanalyse übernehmen möchten.

6. Um eine neue benutzerdefinierte Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regeln für die Protokollanalyse** wird geöffnet.

7. Geben Sie im Abschnitt **Allgemein** die folgenden Daten der neuen Regel ein:

   - **Regelname**
   - **Quelle**

     Wählen Sie das Protokoll aus, dessen Ereignisse für die Analyse verwendet werden sollen. Die folgenden Arten des Windows-Ereignisprotokolls sind verfügbar:

     - Programm
     - Sicherheit
     - System

     Sie können ein neues benutzerdefiniertes Protokoll hinzufügen, indem Sie den Namen des Protokolls in das Feld **Quelle** eingeben.

8. Geben Sie im Abschnitt **Auslöseeinstellungen** die ID der Einträge an, durch die die Regel ausgelöst wird:

   a. Geben Sie den Zahlenwert der ID ein.

   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Die angegebene Regel-ID wird zur Liste hinzugefügt. Sie können für jede Regel eine unbegrenzte Anzahl von IDs hinzufügen.

   c. Klicken Sie auf **OK**.

   Die Regel für die Protokollanalyse wird zur allgemeinen Regelliste hinzugefügt.

Regeln für die Protokollanalyse über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie Regeln für die Protokollanalyse über die Programmkonsole hinzufügen und konfigurieren.

In diesem Abschnitt

Vordefinierte Aufgabenregeln über die Programmkonsole verwalten

► *Um die Einstellungen der heuristischen Analyse für die Aufgabe zur Protokollanalyse anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Protokollanalyse** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Protokollanalyse** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Wählen Sie die Registerkarte **Vorkonfigurierte Regeln** aus.
5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die heuristische Analyse zum Erkennen anomaler Aktivität auf dem geschützten Computer.

   Ist dieses Kontrollkästchen nicht aktiviert, ist die heuristische Analyse deaktiviert und Kaspersky Embedded Systems Security verwendet zum Erkennen anomaler Aktivität die vorinstallierten oder benutzerdefinierte Regeln.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Für die Ausführung der Aufgabe muss zumindest eine Regel für die Protokollanalyse ausgewählt sein.
6. Wählen Sie aus der Liste der vorkonfigurierten Regeln jene Regeln aus, die Sie für die Protokollanalyse verwenden möchten:
   - Ein möglicher Versuch, das Kennwort anhand von Brute-Force zu knacken, wurde entdeckt
   - Anzeichen für eine Gefährdung der Windows-Protokolle wurden gefunden
   - Verdächtige Aktivitäten des neu installierten Dienstes wurden gefunden
   - Eine verdächtige Authentifizierung mit eindeutiger Angabe von Anmeldedaten wurde gefunden
   - Anzeichen für den Angriff Kerberos forged PAC (MS14-068) wurden gefunden

- Verdächtige Veränderungen in der privilegierten Gruppe Administratoren wurden gefunden
- Verdächtige Aktivitäten während der Anmeldesitzung im Netzwerk wurden gefunden

7. Um die Einstellungen der ausgewählten Regeln anzupassen, klicken Sie auf die Registerkarte **Zusätzlich**.
8. Geben Sie im Abschnitt **Verarbeitung von Brute-Force** die Anzahl der Versuche sowie den Zeitraum an, in dem die Versuche ausgeführt wurden, die als Auslösekriterien der heuristischen Analyse dienen sollen.
9. Geben Sie im Abschnitt **Netzwerkanmeldung** den Anfang und das Ende der Zeitspanne an, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.
10. Wählen Sie die Registerkarte **Ausnahmen** aus.
11. Um Benutzer hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Klicken Sie auf die Schaltfläche **Durchsuchen**.
    b. Wählen Sie einen Benutzer aus.
    c. Klicken Sie auf **OK**.

    Der angegebene Benutzer wird zur Liste der vertrauenswürdigen Benutzer hinzugefügt.
12. Um IP-Adressen hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Geben Sie die IP-Adresse ein.
    b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

    Die angegebene IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.
13. Wählen Sie die Registerkarten **Zeitplan** und **Erweitert** aus, um den Zeitplan für den Aufgabenstart anzupassen.
14. Klicken Sie auf **OK**.

    Die Einstellungen der Aufgabe zur Protokollanalyse werden gespeichert.

Regeln für die Protokollanalyse anpassen

Um eine neue benutzerdefinierte Regel für die Protokollanalyse hinzuzufügen und anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Protokollanalyse** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Protokollanalyse** auf den Link **Regeln für die Protokollanalyse**.

   Das Fenster **Regeln für die Protokollanalyse** wird geöffnet.

4. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die benutzerdefinierten Regeln für die Protokollanalyse entsprechend den eingestellten Einstellungen der jeweiligen Regel. Sie können Regeln für die Protokollanalyse hinzufügen, entfernen oder anpassen.

   Wenn das Kontrollkästchen deaktiviert ist, können benutzerdefinierte Regeln weder hinzugefügt noch geändert werden. Kaspersky Embedded Systems Security übernimmt die Standard-Regeleinstellungen.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert. Lediglich die Regel "Ein Pop-up-Fenster einer App wurde gefunden" ist aktiv.

   Sie können kontrollieren, ob die vordefinierten Regeln für die Protokollanalyse übernommen werden. Aktivieren Sie die Kontrollkästchen neben den Regeln, die Sie für die Protokollanalyse übernehmen möchten.

5. Um eine neue benutzerdefinierte Regel zu erstellen, gehen Sie wie folgt vor:
   a. Geben Sie den Namen der neuen Regel ein.
   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Die erstellte Regel wird zur allgemeinen Regelliste hinzugefügt.
6. Um eine beliebige Regel anzupassen, gehen Sie wie folgt vor:
   a. Wählen Sie die Regel mit der linken Maustaste in der Liste aus.

      Im rechten Bereich des Fensters werden auf der Registerkarte **Beschreibung** allgemeine Informationen über die Regel angezeigt.

      Die Beschreibung für eine neue Regel ist leer.

   b. Wählen Sie die Registerkarte **Regelbeschreibung** aus.
   c. Bearbeiten Sie im Abschnitt **Allgemein** erforderlichenfalls den Namen der Regel.
   d. Wählen Sie die **Quelle**.
7. Geben Sie im Abschnitt **Ereignis-IDs** die IDs der Einträge an, durch die die Regel ausgelöst wird:
   a. Geben Sie den Zahlenwert der ID ein.
   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Die angegebene Regel-ID wird zur Liste hinzugefügt. Sie können für jede Regel eine unbegrenzte Anzahl von IDs hinzufügen.
   c. Klicken Sie auf die Schaltfläche **Speichern**.

      Die festgelegten Einstellungen der Regeln für die Protokollanalyse werden angewendet.

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 Computers.

In diesem Kapitel

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, den Arbeitsspeicher des Computers sowie Autostart-Objekte.

In Kaspersky Embedded Systems Security sind die folgenden Systemaufgaben zur Untersuchung auf Befehl vorgesehen:

- Die Aufgabe Untersuchung beim Hochfahren des Betriebssystems wird jedes Mal ausgeführt, wenn Kaspersky Embedded Systems Security gestartet wird. Kaspersky Embedded Systems Security untersucht die Bootsektoren und Master-Bootsektoren der Festplatten und Wechseldatenträger, sowie den Arbeits- und Prozessspeicher. Jedes Mal, wenn Kaspersky Embedded Systems Security die Aufgabe ausführt, wird eine Kopie der nicht infizierten Bootsektoren erstellt. Wird beim nächsten Start eine Bedrohung in dieses Sektoren gefunden, werden sie durch die Backup-Kopie ersetzt.
- 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, Arbeitsspeicher und Prozess-Speicher. Das Programm untersucht Dateien, die sich in Systemordnern befinden, z.B. im Ordner %windir%\system32. Kaspersky Embedded Systems Security verwendet die Sicherheitseinstellungen, deren Werte der Sicherheitsstufe Empfohlen entsprechen (siehe Abschnitt "Über vordefinierte Sicherheitsstufen für Aufgaben zur Untersuchung auf Befehl" auf Seite 429). Sie können die Parameter für die Aufgabe Untersuchung wichtiger Bereiche ändern.

- Die Aufgabe Untersuchung von Quarantäne-Objekten wird standardmäßig jedes Mal nach dem Datenbanken-Update nach Zeitplan ausgeführt. Sie können den Umfang der Aufgabe "Untersuchung von Quarantäne-Objekten" nicht ändern.
- Die Aufgabe "Integritätsprüfung für Programme" 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 Statistik über die Aufgabenausführung enthält Angaben über die Anzahl der untersuchten und beschädigten 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.

Zusätzlich können Sie benutzerdefinierte Aufgaben zur Untersuchung auf Befehl erstellen, beispielsweise eine Aufgabe zur Untersuchung freigegebener Ordner auf dem Computer.

Kaspersky Embedded Systems Security kann gleichzeitig mehrere Aufgaben zur Untersuchung auf Befehl ausführen.

Über den Untersuchungsbereich

Sie können den Untersuchungsbereich für die Aufgaben Untersuchung beim Hochfahren des Betriebssystems und Untersuchung wichtiger Bereiche konfigurieren sowie auch für benutzerdefinierte Aufgaben zur Untersuchung auf Befehl.

Standardmäßig überprüfen die Aufgaben zur Untersuchung auf Befehl alle Objekte im Dateisystem des Computers. Verlangen die Sicherheitsanforderungen keine Untersuchung aller Objekte des Dateisystems, so können Sie den Untersuchungsbereich begrenzen.

In der Programmkonsole wird der Untersuchungsbereich als Struktur oder Liste jener Dateiressourcen des Computers dargestellt, die von Kaspersky Embedded Systems Security überwacht werden können. Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Computers als Liste angezeigt.

► *Um die Anzeige der freigegebenen Netzwerkordner des Computers als Struktur zu aktivieren,*

Wählen Sie im linken unteren Teil des Einstellungsfensters Untersuchungsbereich aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.

Die Knoten der Dateistruktur oder Liste der Dateiressourcen des Computers werden auf folgende Weise dargestellt:

☑ Der Knoten gehört zum Untersuchungsbereich.

☐ Der Knoten gehört nicht zum Untersuchungsbereich.

☑ Mindestens ein diesem Knoten untergeordneter Knoten gehört nicht zum Untersuchungsbereich oder die Sicherheitseinstellungen des oder der untergeordneten Knoten unterscheiden sich von den Sicherheitseinstellungen dieses Knotens (nur für die Baumstruktur-Ansicht).

Das Symbol ☑ wird angezeigt, wenn alle untergeordneten Knoten ausgewählt sind, nicht jedoch der übergeordnete Knoten. In diesem Fall werden Änderungen der Datei- und Ordnerzusammensetzung des übergeordneten Knotens bei der Änderung eines Untersuchungsbereichs für den ausgewählten untergeordneten Knoten nicht automatisch berücksichtigt.

Die Namen von virtuellen Knoten eines Untersuchungsbereichs werden mit blauer Schrift angezeigt.

Vordefinierte Untersuchungsbereiche

Die Liste oder Dateistruktur des Computers wird der ausgewählten Aufgabe zur Untersuchung auf Befehl wird auf der Registerkarte **Untersuchungsbereich - Einstellungen** angezeigt.

Die Dateistruktur oder Liste der Dateiressourcen des Computers enthält die Knoten, für die Sie nach den Sicherheitseinstellungen in Microsoft Windows über Leserechte verfügen.

Kaspersky Embedded Systems Security enthält die folgenden vordefinierten Untersuchungsbereiche:

- Arbeitsplatz. Kaspersky Embedded Systems Security untersucht den gesamten Computer.
- Lokale Festplatten. Kaspersky Embedded Systems Security untersucht Objekte auf den Festplatten des Computers. Sie können alle Festplatten sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.
- Wechseldatenträger. Kaspersky Embedded Systems Security untersucht Dateien auf externen Geräten, z. B. auf CDs oder USB-Laufwerken. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.
- Netzwerkumgebung. 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 ebenfalls nicht in der Dateiressourcenstruktur des Computers angezeigt. Um Objekte auf einem Netzlaufwerk in den Untersuchungsbereich aufzunehmen, geben Sie den Pfad des Ordners an, der diesem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

- Systemspeicher. Kaspersky Embedded Systems Security untersucht ausführbare Dateien und Module von Prozessen, die während der Untersuchung im Betriebssystem ausgeführt werden.
- 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 Computers automatisch gestartet werden.
- Freigegebene Ordner. Sie können die freigegebenen Ordner auf dem geschützten Computer in den Untersuchungsbereich einschließen.
- Virtuelle Festplatten. Sie können in den Untersuchungsbereich dynamische Laufwerke, Ordner und Dateien sowie Laufwerke aufnehmen, die auf dem Computer eingebunden werden, z. B. gemeinsame Cluster-Laufwerke.

  Virtuelle Festplatten, die mit dem Befehl SUBST erzeugt wurden, werden nicht in der Struktur der Computerdateiressourcen in der Programmkonsole angezeigt. Um Objekte auf einer virtuellen Festplatte zu untersuchen, nehmen Sie den Ordner auf dem Computer, mit dem diese virtuelle Festplatte verbunden ist, in den Untersuchungsbereich auf.

Die vordefinierten Untersuchungsbereiche werden standardmäßig in der Struktur der freigegebenen Netzwerkordner des Computers angezeigt und sind zum Hinzufügen in die Liste der Dateiressourcen bei ihrer Erstellung in den Einstellungen des Untersuchungsbereichs verfügbar.

Standardmäßig werden die Aufgaben zur Untersuchung auf Befehl in den folgenden Bereichen ausgeführt:

- Aufgabe Untersuchung beim Hochfahren des Betriebssystems
  - Lokale Festplatten
  - Wechseldatenträger
  - Systemspeicher
- Untersuchung wichtiger Bereiche:
  - Lokale Festplatten (mit Ausnahme der Windows-Ordner)
  - Wechseldatenträger
  - Systemspeicher
  - Autostart-Objekte
- Andere Aufgaben:
  - Lokale Festplatten (mit Ausnahme der Windows-Ordner)
  - Wechseldatenträger
  - Systemspeicher
  - Autostart-Objekte
  - Freigegebene Ordner

Untersuchung von Dateien im Cloud-Speicher

Über Cloud-Dateien

Kaspersky Embedded Systems Security kann mit Dateien in der Microsoft OneDrive Cloud interagieren. Das Programm unterstützt die neue "OneDrive Files On-Demand"-Funktion.

Kaspersky Embedded Systems Security unterstützt keine anderen Cloud-Speicher.

OneDrive Files On-Demand ermöglicht Ihnen den Zugriff auf all Ihre Dateien in OneDrive, 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 Computer gespeichert sind. Solche OneDrive-Dateien besitzen den Status und . Die Dateien mit dem Status werden bei der Untersuchung übersprungen, da sie sich nicht physisch auf dem geschützten Computer 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. Die Datei wird untersucht, wenn der Benutzer darauf zugreift. Wenn der Benutzer auf eine Datei mit dem Status zugreift, wird sie heruntergeladen und lokal verfügbar gemacht und ihr Status wechselt zu . So kann die Datei von der Aufgabe "Echtzeitschutz für Dateien" verarbeitet werden.
- Untersuchung von Cloud-Dateien auf Befehl: Sie können Ordner mit Cloud-Dateien zum Untersuchungsbereich der Aufgabe "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.
- Erstellung und Verwendung der Regeln für die Programmkontrolle: Sie können für Dateien mit dem Status und mithilfe der Aufgabe zum automatischen Erstellen von Regeln für die Kontrolle des Programmstarts Erlaubnisregeln und Verbotsregeln erstellen. Die Aufgabe zur Kontrolle des Programmstarts wendet das Prinzip des standardmäßigen Verbots (Default Deny) an und erstellt Regeln zum Verarbeiten und Blockieren von Cloud-Dateien.

  Die Aufgabe zur 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 einer 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.

Sicherheitseinstellungen für den ausgewählten Knoten in den Aufgaben zur Untersuchung auf Befehl

In der ausgewählten Aufgabe zur Untersuchung auf Befehl können Sie die Werte der standardmäßigen Sicherheitseinstellungen ändern. Dabei können Sie entweder einheitliche Werte für den gesamten Schutzbereich bzw. Untersuchungsbereich oder individuelle Werte für bestimmte Knoten oder Elemente der Struktur oder Liste der Ressourcen des Computers festlegen.

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 Maximale Sicherheit).
- Durch manuelle Änderung der Sicherheitseinstellungen für die ausgewählten Knoten oder Elemente in der Struktur oder Liste der Dateiressourcen des Computers (die Sicherheitsstufe nimmt den Wert Benutzerdefiniert an).

Sie können den Parametersatz eines Knotens in einer Vorlage speichern, um diese Vorlage später für andere Knoten zu übernehmen.

Über vordefinierte Sicherheitsstufen für Aufgaben zur Untersuchung auf Befehl

Die Sicherheitseinstellungen iChecker-Technologie verwenden, iSwift-Technologie verwenden, Heuristische Analyse verwenden und Dateien auf Microsoft-Signatur überprüfen gehören nicht zu den Einstellungen der vordefinierten Sicherheitsstufen. Wenn Sie den Status der Einstellungen iChecker-Technologie verwenden, iSwift-Technologie verwenden, Heuristische Analyse verwenden und Dateien auf Microsoft-Signatur überprüfen ändern, ändert sich die von Ihnen gewählte vordefinierte Sicherheitsstufe nicht.

Für den ausgewählten Knoten in der Struktur der Dateiressourcen des Computers können Sie eine von drei vordefinierten Sicherheitsstufen festlegen: Maximale Leistung, Empfohlen und Maximale Sicherheit. Jede dieser Stufen besitzt eine eigene Auswahl von Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe Maximale Leistung wird empfohlen, wenn es zusätzlich zur Verwendung von Kaspersky Embedded Systems Security auf Computern noch weitere Sicherheitsmaßnahmen innerhalb Ihres Netzwerks gibt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien.

Empfohlen

Die Sicherheitsstufe Empfohlen bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Computer. Diese Stufe ist laut Empfehlung der Experten von Kaspersky Lab für den Schutz von Computern in den meisten Unternehmensnetzwerken ausreichend. Die Sicherheitsstufe Empfohlen gilt als Standard.

Maximale Sicherheit

Die Sicherheitsstufe Maximale Sicherheit wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Computersicherheit hat.

Tabelle 58. Vordefinierte Sicherheitsstufen und entsprechende Werte für die Sicherheitsparameter

Einstellungen	Sicherheitsstufe		
	Maximale Leistung	Empfohlen	Maximale Sicherheit
Objekte untersuchen	Nach Format	Alle Objekte	Alle Objekte
Nur neue und veränderte Dateien untersuchen	Aktiviert	Deaktiviert	Deaktiviert
Aktion für infizierte und andere Objekte	Desinfizieren. Irreparable Objekte löschen	Empfohlene Aktion ausführen (Desinfizieren. Irreparable Objekte löschen)	Desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte	In Quarantäne verschieben	Empfohlene Aktion ausführen (In Quarantäne verschieben)	In Quarantäne verschieben
Dateien ausschließen	Nein	Nein	Nein
Nicht erkennen	Nein	Nein	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	60 Sek.	Nein	Nein
Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	8 MB	Nein	Nein
Alternative NTFS-Ströme	Ja	Ja	Ja
Bootsektoren und MBR	Ja	Ja	Ja

Einstellungen	Sicherheitsstufe		
Zusammengesetzte Objekte untersuchen	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Nur neue und veränderte	• Archive* • SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Alle Objekte	• Archive* • SFX-Archive* • E-Mail-Datenbanken* • Dateien in Mail-Formaten* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Alle Objekte

Über die Untersuchung von Wechseldatenträgern

Sie können die Untersuchung von Wechseldatenträgern anpassen, die über USB an den geschützten Computer angeschlossen werden.

Kaspersky Embedded Systems Security führt die Untersuchung von Wechseldatenträgern mithilfe der Aufgabe Untersuchung auf Befehl aus. Das Programm erstellt automatisch eine neue Aufgabe zur Untersuchung auf Befehl, wenn ein Wechseldatenträger angeschlossen wird, und löscht die erstellte Aufgabe nach Abschluss der Untersuchung. Die erstellte Aufgabe wird mit der vordefinierten Sicherheitsstufe ausgeführt, die für die Untersuchung von Wechseldatenträgern festgelegt wurde. Sie können die Einstellungen der vorübergehenden Aufgabe zur Untersuchung auf Befehl nicht anpassen.

Wenn Sie Kaspersky Embedded Systems Security ohne Antiviren-Datenbanken installiert haben, ist die Untersuchung von Wechseldatenträgern nicht verfügbar.

Kaspersky Embedded Systems Security führt die Untersuchung von Wechseldatenträgern mithilfe der Aufgabe Untersuchung auf Befehl aus. Das Programm erstellt automatisch eine neue Aufgabe zur Untersuchung auf Befehl, wenn ein Wechseldatenträger angeschlossen wird, und löscht die erstellte Aufgabe nach Abschluss der Untersuchung. Die erstellte Aufgabe wird mit der vordefinierten Sicherheitsstufe ausgeführt, die für die Untersuchung von Wechseldatenträgern festgelegt wurde. Sie können die Einstellungen der vorübergehenden Aufgabe zur Untersuchung auf Befehl nicht anpassen.

Kaspersky Embedded Systems Security startet die Untersuchung von über USB angeschlossenen Wechseldatenträgern, wenn diese sich im Betriebssystem als Massenspeichergeräte (USB Mass Storage Device) registrieren. Das Programm führt keine Untersuchung des Wechseldatenträgers durch, wenn sein Anschluss von der Aufgabe zur Gerätekontrolle blockiert wird. Das Programm führt keine Untersuchung von MTP-Mobilgeräten durch.

Kaspersky Embedded Systems Security erlaubt den Zugriff auf Wechseldatenträger während der Untersuchung.

Die Ergebnisse der Untersuchung jedes Wechseldatenträgers werden im Protokoll der Aufgabe "Untersuchung auf Befehl" gespeichert, die beim Anschließen des jeweiligen Datenträgers erstellt wurde.

Sie können die Einstellungswerte der Komponente Wechseldatenträger untersuchen bearbeiten (s. Tabelle unten).

Tabelle 59. Einstellungen der Untersuchung von Wechseldatenträgern

Einstellung	Standardwert	Beschreibung
Wechseldatenträger beim Anschließen über USB untersuchen	Kontrollkästchen ist deaktiviert	Sie können die Untersuchung von Wechseldatenträgern bei ihrem Anschluss über USB an den geschützten Computer aktivieren und deaktivieren.
Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)	1024 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.
Untersuchung starten 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: • Maximale Sicherheit • Empfohlen • Maximale Leistung 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. Systemaufgaben und benutzerdefinierte Aufgaben zur Untersuchung auf Befehl lassen sich konfigurieren.

Tabelle 60. Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl

Einstellung	Bedeutung	Beschreibung
Untersuchungsbereich	Wird in den folgenden Systemaufgaben und benutzerdefinierten Aufgaben verwendet: • Untersuchung beim Hochfahren des Betriebssystems: gesamter Server mit Ausnahme der freigegebenen Ordner und der Objekte des Autostarts • Untersuchung wichtiger Bereiche: gesamter Server mit Ausnahme der freigegebenen Ordner und einiger Dateien des Betriebssystems • Benutzerdefinierte Aufgabe zur Untersuchung auf Befehl: gesamter Server	Sie können den Untersuchungsbereich ändern. Der Untersuchungsbereich für die Systemaufgaben zur Untersuchung von Quarantäne-Objekten und Integritätsprüfung für Programme kann nicht konfiguriert werden.
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, entspricht der Sicherheitsstufe Empfohlen.	Sie können für die ausgewählten Knoten in der Struktur oder Liste der Dateiressourcen des Computers folgende Aktionen ausführen: • eine andere vordefinierte Sicherheitsstufe auswählen • Sicherheitseinstellungen manuell ändern. Sie können die Parameter für Sicherheit des ausgewählten Knotens in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen.
Heuristische Analyse verwenden	Für die Aufgaben Untersuchung wichtiger Bereiche und Untersuchung beim Hochfahren des Betriebssystems sowie für benutzerdefinierte Untersuchungsaufgaben wird die Analysestufe Mittel verwendet. Für die Aufgabe Untersuchung von Quarantäne-Objekten wird die Analysestufe Tief verwendet.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen. Sie können die Analysestufe für die Aufgabe Untersuchung von Quarantäne-Objekten nicht ändern. Die Verwendung der heuristischen Analyse in der Aufgabe Integritätsprüfung für Programme ist nicht vorgesehen.

Einstellung	Bedeutung	Beschreibung
Vertrauenswürdige Zone anwenden	Übernommen (Nicht übernommen für Aufgabe zur Untersuchung von Quarantäne-Objekten)	Einheitliche Liste mit Ausnahmen, die Sie in bestimmten Aufgaben verwenden können.
KSN zur Überprüfung verwenden	Wird verwendet	Sie können Ihren Server durch die Nutzung der Cloud-Dienste von Kaspersky Security Network effektiver schützen.
Einstellungen für den Aufgabenstart mit Rechten	Die Aufgabe wird mit den Rechten des Systemkontos gestartet.	Sie können die Einstellungen für den Start mit den Rechten von Benutzerkonten für alle Systemaufgaben und benutzerdefinierten Aufgaben für die Untersuchung auf Befehl ändern, mit Ausnahme der Aufgaben Untersuchung von Quarantäne-Objekten und Integritätsprüfung für Programme.
Aufgabe im Hintergrundmodus ausführen (geringe Priorität)	Wird nicht verwendet	Sie können die Priorität der Aufgaben für die Untersuchung auf Befehl festlegen.
Zeitplan für den Aufgabenstart	Wird in den folgenden Systemaufgaben verwendet: • Untersuchung beim Hochfahren des Betriebssystems – Bei Programmstart • Untersuchung wichtiger Bereiche – Wöchentlich • Untersuchung von Quarantäne-Objekten – Nach dem Update der Programm-Datenbanken. • Integritätsprüfung für Programme – Täglich Wird in neu erstellten benutzerdefinierten Aufgaben nicht verwendet.	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Registrierung der Ausführung der Untersuchung und Aktualisierung des Schutzstatus des Servers	Der Schutzstatus des Servers wird wöchentlich nach Ausführung der Aufgabe Untersuchung wichtiger Bereiche aktualisiert.	Sie können die Einstellungen für die Registrierung der Aufgabe zur Untersuchung wichtiger Bereiche folgendermaßen konfigurieren: • durch Änderung der Einstellungen im Zeitplan für den Aufgabenstart der Aufgabe Untersuchung wichtiger Bereiche • durch Änderung des Untersuchungsbereichs der Aufgabe zur Untersuchung wichtiger Bereiche • durch Erstellung von benutzerdefinierten Aufgaben für die Untersuchung auf Befehl

Aufgaben zur Untersuchung auf Befehl über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Aufgabeneinstellungen für einen oder alle Computer im Netzwerk konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen

► *Um eine neue benutzerdefinierte Aufgabe zur Untersuchung auf Befehl zu erstellen, gehen Sie wie folgt vor:*

1. Für das Erstellen einer lokalen Aufgabe:
   a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Verwaltungskonsole von Kaspersky Security Center.
   b. Wählen Sie die Administrationsgruppe aus, zu der der Computer gehört.
   c. Öffnen Sie im Ergebnisbereich auf der Registerkarte **Geräte** das Kontextmenü des geschützten Servers.
   d. Wählen Sie den Punkt **Eigenschaften** aus.
   e. Klicken Sie im nächsten Fenster auf die Schaltfläche **Hinzufügen** im Abschnitt **Aufgaben**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.

2. Für das Erstellen einer Gruppenaufgabe:
   a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
   b. Wählen Sie die Administrationsgruppe aus, für die Sie eine Aufgabe erstellen möchten.
   c. Öffnen Sie die Registerkarte **Aufgaben**.
   d. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.
3. Um eine Aufgabe für eine benutzerdefinierte Auswahl von Computern zu erstellen, gehen Sie wie folgt vor:
   a. Klicken Sie im Knoten **Geräteauswahlen** in der Verwaltungskonsole von Kaspersky Security Center auf die Schaltfläche **Auswahl ausführen**, um eine Geräteauswahl durchzuführen.
   b. Öffnen Sie die Registerkarte **Auswahlergebnisse "Auswahlname"**.
   c. Wählen Sie in der Dropdown-Liste **Auswahl durchführen** die Option **Aufgabe für ein Auswahlergebnis erstellen**aus.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.
4. Wählen Sie die Aufgabe Untersuchung auf Befehl aus der Liste der für Kaspersky Embedded Systems Security verfügbaren Aufgaben aus.
5. Klicken Sie auf **Weiter**.

   Das Fenster Einstellungen wird geöffnet.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

► *Um eine bestehende Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:*

Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben von Kaspersky Security Center.

Das Fenster **Eigenschaften: Untersuchung auf Befehl** wird geöffnet.

Aufgabeneigenschaften für die Untersuchung auf Befehl öffnen

► *Um die Programmeinstellungen für die Aufgabe zur Untersuchung auf Befehl für einen einzelnen Computer zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, zu der der geschützte Computer gehört.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Doppelklicken Sie auf den Namen des Computers, für den Sie den Untersuchungsbereich anpassen möchten.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
5. Wählen Sie den Abschnitt **Aufgaben** aus.
6. Wählen Sie in der Liste der für das Gerät erstellten Aufgaben die Aufgabe zur Untersuchung auf Befehl aus, die Sie erstellt haben.
7. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Eigenschaften: Untersuchung auf Befehl** wird geöffnet.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

Erstellen einer Aufgabe zur Untersuchung auf Befehl

► *Um eine benutzerdefinierte Aufgabe zur Untersuchung auf Befehl zu erstellen, gehen Sie wie folgt vor:*

1. Öffnen Sie die Einstellungen (siehe Abschnitt "**Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen**" auf Seite 435) im **Assistenten für neue Aufgabe**.
2. Wählen Sie die gewünschte Aufgabenerstellungsmethode aus.
3. Klicken Sie auf **Weiter**.
4. Erstellen Sie im Fenster Untersuchungsbereich einen Untersuchungsbereich:

   Standardmäßig gehören zum Untersuchungsbereich wichtige Bereiche des Computers. 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 alle wichtigen Untersuchungsbereiche von der Untersuchung auszuschließen, öffnen Sie nacheinander für jede einzelne Zeile das Kontextmenü und wählen Sie Bereich 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 mit der rechten Maustaste auf die Tabelle Untersuchungsbereich und wählen Sie Bereich hinzufügen oder klicken Sie auf die Schaltfläche Hinzufügen.
     b. Wählen Sie im Fenster Zum Untersuchungsbereich hinzufügen entweder einen vordefinierten Bereich aus der Liste Vordefinierter Bereich aus oder geben Sie eine Festplatte des Computers, einen Ordner, ein Netzwerkobjekt oder eine Datei auf dem Computer oder auf einem anderen Computer im Netzwerk an und klicken Sie dann auf OK.
   - Um Unterordner oder Dateien von der Untersuchung auszuschließen, wählen Sie den hinzugefügten Ordner (das hinzugefügte Laufwerk) im Fenster Untersuchungsbereich des Assistenten aus:
     a. Öffnen Sie das Kontextmenü und wählen Sie die Option Anpassen.
     b. Klicken Sie auf die Schaltfläche Einstellungen im Fenster Sicherheitsstufe.
     c. Deaktivieren Sie auf der Registerkarte Allgemein im Fenster Untersuchung auf Befehl die Kontrollkästchen Untergeordnete Ordner und Untergeordnete Dateien.
   - Um die Sicherheitseinstellungen des Untersuchungsbereichs zu ändern, gehen Sie wie folgt vor:
     a. Öffnen Sie das Kontextmenü für den Bereich, dessen Einstellungen Sie ändern wollen, und wählen Sie Anpassen.
     b. Wählen Sie im Fenster Untersuchung auf Befehl eine der vordefinierten Sicherheitsstufen aus oder klicken Sie auf die Schaltfläche Einstellungen, um die Sicherheitseinstellungen manuell anzupassen.

Die Sicherheitseinstellungen werden auf die gleiche Weise wie bei der Aufgabe Echtzeitschutz für Dateien konfiguriert (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 265).

- Um eingebettete Objekte in hinzugefügten Untersuchungsbereich zu überspringen, gehen Sie wie folgt vor:

  a. Öffnen Sie das Kontextmenü für die Tabelle Untersuchungsbereich und wählen Sie Ausnahme hinzufügen.

  b. Geben Sie die Objekte an, die ausgeschlossen werden sollen: Wählen Sie den vordefinierten Gültigkeitsbereich in der Liste Vordefinierter Bereich aus, geben Sie das Computerlaufwerk, den Ordner, das Netzwerkobjekt bzw. die Datei auf dem Computer oder einem anderen Computer im Netzwerk an.

  c. Klicken Sie auf OK.

5. Passen Sie im Fenster Einstellungen die heuristische Analyse und Integration mit anderen Komponenten an:.

- Passen Sie die Verwendung der heuristischen Analyse an (siehe Abschnitt "Heuristische Analyse und Integration mit anderen Programmkomponenten" auf Seite 261).
- Aktivieren Sie das Kontrollkästchen Vertrauenswürdige Zone anwenden, wenn Sie Objekte, die zur Liste der vertrauenswürdigen Zonen hinzugefügt wurden, vom Untersuchungsbereich der Aufgabe ausschließen möchten.

  Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

  Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

  Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs für die Aufgabe.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Aktivieren Sie das Kontrollkästchen KSN zur Überprüfung verwenden, wenn Sie die Cloud-Dienste von Kaspersky Security Network für die Aufgabe nutzen möchten.

  Mithilfe dieses Kontrollkästchens wird die Verwendung der Cloud-Dienste von Kaspersky Security Network (KSN) in der Aufgabe aktiviert bzw. deaktiviert.

  Ist das Kontrollkästchen aktiviert, so verwendet das Programm die von den KSN-Diensten übermittelten Daten, was eine schnellere Reaktion des Programms auf neue Bedrohungen gewährleistet und die Wahrscheinlichkeit von Fehlalarmen verringert.

  Ist das Kontrollkästchen deaktiviert, werden die KSN-Dienste von der Aufgabe zur Untersuchung auf Befehl nicht verwendet.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Basispriorität *Niedrig* zuzuweisen, aktivieren Sie im Fenster Einstellungen das Kontrollkästchen Aufgabe im Hintergrundmodus ausführen.

Dieses Kontrollkästchen ändert die Priorität der Aufgabe.

Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabenpriorität im Betriebssystem gesenkt. Das Betriebssystem stellt Ressourcen zur Verfügung, um die Aufgabe in Abhängigkeit von der Belastung der CPU und des Dateisystems des Computers durch andere Aufgaben von Kaspersky Embedded Systems Security und Programme auszuführen. Die Aufgabe wird daher bei einer Erhöhung der Belastung langsamer und bei einer Reduzierung der Belastung schneller ausgeführt.

Wenn dieses Kontrollkästchen deaktiviert ist, wird die Aufgabe mit derselben Priorität ausgeführt wie die übrigen Aufgaben von Kaspersky Embedded Systems Security und die anderen Programme. In diesem Fall wird die Aufgabe schneller ausgeführt.

Das Kontrollkästchen ist standardmäßig deaktiviert.

Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

- Um die erstellte Aufgabe als Untersuchung wichtiger Bereiche zu verwenden, aktivieren Sie im Fenster Einstellungen das Kontrollkästchen Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten.

  Dieses Kontrollkästchen ändert die Priorität einer Aufgabe: Es aktiviert oder deaktiviert das Protokollieren des Ereignisses *Untersuchung wichtiger Bereiche* und das Update des Schutzstatus des Computers. Kaspersky Security Center überprüft die Sicherheitsstufe des Computers (der Computer) mithilfe der Leistungsergebnisse von Aufgaben mit dem Status *Untersuchung wichtiger Bereiche*. In den Eigenschaften von lokalen System- und benutzerdefinierten Aufgaben von Kaspersky Embedded Systems Security ist das Kontrollkästchen nicht verfügbar. Sie können den Wert dieser Einstellung nur auf Seiten von Kaspersky Security Center ändern.

  Wenn dieses Kontrollkästchen aktiviert ist, protokolliert der Administrationsserver den Abschluss der Untersuchung wichtiger Bereiche und aktualisiert den Schutzstatus des Computers anhand der Ergebnisse der Aufgabenausführung. Die Untersuchungsaufgabe hat eine hohe Priorität.

  Ist das Kontrollkästchen deaktiviert, so wird die Untersuchungsaufgabe mit niedriger Priorität ausgeführt.

  Das Kontrollkästchen ist für benutzerdefinierte Aufgaben zur Untersuchung auf Befehl standardmäßig deaktiviert.

6. Klicken Sie auf **Weiter**.
7. Legen Sie im Fenster Zeitplan die Einstellungen für den Zeitplan für den Aufgabenstart fest.
8. Klicken Sie auf **Weiter**.
9. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, das Sie verwenden möchten.
10. Klicken Sie auf **Weiter**.
11. Geben Sie einen Aufgabennamen an.

12. Klicken Sie auf **Weiter**.

    Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

    Daraufhin wird das Fenster **Erstellung der Aufgabe abschließen** geöffnet.

13. Sie können die Aufgabe optional ausführen, nachdem der Assistent abgeschlossen wurde, indem Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** aktivieren.

14. Klicken Sie auf Fertig stellen, um die Erstellung der Aufgabe fertig zu stellen.

Die neue Aufgabe zur Untersuchung auf Befehl wird für einen ausgewählten Computer oder eine Computergruppe erstellt.

In diesem Abschnitt

Zuweisen des Status "Aufgabe zur Untersuchung wichtiger Bereiche" an eine Aufgabe zur Untersuchung auf Befehl

Standardmäßig weist Kaspersky Security Center einem Computer den Status *Warnung* zu, wenn die Aufgabe "Untersuchung wichtiger Bereiche" seltener ausgeführt wird als durch die Einstellung Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt von Kaspersky Embedded Systems Security angegeben ist.

► *Gehen Sie folgendermaßen vor, um die Untersuchung aller Computer anzupassen, die zu einer Administrationsgruppe gehören:*

1. Erstellen Sie eine Gruppenaufgabe zur Untersuchung auf Befehl (siehe Abschnitt "Erstellen einer Aufgabe zur Untersuchung auf Befehl" auf Seite 437)
2. Aktivieren Sie im Fenster Einstellungen des Assistenten für die Aufgabenerstellung das Kontrollkästchen Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten. Die von Ihnen angegebenen Aufgabeneinstellungen (der Untersuchungsbereich und die Sicherheitseinstellungen) werden für alle Computer der Gruppe übernommen. Stellen Sie den Aufgabenzeitplan ein.

   Sie können das Kontrollkästchen Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten aktivieren, wenn Sie die Aufgabe zur Untersuchung auf Befehl für eine Gruppe von Computern erstellen, oder später im Fenster **Eigenschaften: <Aufgabenname>** (siehe Abschnitt "Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen" auf Seite 436).

3. Deaktivieren Sie mithilfe einer neuen oder vorhandenen Richtlinie die geplanten Starts der Systemaufgaben zur Untersuchung auf Befehl (siehe Abschnitt "Zeitplan für den Start von lokalen Systemaufgaben anpassen" auf Seite 103) auf den Computern der Gruppe.

Von diesem Zeitpunkt an berücksichtigt der Kaspersky Security Center-Administrationsserver bei der Bewertung des Sicherheitszustands des geschützten Computers und bei der Benachrichtigung darüber die Ergebnisse der letzten Ausführung der Aufgabe mit dem Status *Untersuchung wichtiger Bereiche*, und nicht die Ausführungsergebnisse der Systemaufgabe Untersuchung wichtiger Bereiche.

Sie können den Status *Aufgabe zur Untersuchung wichtiger Bereiche* nicht nur Gruppenaufgaben, sondern auch Aufgaben für Zusammenstellungen von Computern zur Untersuchung auf Befehl zuweisen.

In der Programmkonsole können Sie überprüfen, ob eine Aufgabe zur Untersuchung auf Befehl als Aufgabe zur Untersuchung wichtiger Bereiche betrachtet wird.

In der Programmkonsole wird das Kontrollkästchen Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten in den Aufgabeneigenschaften nur angezeigt und kann nicht geändert werden.

Ausführung einer Aufgabe zur Untersuchung auf Befehl im Hintergrundmodus

Prozesse, in denen Aufgaben von Kaspersky Embedded Systems Security ausgeführt werden, besitzen die Basispriorität *Mittel* (Normal).

Sie können einem Prozess, in dem eine Aufgabe zur Untersuchung auf Befehl ausgeführt wird, die Basispriorität *Niedrig* (Low) zuweisen. Wenn die Priorität eines Prozesses gesenkt wird, erhöht sich dadurch die Ausführungsdauer der Aufgabe und die Ausführungsgeschwindigkeit der Prozesse anderer aktiver Anwendungen wird gesteigert.

In einem aktiven Prozess mit niedriger Priorität können mehrere Aufgaben im Hintergrundmodus ausgeführt werden. Sie können die maximale Anzahl der Prozesse von Aufgaben zur Untersuchung auf Befehl im Hintergrund angeben.

► *Um die Priorität einer bestehenden Aufgabe zur Untersuchung auf Befehl zu ändern, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl** (siehe Abschnitt "Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen" auf Seite 435).
2. Aktivieren oder deaktivieren Sie das Kontrollkästchen Aufgabe im Hintergrundmodus ausführen.

   Dieses Kontrollkästchen ändert die Priorität der Aufgabe.

   Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabenpriorität im Betriebssystem gesenkt. Das Betriebssystem stellt Ressourcen zur Verfügung, um die Aufgabe in Abhängigkeit von der Belastung der CPU und des Dateisystems des Computers durch andere Aufgaben von Kaspersky Embedded Systems Security und Programme auszuführen. Die Aufgabe wird daher bei einer Erhöhung der Belastung langsamer und bei einer Reduzierung der Belastung schneller ausgeführt.

   Wenn dieses Kontrollkästchen deaktiviert ist, wird die Aufgabe mit derselben Priorität ausgeführt wie die übrigen Aufgaben von Kaspersky Embedded Systems Security und die anderen Programme. In diesem Fall wird die Aufgabe schneller ausgeführt.

   Das Kontrollkästchen ist standardmäßig deaktiviert.
3. 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.

Registrierung der Ausführung der Aufgabe zur Untersuchung wichtiger Bereiche

Standardmäßig wird der Schutzstatus des Computers im Detailbereich des Knotens **Kaspersky Embedded Systems Security** angezeigt und wöchentlich nach Abschluss der Aufgabe Untersuchung wichtiger Bereiche aktualisiert.

Der Zeitpunkt, zu dem der Schutzstatus des Computers aktualisiert wird, ist mit dem Zeitplan der Aufgabe zur Untersuchung auf Befehl ab, in deren Einstellungen das Kontrollkästchen Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten aktiviert ist. Standardmäßig ist das Kontrollkästchen nur für die Aufgabe zur Untersuchung wichtiger Bereiche aktiviert und kann für diese Aufgabe nicht geändert werden.

Sie können die Aufgabe zur Untersuchung auf Befehl, die mit dem Schutzstatus des Computers verknüpft ist, nur aus Kaspersky Security Center auswählen.

Untersuchungsbereich der Aufgabe anpassen

Wenn Sie den Untersuchungsbereich in den Aufgaben "Untersuchung beim Hochfahren des Betriebssystems" und zur "Untersuchung wichtiger Bereiche" geändert haben, können Sie in diesen Aufgaben den standardmäßigen Untersuchungsbereich wiederherstellen. Führen Sie dazu die Wiederherstellung von Kaspersky Embedded Systems Security aus (**Start** > **Programme** > Kaspersky Embedded Systems Security > Ändern oder Löschen). Aktivieren Sie im Installationsassistenten die Option Installierte Komponenten reparieren und klicken Sie auf Weiter; aktivieren Sie anschließend das Kontrollkästchen Empfohlene Programmeinstellungen wiederherstellen.

► *Um einen Untersuchungsbereich einer bestehenden Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl** (siehe Abschnitt "Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen" auf Seite 436).
2. Wählen Sie die Registerkarte Untersuchungsbereich aus.
3. Um Objekte in den Untersuchungsbereich einzuschließen, gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü im leeren Bereich der Liste der Untersuchungsbereiche.
   b. Wählen Sie die Kontextmenüoption Untersuchungsbereich hinzufügen aus.
   c. Wählen Sie im geöffneten Fenster Objekte zum Untersuchungsbereich hinzufügen den Typ des Objektes aus, das Sie hinzufügen möchten:
      - Vordefinierter Bereich, wenn Sie einen der vordefinierten Bereiche auf dem geschützten Server hinzufügen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Untersuchungsbereich aus.
      - Laufwerk, Ordner oder Netzwerkobjekt, wenn Sie in den Untersuchungsbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Gültigkeitsbereich über die Schaltfläche Durchsuchen aus.
      - Datei, wenn Sie in den Untersuchungsbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Gültigkeitsbereich über die Schaltfläche Durchsuchen aus.

Sie können ein Objekt nicht zum Untersuchungsbereich hinzufügen, wenn es bereits als Ausnahme aus dem Schutzbereich hinzugefügt wurde.

4. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten, oder führen Sie folgenden Aktionen aus:
   a. Öffnen Sie das Kontextmenü des Untersuchungsbereichs mit der rechten Maustaste.
   b. Wählen Sie im Kontextmenü den Punkt Ausnahme hinzufügen.
   c. Wählen Sie im geöffneten Fenster Ausnahme hinzufügen den Typ des Objektes aus, das Sie als Ausnahme aus dem Untersuchungsbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Untersuchungsbereich.
5. Um den hinzugefügten Untersuchungsbereich oder die hinzugefügte Ausnahme im Kontextmenü des Untersuchungsbereichs, den Sie ändern möchten, zu ändern, wählen Sie den Punkt Bereich ändern.
6. Um die Anzeige eines zuvor hinzugefügten Untersuchungsbereichs bzw. einer zuvor hinzugefügten Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des zu verbergenden Untersuchungsbereichs den Punkt Aus Liste löschen aus.

   Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

7. Klicken Sie auf **OK**.

Das Fenster "Untersuchungsbereich - Einstellungen" wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen

Für ein in der Liste der freigegebenen Netzwerkordner des Computers ausgewähltes Objekt kann eine von drei vordefinierten Sicherheitsstufen übernommen werden: **Maximale Leistung**, **Empfohlen** und **Maximale Sicherheit**.

► *Um eine der vordefinierten Sicherheitsstufen auszuwählen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl** (siehe Abschnitt "**Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen**" auf Seite 436).
2. Wählen Sie die Registerkarte Untersuchungsbereich aus.
3. Wählen Sie in der Liste des Computers ein Element aus dem Untersuchungsbereich aus, um die vordefinierte Sicherheitsstufe festzulegen.
4. Klicken Sie auf die Schaltfläche Konfigurieren.

   Das Fenster Untersuchung auf Befehl wird geöffnet.
5. Wählen Sie auf der Registerkarte Sicherheitsstufe die Sicherheitsstufe aus, die Sie übernehmen möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.

6. Klicken Sie auf **OK**.
7. Klicken Sie auf die Schaltfläche **OK** im Fenster **Eigenschaften: Untersuchung auf Befehl**.

   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 (siehe Abschnitt "Vordefinierte Sicherheitsstufen " auf S. 252).

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des Computers oder den Knoten in der Struktur festlegen.

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

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl** (siehe Abschnitt "Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen" auf Seite 436).
2. Wählen Sie die Registerkarte Untersuchungsbereich aus.
3. Wählen Sie die Elemente in der Liste der Untersuchungsbereiche aus, für die Sie Parameter für Sicherheit anpassen möchten.

   Für einen ausgewählten Knoten oder ein Element im Untersuchungsbereich kann eine vordefinierte Vorlage mit Sicherheitseinstellungen übernommen werden (siehe Abschnitt "Über Vorlagen für Sicherheitseinstellungen" auf Seite 167).

4. Klicken Sie auf die Schaltfläche Konfigurieren.

   Das Fenster Untersuchung auf Befehl wird geöffnet.

5. Passen Sie die Sicherheitseinstellungen des ausgewählten Knotens oder Elements entsprechend ihren Anforderungen an:
   - Allgemeine Einstellungen (siehe Abschnitt "Allgemeine Aufgabeneinstellungen anpassen" auf Seite 445)
   - Aktionen (siehe Abschnitt "**Aktionen anpassen**" auf Seite 448)
   - Optimierung (siehe Abschnitt "**Leistung optimieren**" auf Seite 449)
6. Klicken Sie im Fenster Untersuchung auf Befehl auf **OK**.
7. Klicken Sie im Fenster Untersuchungsbereich auf **OK**.

Die neuen Einstellungen des Untersuchungsbereichs werden gespeichert.

In diesem Abschnitt

Allgemeine Aufgabeneinstellungen anpassen

► *Um allgemeine Einstellungen für Aufgaben zur Untersuchung auf Befehl anpassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl** (siehe Abschnitt "**Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen**" auf Seite 436).
2. Wählen Sie die Registerkarte Untersuchungsbereich aus.
3. Klicken Sie auf die Schaltfläche Konfigurieren.

   Das Fenster Untersuchung auf Befehl wird geöffnet.
4. Klicken Sie auf die Schaltfläche Einstellungen.
5. Geben Sie auf der Registerkarte Allgemein im Abschnitt Objekte untersuchen das Objekt an, das Sie in den Untersuchungsbereich einschließen möchten:
   - Zu untersuchende Objekte
     - Alle Objekte

       Kaspersky Embedded Systems Security untersucht alle Objekte.
     - Objekte, die nach Format untersucht werden

       Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats.

       Die Liste der Dateiformate wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
     - Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden

       Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung.

       Die Erweiterungsliste wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
     - Objekte, die nach der angegebenen Erweiterungsliste untersucht werden

       Kaspersky Embedded Systems Security untersucht Dateien auf der Grundlage der Dateierweiterung. Die Dateierweiterungsliste können Sie im Fenster Erweiterungsliste mithilfe der Schaltfläche Ändern manuell anpassen.
   - Unterordner
   - Untergeordnete Dateien

- Bootsektoren und MBR

  Aktivierung des Schutzes für Laufwerk-Bootsektoren und Master Boot Records (MBR)

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security die Bootsektoren und Master Boot Records auf Festplatten und Wechseldatenträgern des Computers.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Alternative NTFS-Ströme

  Untersuchung zusätzlicher Ströme von Dateien und Ordnern auf den Laufwerken des NTFS-Dateisystems.

  Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm ein möglicherweise infiziertes Objekt und alle NTFS-Streams, die mit diesem Objekte verbunden sind.

  Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm nur das Objekt, das gefunden und als möglicherweise infiziert betrachtet wurde.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Aktivieren oder deaktivieren Sie im Abschnitt Optimierung das Kontrollkästchen Nur neue und veränderte Dateien untersuchen.

   Mit diesem Kontrollkästchen werden die Untersuchung und der Schutz von Dateien, die Kaspersky Embedded Systems Security als neu oder seit der letzten Untersuchung geändert erkennt, aktiviert oder deaktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, untersucht und schützt Kaspersky Embedded Systems Security nur die Dateien, die als neu oder seit der letzten Untersuchung verändert erkannt wurden.

   Wenn das Kontrollkästchen deaktiviert ist, können Sie auswählen, ob Sie nur neue Dateien oder alle Dateien unabhängig von deren Änderungsstatus untersuchen möchten.

   Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert. Wurde die Sicherheitsstufe Maximale Sicherheit oder Empfohlen ausgewählt, ist das Kontrollkästchen deaktiviert.

   Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

7. Geben Sie im Abschnitt Zusammengesetzte Objekte untersuchen die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - **Alle /** nur neue Archive

     Untersuchung von Archiven in den Formaten ZIP, CAB, RAR, ARJ u. a.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Schutzebene abhängig.

- **Alle /** Nur neue SFX-Archive

  Selbstentpackende Archive untersuchen.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security SFX-Archive.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

  Diese Einstellung ist aktiv, wenn das Kontrollkästchen Archive deaktiviert ist.

- **Alle /** Nur neue E-Mail-Datenbanken

  Dateien in Mail-Datenbanken für Microsoft Outlook und Microsoft Outlook Express werden untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Mail-Datenbankdateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Mail-Datenbankdateien von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** nur neue gepackte Objekte

  Untersuchung von ausführbaren Dateien, die mit Packprogrammen für Binärcode wie beispielsweise UPX oder ASPack gepackt wurden.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security ausführbare Dateien, die mit Packprogrammen gepackt wurden.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden ausführbare Dateien, die mit Packprogrammen gepackt wurden, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

- **Alle /** nur neue Dateien in Mail-Formaten

  Dateien in Mail-Formaten werden untersucht. Dazu zählen beispielsweise Nachrichten der Formate Microsoft Outlook und Microsoft Outlook Express.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien in Mail-Formaten.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Dateien in Mail-Formaten von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** Nur neue eingebettete OLE-Objekte

  Untersuchung von Objekten, die in eine Datei eingebettet sind (beispielsweise Excel-Tabellen, Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten).

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte, die in eine Datei eingebettet sind.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Objekte, die in eine Datei eingebettet sind, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

8. Klicken Sie auf **OK**.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

► *Um die Aktionen für infizierte und andere gefundene Objekte während der Ausführung der Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl** (siehe Abschnitt "**Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen**" auf Seite 436).
2. Wählen Sie die Registerkarte Untersuchungsbereich aus.
3. Klicken Sie auf die Schaltfläche Konfigurieren.

   Das Fenster Untersuchung auf Befehl wird geöffnet.
4. Klicken Sie auf die Schaltfläche Einstellungen.
5. Wählen Sie die Registerkarte Aktionen aus.
6. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.
   - Desinfizieren.
   - Desinfizieren. Irreparable Objekte löschen.
   - Löschen.
   - Empfohlene Aktion ausführen.
7. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.
   - In Quarantäne verschieben.
   - Löschen.
   - Empfohlene Aktion ausführen.

8. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen Aktionen je nach Typ des erkannten Objekts ausführen.

      Wenn das Kontrollkästchen aktiviert ist, können Sie für jeden gefundenen Objekttyp einzeln eine primäre und eine sekundäre Aktion festlegen, indem Sie auf die Schaltfläche Einstellungen neben dem Kontrollkästchen klicken. Unabhängig von Ihrer Auswahl gestattet Kaspersky Embedded Systems Security Ihnen nicht, ein infiziertes Objekt zu öffnen oder auszuführen.

      Wenn das Kontrollkästchen deaktiviert ist, führt Kaspersky Embedded Systems Security Aktionen durch, die in den Abschnitten Aktion für infizierte und andere Objekte und Aktion für möglicherweise infizierte Objekte für die jeweils benannten Objekttypen ausgewählt sind.

      Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Klicken Sie auf die Schaltfläche Einstellungen.
   c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts die primäre und die sekundäre Aktion (falls die primäre Aktion nicht durchgeführt werden kann) aus.
   d. Klicken Sie auf **OK**.
9. Wählen Sie die Aktion für nicht desinfizierbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen Vom Programm nicht modifizierbare zusammengesetzte Datei vollständig entfernen, wenn ein eingebettetes Objekt gefunden wird.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert das erzwungene Löschen der übergeordneten zusammengesetzten Datei, wenn ein schädliches und möglicherweise infiziertes oder ein anderes untergeordnetes und eingebettetes Objekt gefunden wird.

   Wenn das Kontrollkästchen aktiviert und die Aufgabe so konfiguriert ist, dass infizierte und möglicherweise infizierte Objekte gelöscht werden, erzwingt Kaspersky Embedded Systems Security das Löschen des gesamten übergeordneten zusammengesetzten Objekts, wenn ein schädliches oder ein anderes eingebettetes Objekt gefunden wird. Das erzwungene Löschen einer übergeordneten Datei mit ihrem Gesamtinhalt wird durchgeführt, wenn es dem Programm nicht gelingt, nur das gefundene untergeordnete Objekt zu löschen (zum Beispiel, wenn das übergeordnete Objekt nicht bearbeitet werden kann).

   Wenn das Kontrollkästchen deaktiviert und die Aufgabe so konfiguriert ist, das infizierte und möglicherweise infizierte Objekte gelöscht werden, führt Kaspersky Embedded Systems Security die festgelegte Aktion nicht aus, wenn das übergeordnete Objekt nicht bearbeitet werden kann.
10. Klicken Sie auf **OK**.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

► *So optimieren Sie die Leistung der Aufgabe Untersuchung auf Befehl:*

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl (siehe Abschnitt "Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen" auf Seite** 436**).**
2. Wählen Sie die Registerkarte Untersuchungsbereich aus.
3. Klicken Sie auf die Schaltfläche Konfigurieren.

   Das Fenster Untersuchung auf Befehl wird geöffnet.
4. Klicken Sie auf die Schaltfläche Einstellungen.
5. Wählen Sie die Registerkarte Optimierung aus.
6. Im Abschnitt Ausnahmen:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Dateien ausschließen.

     Ausnahme von Dateien nach Dateiname oder Dateinamensmaske von der Untersuchung.

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen Objekte bei der Untersuchung.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security alle Objekte.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Nicht erkennen.

     Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie https://encyclopedia.kaspersky.de/knowledge/classification/ .

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen erkennbaren Objekte bei der Untersuchung.

     Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security alle Objekte, die im Programm standardmäßig angegeben sind.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Klicken Sie für jede Einstellung auf die Schaltfläche Ändern, um Ausnahmen hinzuzufügen.
7. Im Abschnitt Erweiterte Einstellungen:
   - Untersuchung beenden, wenn sie länger dauert als (Sek.)

     Beschränkung der Untersuchungsdauer für ein Objekt. Als Standard gilt der Wert 60 Sek.

     Wenn dieses Kontrollkästchen aktiviert ist, wird die maximale Untersuchungsdauer für ein Objekt auf den festgelegten Wert begrenzt.

     Wenn dieses Kontrollkästchen deaktiviert ist, gilt keine Beschränkung für die Untersuchungsdauer.

     Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

- Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)

  Ausnahme zusammengesetzter Objekte, die die maximale Größe übersteigen, von der Untersuchung.

  Wenn dieses Kontrollkästchen aktiviert ist, werden zusammengesetzte Objekte, deren Größe über dem festgelegten Wert liegt, von Kaspersky Embedded Systems Security bei der Untersuchung auf Viren übersprungen.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security zusammengesetzte Objekte jeder Größe.

  Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

- iSwift-Technologie verwenden

  iSwift vergleicht die NTFS-ID der Datei, die in einer Datenbank gespeichert ist, mit einer aktuellen ID. Es werden nur Dateien, deren IDs sich geändert haben (neue Dateien und seit der letzten Untersuchung des NTFS-Dateisystems geänderte Dateien), untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte des NTFS-Systems unabhängig vom Erstellungs- oder Änderungsdatum, ausgenommen Dateien aus Netzwerkordnern.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- iChecker-Technologie verwenden

  iChecker berechnet und speichert Prüfsummen von untersuchten Dateien. Wenn ein Objekt geändert wird, ändert sich die Prüfsumme. Das Programm vergleicht alle Prüfsummen während der Untersuchung und untersucht nur neue und seit der letzten Untersuchung veränderte Dateien.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder veränderte Dateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien unabhängig vom Erstellungs- oder Änderungsdatum.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

8. Klicken Sie auf **OK**.

Die neue Aufgabenkonfiguration wird gespeichert.

Untersuchung von Wechseldatenträgern anpassen

► *Um die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an den geschützten Computer anzupassen, gehen Sie wie folgt vor:*

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

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.

   Wählen Sie im nächsten Fenster **Richtlinien: <Name der Richtlinie>** den Abschnitt Zusätzlich.
5. Klicken Sie auf die Schaltfläche Einstellungen im Unterabschnitt Untersuchung von Wechseldatenträgern.

   Das Fenster Untersuchung von Wechseldatenträgern wird geöffnet.
6. Im Abschnitt Einstellungen für Untersuchung beim Anschließen gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen Wechseldatenträger beim Anschließen über USB untersuchen, wenn Sie möchten, dass Kaspersky Embedded Systems Security automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB) und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste Untersuchung starten 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.

Aufgaben zur Untersuchung auf Befehl über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem lokalen Computer konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen

► *Um die allgemeinen Einstellungen der Aufgabe zur Untersuchung auf Befehl über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten Untersuchung auf Befehl.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe entspricht, die Sie konfigurieren möchten.
3. Klicken Sie im untergeordneten Knoten im Detailbereich auf Eigenschaften.

   Das Fenster Aufgabeneinstellungen wird geöffnet.

► *Um das Fenster "Einstellungen des Untersuchungsbereichs" über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Programmkonsole 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 Detailbereich des ausgewählten Knotens auf den Link Untersuchungsbereich anpassen.

   Das Fenster Untersuchungsbereich - Einstellungen wird geöffnet.

Aufgabe zur Untersuchung auf Befehl erstellen und anpassen

Sie können im Knoten Untersuchung auf Befehl benutzerdefinierte Aufgaben für einen einzelnen Computer erstellen. In den anderen funktionellen Komponenten von Kaspersky Embedded Systems Security ist das Erstellen von benutzerdefinierten Aufgaben nicht verfügbar.

► *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 den Punkt Aufgabe hinzufügen aus.

   Das Fenster Aufgabe hinzufügen wird geöffnet.
3. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Name – Aufgabenname, maximal 100 Zeichen, kann aus beliebigen Zeichen mit Ausnahme von **" * < > & \ : |** bestehen.

Ohne die Angabe des Aufgabennamens können Sie weder die neue Aufgabe speichern noch zur Konfiguration der Einstellungen der neuen Aufgabe auf den Registerkarten Zeitplan, Erweitert und Mit folgenden Rechten starten wechseln.

- Beschreibung – beliebige Zusatzinformationen über die Aufgabe, maximal 2.000 Zeichen. Diese Informationen werden im Fenster Eigenschaften der Aufgabe angezeigt.
- Heuristische Analyse verwenden

  Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der heuristischen Analyse bei der Objektuntersuchung.

  Wenn dieses Kontrollkästchen aktiviert ist, ist die heuristische Analyse aktiviert.

  Wurde dieses Kontrollkästchen deaktiviert, ist die heuristische Analyse deaktiviert.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
- Aufgabe im Hintergrundmodus ausführen

  Dieses Kontrollkästchen ändert die Priorität der Aufgabe.

  Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabenpriorität im Betriebssystem gesenkt. Das Betriebssystem stellt Ressourcen zur Verfügung, um die Aufgabe in Abhängigkeit von der Belastung der CPU und des Dateisystems des Computers durch andere Aufgaben von Kaspersky Embedded Systems Security und Programme auszuführen. Die Aufgabe wird daher bei einer Erhöhung der Belastung langsamer und bei einer Reduzierung der Belastung schneller ausgeführt.

  Wenn dieses Kontrollkästchen deaktiviert ist, wird die Aufgabe mit derselben Priorität ausgeführt wie die übrigen Aufgaben von Kaspersky Embedded Systems Security und die anderen Programme. In diesem Fall wird die Aufgabe schneller ausgeführt.

  Das Kontrollkästchen ist standardmäßig deaktiviert.
- Vertrauenswürdige Zone anwenden

  Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

  Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

  Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs für die Aufgabe.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
- Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten

  Dieses Kontrollkästchen ändert die Priorität einer Aufgabe: Es aktiviert oder deaktiviert das Protokollieren des Ereignisses *Untersuchung wichtiger Bereiche* und das Update des Schutzstatus des Computers. Kaspersky Security Center überprüft die Sicherheitsstufe des Computers (der Computer) mithilfe der Leistungsergebnisse von Aufgaben mit dem Status *Untersuchung wichtiger Bereiche*. In den Eigenschaften von lokalen System- und benutzerdefinierten Aufgaben von Kaspersky Embedded Systems Security ist das Kontrollkästchen nicht verfügbar. Sie können den Wert dieser Einstellung nur auf Seiten von Kaspersky Security Center ändern.

Wenn dieses Kontrollkästchen aktiviert ist, protokolliert der Administrationsserver den Abschluss der Untersuchung wichtiger Bereiche und aktualisiert den Schutzstatus des Computers anhand der Ergebnisse der Aufgabenausführung. Die Untersuchungsaufgabe hat eine hohe Priorität.

Ist das Kontrollkästchen deaktiviert, so wird die Untersuchungsaufgabe mit niedriger Priorität ausgeführt.

Das Kontrollkästchen ist für benutzerdefinierte Aufgaben zur Untersuchung auf Befehl standardmäßig deaktiviert.

- KSN zur Überprüfung verwenden

  Mithilfe dieses Kontrollkästchens wird die Verwendung der Cloud-Dienste von Kaspersky Security Network (KSN) in der Aufgabe aktiviert bzw. deaktiviert.

  Ist das Kontrollkästchen aktiviert, so verwendet das Programm die von den KSN-Diensten übermittelten Daten, was eine schnellere Reaktion des Programms auf neue Bedrohungen gewährleistet und die Wahrscheinlichkeit von Fehlalarmen verringert.

  Ist das Kontrollkästchen deaktiviert, werden die KSN-Dienste von der Aufgabe zur Untersuchung auf Befehl nicht verwendet.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Passen Sie die Einstellungen für den Zeitplan für den Aufgabenstart (siehe Abschnitt "Einstellungen des Zeitplans für den Aufgabenstart anpassen" auf Seite 160) auf den Registerkarten Zeitplan und Erweitert an.
5. Passen Sie auf der Registerkarte Mit folgenden Rechten starten die Einstellungen für den Aufgabenstart mit Benutzerrechten an (siehe Abschnitt "Festlegen eines Benutzerkontos für den Aufgabenstart" auf Seite 163).
6. Klicken Sie im Fenster Aufgabe hinzufügen auf **OK**.

   Es wird eine neue benutzerdefinierte Aufgabe zur Untersuchung auf Befehl erstellt. Der Knoten mit dem Namen der neuen Aufgabe wird in der Programmkonsolenstruktur angezeigt. Die Operation wird im Systemaudit-Protokoll registriert (auf Seite 214).
7. Wählen Sie bei Bedarf im Detailbereich des ausgewählten Knotens Untersuchungsbereich anpassen aus.

   Das Fenster Untersuchungsbereich - Einstellungen wird geöffnet.
8. Wählen Sie in der Struktur oder Liste der Dateiressourcen des Computers diejenigen Knoten oder Elemente aus, die Sie dem Untersuchungsbereich hinzufügen möchten.
9. Wählen Sie eine der voreingestellten Sicherheitsstufen aus (siehe Abschnitt "Über vordefinierte Sicherheitsstufen für Aufgaben zur Untersuchung auf Befehl" auf Seite 429) oder passen Sie die Untersuchungseinstellungen manuell an (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 461).
10. Klicken Sie im Fenster Untersuchungsbereich - Einstellungen auf **Speichern**.

Die vorgenommenen Einstellungen werden beim nächsten Aufgabenstart übernommen.

Untersuchungsbereich in den Aufgaben zur Untersuchung auf Befehl

Dieser Abschnitt enthält Informationen über die Erstellung und Verwendung eines Untersuchungsbereichs in den Aufgaben zur Untersuchung auf Befehl.

In diesem Abschnitt

Einstellungen für die Anzeige der freigegebenen Netzwerkordner des Untersuchungsbereichs anpassen

► *Um die Art der Anzeige der freigegebenen Netzwerkordner des Computers beim Anpassen der Einstellungen für den Untersuchungsbereich auszuwählen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Öffnen Sie in der linken oberen Ecke des geöffneten Fensters die Dropdown-Liste. Führen Sie eine der Aktionen durch:
   - Wählen Sie den Punkt Als Baumstruktur anzeigen, wenn Sie möchten, dass die freigegebenen Netzwerkordner als Baumstruktur angezeigt werden.
   - Wählen Sie den Punkt Als Liste anzeigen, wenn Sie möchten, dass die freigegebenen Netzwerkordner des geschützten Computers in Form einer Liste angezeigt werden.

   Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Computers als Liste angezeigt.
3. Klicken Sie auf die Schaltfläche Speichern.

Das Einstellungsfenster für den Untersuchungsbereich wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden angewandt.

Untersuchungsbereich erstellen

Wenn Sie Kaspersky Embedded Systems Security auf dem geschützten Computer im Remote-Betrieb über die Programmkonsole verwalten, die am Administrator-Arbeitsplatz installiert ist, müssen Sie zur Gruppe der Administratoren auf dem geschützten Computer gehören, um die dort befindlichen Ordner zu sehen.

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

Wenn Sie den Untersuchungsbereich in den Aufgaben "Untersuchung beim Hochfahren des Betriebssystems" und zur "Untersuchung wichtiger Bereiche" geändert haben, können Sie in diesen Aufgaben den standardmäßigen Untersuchungsbereich wiederherstellen. Führen Sie dazu die Wiederherstellung von Kaspersky Embedded Systems Security aus (**Start** > **Programme** > Kaspersky Embedded Systems Security > Ändern oder Löschen). Aktivieren Sie im Installationsassistenten die Option Installierte Komponenten reparieren und klicken Sie auf Weiter; aktivieren Sie anschließend das Kontrollkästchen Empfohlene Programmeinstellungen wiederherstellen.

Die Vorgehensweise beim Erstellen des Untersuchungsbereichs in der Aufgabe zur Untersuchung auf Befehl hängt vom Typ der Anzeige der freigegebenen Netzwerkordner ab (siehe Abschnitt "Einstellungen für die Anzeige der freigegebenen Netzwerkordner anpassen" auf Seite 456). Sie können die Anzeige der freigegebenen Netzwerkordner in Form einer Liste (wird standardmäßig verwendet) oder in Form einer Baumstruktur festlegen.

► *Um bei der Arbeit mit der Struktur der freigegebenen Netzwerkordner einen Untersuchungsbereich zu erstellen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Öffnen Sie im rechten Teil des geöffneten Fensters die Struktur mit den freigegebenen Netzwerkordnern des Computers, um alle Knoten anzuzeigen.
3. Führen Sie folgende Aktionen aus:
   - Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten.
   - Deaktivieren Sie das Kontrollkästchen Arbeitsplatz, um einzelne Knoten in den Untersuchungsbereich einzuschließen, und gehen Sie wie folgt vor:
     - Um alle Laufwerke eines bestimmten Typs in den Untersuchungsbereich aufzunehmen, aktivieren Sie das Kontrollkästchen neben dem Namen des entsprechenden Datenträgertyps (z. B. um alle Wechseldatenträger auf dem Computer einzuschließen, aktivieren Sie das Kontrollkästchen Wechseldatenträger).
     - Um einen einzelnen Datenträger eines bestimmten Typs in den Untersuchungsbereich aufzunehmen, öffnen Sie den Knoten, der die Liste dieses Datenträgertyps enthält, und aktivieren Sie das Kontrollkästchen für das entsprechende Laufwerk. Um beispielsweise den Wechseldatenträger **F:** auszuwählen, erweitern Sie den Knoten Wechseldatenträger und aktivieren Sie das Kontrollkästchen für das Laufwerk **F:**.
     - Wenn Sie nur einen einzelnen Ordner oder eine einzelne Datei auf dem Laufwerk in den Schutzbereich einschließen möchten, aktivieren Sie das Kontrollkästchen neben dem Namen dieses Ordners bzw. dieser Datei.
4. Klicken Sie auf die Schaltfläche Speichern.

Das Fenster "Untersuchungsbereich - Einstellungen" wird geschlossen. Die neu vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

► *Um mithilfe der Liste der freigegebenen Netzwerkordner einen Untersuchungsbereich zu erstellen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Deaktivieren Sie das Kontrollkästchen Arbeitsplatz, um einzelne Knoten in den Untersuchungsbereich einzuschließen, und gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü des Untersuchungsbereichs mit der rechten Maustaste.

b. Wählen Sie im Kontextmenü der Schaltfläche den Punkt Untersuchungsbereich hinzufügen aus.

c. Wählen Sie im geöffneten Fenster Untersuchungsbereich hinzufügen den Typ des Objektes aus, das Sie hinzufügen möchten:

- Vordefinierter Bereich, wenn Sie einen der vordefinierten Bereiche auf dem geschützten Computer hinzufügen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Untersuchungsbereich aus.
- Laufwerk, Ordner oder Netzwerkobjekt, wenn Sie in den Untersuchungsbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Gültigkeitsbereich über die Schaltfläche Durchsuchen aus.
- Datei, wenn Sie in den Untersuchungsbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Gültigkeitsbereich über die Schaltfläche Durchsuchen aus.

Sie können ein Objekt nicht zum Untersuchungsbereich hinzufügen, wenn es bereits als Ausnahme aus dem Schutzbereich hinzugefügt wurde.

3. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten, oder führen Sie folgenden Aktionen aus:

   a. Öffnen Sie das Kontextmenü des Untersuchungsbereichs mit der rechten Maustaste.

   b. Wählen Sie im Kontextmenü den Punkt Ausnahme hinzufügen.

   c. Wählen Sie im geöffneten Fenster Ausnahme hinzufügen den Typ des Objektes aus, das Sie als Ausnahme aus dem Untersuchungsbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Untersuchungsbereich.

4. Um den hinzugefügten Untersuchungsbereich oder die hinzugefügte Ausnahme im Kontextmenü des Untersuchungsbereichs, den Sie ändern möchten, zu ändern, wählen Sie den Punkt Bereich ändern.

5. Um die Anzeige eines zuvor hinzugefügten Untersuchungsbereichs bzw. einer zuvor hinzugefügten Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des zu verbergenden Untersuchungsbereichs den Punkt Aus Liste löschen aus.

Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

6. Klicken Sie auf die Schaltfläche Speichern.

Das Fenster "Untersuchungsbereich - Einstellungen" wird geschlossen. Die neu vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Netzwerkobjekte in den Untersuchungsbereich aufnehmen

Sie können Netzlaufwerke, Ordner und Dateien in den Untersuchungsbereich aufnehmen. Geben Sie dazu die Netzwerkpfade im UNC-Format (Universal Naming Convention) an.

Sie können keine Netzwerkordner untersuchen, wenn Sie unter dem Systemkonto arbeiten.

► *Um eine Netzwerkressource zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie im linken unteren Teil des Fensters aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.
3. Gehen Sie im Kontextmenü des Knotens Netzwerkumgebung wie folgt vor:
   - Wählen Sie den Punkt Netzwerkordner hinzufügen aus, wenn Sie einen Netzwerkordner zum Untersuchungsbereich hinzufügen möchten.
   - Wählen Sie den Punkt Netzwerkdatei hinzufügen aus, wenn Sie eine Netzwerkdatei zum Untersuchungsbereich hinzufügen möchten.
4. Geben Sie den Pfad des Netzwerkordners oder der Netzwerkdatei im UNC-Format (Universal Naming Convention) an und drücken Sie die **EINGABE**-Taste.
5. Aktivieren Sie das Kontrollkästchen neben dem Namen des hinzugefügten Netzwerkobjekts, um es in den Untersuchungsbereich aufzunehmen.
6. Ändern Sie, falls erforderlich, die Sicherheitseinstellungen für das hinzugefügte Netzwerkobjekt.
7. Klicken Sie auf die Schaltfläche Speichern.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Virtuelle Untersuchungsbereiche erstellen

Sie können in den Untersuchungsbereich dynamische Laufwerke, Ordner und Dateien aufnehmen – einen virtuellen Untersuchungsbereich erstellen.

Sie können separate virtuelle Festplatten, Ordner oder Dateien nur dann zum Schutzbereich bzw. Untersuchungsbereich hinzufügen, wenn der Schutzbereich bzw. Untersuchungsbereich in Form einer Struktur der Dateiressourcen angezeigt wird (siehe Abschnitt "Einstellungen für die Anzeige der freigegebenen Netzwerkordner des Untersuchungsbereichs anpassen" auf Seite 456).

► *Um eine virtuelle Festplatte zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie im linken unteren Teil des Fensters aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.
3. Öffnen Sie in der Struktur der Dateiressourcen des Computers das Kontextmenü für den Knoten Virtuelle Festplatten, klicken Sie auf Virtuelle Festplatte hinzufügen und wählen Sie in der Liste der verfügbaren Namen einen Namen für die anzulegende virtuelle Festplatte.
4. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Laufwerk, um das Laufwerk in den Untersuchungsbereich aufzunehmen.
5. Klicken Sie auf die Schaltfläche Speichern.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

► *Um einen virtuellen Ordner oder eine virtuelle Datei zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie im linken unteren Teil des Fensters aus der Dropdown-Liste den Punkt Als Baumstruktur anzeigen.
3. Öffnen Sie in der Struktur der Dateiressourcen des Computers das Kontextmenü des Knotens, zu dem Sie einen Ordner oder eine Datei hinzufügen möchten, und wählen Sie einen der folgenden Punkte aus:
   - Virtuellen Ordner hinzufügen, wenn Sie einen virtuellen Ordner zum Untersuchungsbereich hinzufügen möchten.
   - Virtuelle Datei hinzufügen, wenn Sie eine virtuelle Datei zum Untersuchungsbereich hinzufügen möchten.
4. Tragen Sie im Eingabefeld den Namen für den Ordner bzw. die Datei ein.
5. In der Zeile mit dem Namen des erstellten Ordners bzw. der erstellten Datei aktivieren Sie das Kontrollkästchen, um den Ordner bzw. die Datei in den Untersuchungsbereich zu übernehmen.
6. Klicken Sie auf die Schaltfläche Speichern.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen

Für einen Knoten oder ein Element, der bzw. das in der Struktur bzw. in der Liste der freigegebenen Netzwerkordner des Computers ausgewählt ist, kann eine von drei vordefinierten Sicherheitsstufen übernommen werden: **Maximale Leistung**, **Empfohlen** und **Maximale Sicherheit**.

► *Um eine der vordefinierten Sicherheitsstufen auszuwählen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie in der Baumstruktur oder in der Liste der freigegebenen Netzwerkordner des Computers einen Knoten oder ein Element aus, für den bzw. das Sie eine vordefinierte Sicherheitsstufe auswählen möchten.
3. Vergewissern Sie sich, dass der ausgewählte Knoten bzw. das Element zum Untersuchungsbereich gehört.
4. Wählen Sie im rechten Teil des Fensters auf der Registerkarte Sicherheitsstufe die Sicherheitsstufe aus, die Sie anwenden möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
5. Klicken Sie auf die Schaltfläche Speichern.

   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 (siehe Abschnitt "Vordefinierte Sicherheitsstufen " auf S. 252).

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des Computers oder den Knoten in der Struktur festlegen.

Bei der Arbeit mit der Struktur der Dateiressourcen im Netzwerk 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.

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

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie im linken Bereich des Fensters den Knoten oder das Element aus, dessen Sicherheitsanstellungen Sie konfigurieren möchten.

   Für einen ausgewählten Knoten oder ein Element im Untersuchungsbereich kann eine vordefinierte Vorlage mit Sicherheitseinstellungen übernommen werden (siehe Abschnitt "Über Vorlagen für Sicherheitseinstellungen" auf Seite 167).
3. Passen Sie die Sicherheitseinstellungen des ausgewählten Knotens oder Elements entsprechend ihren Anforderungen auf den folgenden Registerkarten an:
   - Allgemeine Einstellungen (siehe Abschnitt "Allgemeine Aufgabeneinstellungen anpassen" auf Seite 461)
   - Aktionen (siehe Abschnitt "Aktionen anpassen" auf Seite 464)
   - Optimierung (siehe Abschnitt "Leistung optimieren" auf Seite 466)
   - Hierarchischer Speicher
4. Klicken Sie im Fenster Untersuchungsbereich - Einstellungen auf Speichern.

Die neuen Einstellungen des Untersuchungsbereichs werden gespeichert.

In diesem Abschnitt

Allgemeine Aufgabeneinstellungen anpassen

► *So passen Sie die allgemeinen Sicherheitseinstellungen der Untersuchung auf Befehl an:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie die Registerkarte Allgemein aus.
3. Geben Sie im Abschnitt Objekte untersuchen das Objekt an, das Sie in den Untersuchungsbereich einschließen möchten:
   - Zu untersuchende Objekte
     - Alle Objekte

       Kaspersky Embedded Systems Security untersucht alle Objekte.
     - Objekte, die nach Format untersucht werden

       Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats.

       Die Liste der Dateiformate wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
     - Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden

       Kaspersky Embedded Systems Security untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung.

       Die Erweiterungsliste wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Embedded Systems Security enthalten.
     - Objekte, die nach der angegebenen Erweiterungsliste untersucht werden

       Kaspersky Embedded Systems Security untersucht Dateien auf der Grundlage der Dateierweiterung. Die Dateierweiterungsliste können Sie im Fenster Erweiterungsliste mithilfe der Schaltfläche Ändern manuell anpassen.
   - Bootsektoren und MBR

     Aktivierung des Schutzes für Laufwerk-Bootsektoren und Master Boot Records (MBR)

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security die Bootsektoren und Master Boot Records auf Festplatten und Wechseldatenträgern des Computers.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
   - Alternative NTFS-Ströme

     Untersuchung zusätzlicher Ströme von Dateien und Ordnern auf den Laufwerken des NTFS-Dateisystems.

     Wenn das Kontrollkästchen aktiviert ist, untersucht das Programm ein möglicherweise infiziertes Objekt und alle NTFS-Streams, die mit diesem Objekte verbunden sind.

     Wenn das Kontrollkästchen deaktiviert ist, untersucht das Programm nur das Objekt, das gefunden und als möglicherweise infiziert betrachtet wurde.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Aktivieren oder deaktivieren Sie im Abschnitt Optimierung das Kontrollkästchen Nur neue und veränderte Dateien untersuchen.

   Mit diesem Kontrollkästchen werden die Untersuchung und der Schutz von Dateien, die Kaspersky Embedded Systems Security als neu oder seit der letzten Untersuchung geändert erkennt, aktiviert oder deaktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, untersucht und schützt Kaspersky Embedded Systems Security nur die Dateien, die als neu oder seit der letzten Untersuchung verändert erkannt wurden.

   Wenn das Kontrollkästchen deaktiviert ist, können Sie auswählen, ob Sie nur neue Dateien oder alle Dateien unabhängig von deren Änderungsstatus untersuchen möchten.

   Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert. Wurde die Sicherheitsstufe Maximale Sicherheit oder Empfohlen ausgewählt, ist das Kontrollkästchen deaktiviert.

Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

5. Geben Sie im Abschnitt Zusammengesetzte Objekte untersuchen die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - **Alle /** nur neue Archive

     Untersuchung von Archiven in den Formaten ZIP, CAB, RAR, ARJ u. a.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Schutzebene abhängig.

   - **Alle /** Nur neue SFX-Archive

     Selbstentpackende Archive untersuchen.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security SFX-Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Schutzebene abhängig.

     Diese Einstellung ist aktiv, wenn das Kontrollkästchen Archive deaktiviert ist.

   - **Alle /** Nur neue E-Mail-Datenbanken

     Dateien in Mail-Datenbanken für Microsoft Outlook und Microsoft Outlook Express werden untersucht.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Mail-Datenbankdateien.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Mail-Datenbankdateien von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** nur neue gepackte Objekte

  Untersuchung von ausführbaren Dateien, die mit Packprogrammen für Binärcode wie beispielsweise UPX oder ASPack gepackt wurden.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security ausführbare Dateien, die mit Packprogrammen gepackt wurden.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden ausführbare Dateien, die mit Packprogrammen gepackt wurden, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

- **Alle /** nur neue Dateien in Mail-Formaten

  Dateien in Mail-Formaten werden untersucht. Dazu zählen beispielsweise Nachrichten der Formate Microsoft Outlook und Microsoft Outlook Express.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien in Mail-Formaten.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Dateien in Mail-Formaten von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle /** Nur neue eingebettete OLE-Objekte

  Untersuchung von Objekten, die in eine Datei eingebettet sind (beispielsweise Excel-Tabellen, Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten).

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte, die in eine Datei eingebettet sind.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Objekte, die in eine Datei eingebettet sind, von Kaspersky Embedded Systems Security bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Schutzebene abhängig.

6. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

► *So passen Sie die Aktionen für infizierte und andere gefundene Objekte für die Untersuchung auf Befehl an:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie die Registerkarte Aktionen aus.
3. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.

- Desinfizieren.
- Desinfizieren. Irreparable Objekte löschen.
- Löschen.
- Empfohlene Aktion ausführen.

4. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - Nur informieren.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Embedded Systems Security den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Protokoll der Aufgabenausführung registriert: *Objekt nicht desinfiziert*. *Grund: Aufgrund benutzerdefinierter Einstellungen wurde keine Aktion ausgeführt, um das erkannte Objekt zu neutralisieren.* Das Ereignis gibt alle verfügbaren Informationen bezüglich des gefundenen Objekts an.

     Der Modus Nur informieren muss für jeden Schutz- bzw. Untersuchungsbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security die Sicherheitsstufe automatisch auf Benutzerdefiniert.

   - In Quarantäne verschieben.
   - Löschen.
   - Empfohlene Aktion ausführen.

5. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen Aktionen je nach Typ des erkannten Objekts ausführen.

      Wenn das Kontrollkästchen aktiviert ist, können Sie für jeden gefundenen Objekttyp einzeln eine primäre und eine sekundäre Aktion festlegen, indem Sie auf die Schaltfläche Einstellungen neben dem Kontrollkästchen klicken. Unabhängig von Ihrer Auswahl gestattet Kaspersky Embedded Systems Security Ihnen nicht, ein infiziertes Objekt zu öffnen oder auszuführen.

      Wenn das Kontrollkästchen deaktiviert ist, führt Kaspersky Embedded Systems Security Aktionen durch, die in den Abschnitten Aktion für infizierte und andere Objekte und Aktion für möglicherweise infizierte Objekte für die jeweils benannten Objekttypen ausgewählt sind.

      Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Klicken Sie auf die Schaltfläche Einstellungen.
   c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts die primäre und die sekundäre Aktion (falls die primäre Aktion nicht durchgeführt werden kann) aus.
   d. Klicken Sie auf **OK**.

6. Wählen Sie die Aktion für nicht desinfizierbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen Vom Programm nicht modifizierbare zusammengesetzte Datei vollständig entfernen, wenn ein eingebettetes Objekt gefunden wird.

Dieses Kontrollkästchen aktiviert bzw. deaktiviert das erzwungene Löschen der übergeordneten zusammengesetzten Datei, wenn ein schädliches und möglicherweise infiziertes oder ein anderes untergeordnetes und eingebettetes Objekt gefunden wird.

Wenn das Kontrollkästchen aktiviert und die Aufgabe so konfiguriert ist, dass infizierte und möglicherweise infizierte Objekte gelöscht werden, erzwingt Kaspersky Embedded Systems Security das Löschen des gesamten übergeordneten zusammengesetzten Objekts, wenn ein schädliches oder ein anderes eingebettetes Objekt gefunden wird. Das erzwungene Löschen einer übergeordneten Datei mit ihrem Gesamtinhalt wird durchgeführt, wenn es dem Programm nicht gelingt, nur das gefundene untergeordnete Objekt zu löschen (zum Beispiel, wenn das übergeordnete Objekt nicht bearbeitet werden kann).

Wenn das Kontrollkästchen deaktiviert und die Aufgabe so konfiguriert ist, das infizierte und möglicherweise infizierte Objekte gelöscht werden, führt Kaspersky Embedded Systems Security die festgelegte Aktion nicht aus, wenn das übergeordnete Objekt nicht bearbeitet werden kann.

7. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

► *So optimieren Sie die Leistung der Aufgabe Untersuchung auf Befehl:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Wählen Sie die Registerkarte Optimierung aus.
3. Im Abschnitt Ausnahmen:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Dateien ausschließen.

     Ausnahme von Dateien nach Dateiname oder Dateinamensmaske von der Untersuchung.

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen Objekte bei der Untersuchung.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security alle Objekte.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen Nicht erkennen.

     Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie https://encyclopedia.kaspersky.de/knowledge/classification/ .

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen erkennbaren Objekte bei der Untersuchung.

     Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security alle Objekte, die im Programm standardmäßig angegeben sind.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - Klicken Sie für jede Einstellung auf die Schaltfläche Ändern, um Ausnahmen hinzuzufügen.

4. Im Abschnitt Erweiterte Einstellungen:

   - Untersuchung beenden, wenn sie länger dauert als (Sek.)

     Beschränkung der Untersuchungsdauer für ein Objekt. Als Standard gilt der Wert 60 Sek.

     Wenn dieses Kontrollkästchen aktiviert ist, wird die maximale Untersuchungsdauer für ein Objekt auf den festgelegten Wert begrenzt.

     Wenn dieses Kontrollkästchen deaktiviert ist, gilt keine Beschränkung für die Untersuchungsdauer.

     Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

   - Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)

     Ausnahme zusammengesetzter Objekte, die die maximale Größe übersteigen, von der Untersuchung.

     Wenn dieses Kontrollkästchen aktiviert ist, werden zusammengesetzte Objekte, deren Größe über dem festgelegten Wert liegt, von Kaspersky Embedded Systems Security bei der Untersuchung auf Viren übersprungen.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security zusammengesetzte Objekte jeder Größe.

     Das Kontrollkästchen ist für die Sicherheitsstufe Maximale Leistung standardmäßig aktiviert.

   - iSwift-Technologie verwenden

     iSwift vergleicht die NTFS-ID der Datei, die in einer Datenbank gespeichert ist, mit einer aktuellen ID. Es werden nur Dateien, deren IDs sich geändert haben (neue Dateien und seit der letzten Untersuchung des NTFS-Dateisystems geänderte Dateien), untersucht.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Objekte des NTFS-Systems unabhängig vom Erstellungs- oder Änderungsdatum, ausgenommen Dateien aus Netzwerkordnern.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - iChecker-Technologie verwenden

     iChecker berechnet und speichert Prüfsummen von untersuchten Dateien. Wenn ein Objekt geändert wird, ändert sich die Prüfsumme. Das Programm vergleicht alle Prüfsummen während der Untersuchung und untersucht nur neue und seit der letzten Untersuchung veränderte Dateien.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security nur neue oder veränderte Dateien.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security Dateien unabhängig vom Erstellungs- oder Änderungsdatum.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

5. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Konfigurieren des hierarchischen Speichers

► *So passen Sie die Aktionen für infizierte und andere gefundene Objekte für die Untersuchung auf Befehl an:*

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen (auf S. 453).
2. Klicken Sie auf die Registerkarte **Hierarchischer Speicher**.
3. Wählen Sie eine Aktion für die Offlinedateien aus:
   - **Nicht untersuchen**.
   - **Nur den residenten Teil einer Datei untersuchen**.
   - **Datei vollständig untersuchen**.

     Wenn diese Aktion ausgewählt ist, können Sie die folgenden Optionen festlegen:

     - Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Nur, wenn auf die Datei innerhalb des angegebenen Zeitraums zugegriffen wurde (Tage)** und geben Sie die Anzahl von Tagen an.
     - Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datei, wenn möglich, nicht auf die lokale Festplatte kopieren**.
4. Klicken Sie auf Speichern.

Die neue Aufgabenkonfiguration wird gespeichert.

Wechseldatenträger untersuchen

► *Um die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an den geschützten Computer in der Programmkonsole anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens Kaspersky Embedded Systems Security und wählen Sie die Option Untersuchung von Wechseldatenträgern aus.

   Das Fenster Untersuchung von Wechseldatenträgern wird geöffnet.
2. Im Abschnitt Einstellungen für Untersuchung beim Anschließen gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen Wechseldatenträger beim Anschließen über USB untersuchen, wenn Sie möchten, dass Kaspersky Embedded Systems Security automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB) und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste Untersuchung starten mit Sicherheitsstufe die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.
3. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und übernommen.

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 bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen.

Diese Informationen stehen auch zur Verfügung, wenn Sie eine Aufgabe anhalten. Sie können die Aufgabenstatistik im Protokoll der Aufgabenausführung aufrufen (siehe Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in Protokollen der Aufgabenausführung anzeigen" auf Seite 218).

► *Um die Statistik der Aufgabe zur Untersuchung auf Befehl anzusehen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Programmkonsole 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 bis zum jetzigen Zeitpunkt verarbeitet hat, werden in der nachfolgenden Tabelle angezeigt.

Tabelle 61. Statistik von Aufgaben zur Untersuchung auf Befehl

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 dieselbe Schadsoftware, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Infizierte und andere gefundene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security als infiziert eingestuft hat, oder gefundene legale Software, die nicht aus dem Gültigkeitsbereich der Aufgaben zum Echtzeitschutz oder zur Untersuchung auf Befehl ausgeschlossen und als legitime Software klassifiziert wurden, die von Eindringlingen verwendet werden kann, um Ihren Computer oder persönliche Daten zu beschädigen.
Möglicherweise infizierte Objekte gefunden	Anzahl der von Kaspersky Embedded Systems Security gefundenen Objekte, die als möglicherweise infiziert eingestuft wurden
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security aus folgenden Gründen nicht desinfiziert wurden: • Der Typ des gefundenen Objekts kann nicht desinfiziert werden • Bei der Desinfektion ist eine Störung aufgetreten
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos versucht hat, in die Quarantäne zu verschieben, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Nicht gelöschte 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 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 anders Programm gesperrt war.

Feld	Beschreibung
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu kopieren versucht hat, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Verarbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden.
In Quarantäne verschoben	Anzahl der Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Embedded Systems Security im Backup gespeichert wurden.
Gelöschte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security entfernt 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.
Verarbeitete Objekte	Objekte insgesamt, die von Kaspersky Embedded Systems Security verarbeitet wurden.

Sie können auch eine Statistik der Aufgaben zur Untersuchung auf Befehl im Protokoll der Aufgabenausführung über den Link Protokoll der Aufgabenausführung öffnen im Abschnitt Verwaltung des Detailbereichs anzeigen.

Es wird empfohlen, nach Abschluss der Aufgabe die im Protokoll der Aufgabenausführung registrierten Ereignisse auf der Registerkarte Ereignisse manuell zu bearbeiten.

Vertrauenswürdige Zone

Dieser Abschnitt enthält Informationen über die vertrauenswürdige Zone für Kaspersky Embedded Systems Security, Anweisungen zum Hinzufügen von Objekten in die vertrauenswürdige Zone sowie zur Anwendung der vertrauenswürdigen Zone beim Ausführen von Aufgaben.

In diesem Kapitel

Über die vertrauenswürdige Zone

Bei der vertrauenswürdigen Zone handelt es sich um eine Liste von Ausnahmen vom Schutz- oder Untersuchungsbereich, die Sie erstellen und auf die Aufgaben "Untersuchung auf Befehl" und "Echtzeitschutz für Dateien" anwenden können.

Wenn Sie bei der Installation von Kaspersky Embedded Systems Security die Kontrollkästchen **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen** und **Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen** aktiviert haben, fügt Kaspersky Embedded Systems Security für die Aufgaben zum Echtzeitschutz für Computer jene Dateien zur vertrauenswürdigen Zone hinzu, die von Microsoft und Kaspersky Lab empfohlen werden.

Anhand folgender Regeln können Sie in Kaspersky Embedded Systems Security eine vertrauenswürdige Zone erstellen:

- Vertrauenswürdige Prozesse. In die vertrauenswürdige Zone werden Objekte aufgenommen, auf welche die Prozesse von Programmen zugreifen, die sensibel auf das Abfangen von Dateien reagieren.
- Backup-Operationen. In die vertrauenswürdige Zone werden Objekte aufgenommen, auf die Systeme für Backup-Operationen von Festplatten auf externe Geräte zugreifen.
- Ausnahmen. In die vertrauenswürdige Zone werden Objekte anhand ihres Speicherorts und / oder anhand eines in ihnen erkannten Objekts aufgenommen.

Sie können die vertrauenswürdige Zone in der Aufgabe "Echtzeitschutz für Dateien", in vom Benutzer neu erstellten Aufgaben zur Untersuchung auf Befehl sowie in allen Systemaufgaben zur Untersuchung auf Befehl anwenden. Eine Ausnahme bildet die Aufgabe zur Untersuchung von Quarantäne-Objekten.

In den Aufgaben zum Echtzeitschutz für Dateien und zur Untersuchung auf Befehl wird die vertrauenswürdige Zone standardmäßig übernommen.

Sie können die Liste mit den Regeln für die Erstellung einer vertrauenswürdigen Zone in eine Konfigurationsdatei im XML-Format exportieren, um sie später auf einem anderen Computer in Kaspersky Embedded Systems Security zu importieren.

Vertrauenswürdige Prozesse

Wird in den Aufgaben zum Echtzeitschutz für Dateien und zum Schutz des Datenverkehrs verwendet.

Bestimmte Programme auf dem Computer können instabil werden, wenn Dateien, auf die das Programm zugreift, von Kaspersky Embedded Systems Security abgefangen werden. Zu diesen Anwendungen zählen beispielsweise Systemprogramme von Domain-Controllern.

Damit solche Programme nicht negativ beeinflusst werden, können Sie den Schutz für jene Dateien deaktivieren, auf die die aktiven Prozesse dieser Programme zugreifen. Dazu wird in der vertrauenswürdigen Zone eine Liste mit vertrauenswürdigen Prozessen angelegt.

Microsoft empfiehlt, bestimmte Dateien des Betriebssystems Microsoft Windows und Programmdateien der Firma Microsoft als nicht infizierbar vom Echtzeitschutz für Dateien auszuschließen. Eine Auswahl der empfohlenen Ausnahmen finden Sie auf der Microsoft-Website http://www.microsoft.com/de-de (Artikelcode: KB822158).

Sie können das Übernehmen von vertrauenswürdigen Prozessen in der vertrauenswürdigen Zone aktivieren und deaktivieren.

Wenn die ausführbare Datei eines Prozesses beispielsweise durch ein Update verändert wird, schließt Kaspersky Embedded Systems Security den Prozess aus der Liste vertrauenswürdiger Prozesse aus.

Das Programm wendet den Wert des Dateipfads nicht auf einem geschützten Computer für die Kennzeichnung des Prozesses als vertrauenswürdig an. Der Dateipfad auf dem geschützten Computer wird nur für die Suche der Datei und die Berechnung ihrer Prüfsumme verwendet, sowie für das Informieren des Benutzers über die Quelle der ausführbaren Datei.

Backup-Operationen

Wird in den Aufgaben zum Echtzeit-Computerschutz verwendet.

Sie können den Schutz für Objekte, auf die beim Verschieben von Festplattendaten ins Backup auf externe Geräte zugegriffen wird, während der Backup-Operationen ausschalten. Kaspersky Embedded Systems Security untersucht Objekte, die vom Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden.

Ausnahmen

Gilt für die Aufgaben "Echtzeitschutz für Dateien" und "Untersuchung auf Befehl".

Sie können die Aufgaben auswählen, auf die Sie jede zur vertrauenswürdigen Zone hinzugefügte Ausnahme anwenden möchten. Darüber hinaus können Sie für jede einzelne Aufgabe in Kaspersky Embedded Systems Security Objekte von der Untersuchung ausschließen. Dies geschieht in den Einstellungen der Sicherheitsstufe der Aufgabe.

Sie können Objekte zur vertrauenswürdigen Zone entweder über ihrem Speicherort auf dem Computer, nach dem Namen bzw. der Namensmaske der in ihnen gefundenen Objekte, oder über beide Einstellungen hinzufügen.

Auf Grundlage der Ausnahme kann Kaspersky Embedded Systems Security in den festgelegten Aufgaben Objekte gemäß der folgenden Einstellungen überspringen:

- Angegebene Objekte, die nach Name oder Namensmaske in den angegebenen Bereichen des Computers erkannt werden können.
- Alle erkennbaren Objekte in den angegebenen Bereichen des Computers.
- Festgelegte gefundene Objekte nach Name oder Namensmaske in allen Schutzbereichen bzw. Untersuchungsbereichen

Vertrauenswürdige Zone über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie durch die Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und die vertrauenswürdige Zone für einen oder alle Computer im Netzwerk konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Programm über das Kaspersky Security Center verwalten

► *Um die vertrauenswürdige Zone über die Richtlinie für Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Richtlinien: <Name der Richtlinie>** den Abschnitt **Zusätzlich**.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Vertrauenswürdige Zone**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

Konfigurieren Sie die Richtlinie nach Bedarf.

Wenn ein Computer durch eine aktive Richtlinie von Kaspersky Security Center verwaltet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht über die Programmkonsole geändert werden.

Einstellungsfenster der vertrauenswürdigen Zone öffnen

► *Um die vertrauenswürdige Zone im Fenster "Eigenschaften des Programms" zu verwalten, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des geschützten Computers.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Computers aus.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
5. Wählen Sie im Abschnitt **Programme** die Option **Kaspersky Embedded Systems Security** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Einstellungen für Kaspersky Embedded Systems Security** wird geöffnet.
7. Wählen Sie den Abschnitt **Zusätzlich**.
8. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Vertrauenswürdige Zone**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

Konfigurieren Sie die vertrauenswürdige Zone nach Bedarf.

Einstellungen der vertrauenswürdigen Zone über das Verwaltungs-Plug-in anpassen

Die vertrauenswürdige Zone wird standardmäßig für alle neu erstellten Richtlinien und Aufgaben übernommen.

Um die Einstellungen der vertrauenswürdigen Zone anzupassen, gehen Sie wie folgt vor:

1. Zu überspringende Objekte festlegen (siehe Abschnitt "Ausnahme hinzufügen" auf Seite 475) mithilfe von Kaspersky Embedded Systems Security während der Aufgabenausführung auf der Registerkarte **Ausnahmen**.
2. Zu überspringende Prozesse festlegen (siehe Abschnitt "Vertrauenswürdige Prozesse hinzufügen" auf Seite 476) mithilfe von Kaspersky Embedded Systems Security während der Aufgabenuntersuchung auf der Registerkarte **Vertrauenswürdige Prozesse**.
3. Not-a-virus-Maske anwenden (siehe Abschnitt "Anwenden der Not-a-virus-Maske" auf Seite 479).

In diesem Abschnitt

Ausnahme hinzufügen

► *Um eine Ausnahme zur vertrauenswürdigen Zone über die Richtlinie für Kaspersky Security Center hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Vertrauenswürdige Zone (siehe Abschnitt "Programm über das Kaspersky Security Center verwalten" auf Seite** 473**).**
2. Geben Sie auf der Registerkarte **Ausnahmen** die Objekte an, die Kaspersky Embedded Systems Security bei der Untersuchung überspringen soll:
   - Klicken Sie auf die Schaltfläche **Empfohlene Ausnahmen hinzufügen**, wenn Sie die empfohlenen Ausnahmen hinzufügen möchten.

     Bei Anklicken dieser Schaltfläche werden der Liste mit den Ausnahmen von Microsoft empfohlene Ausnahmen und von Kaspersky Lab empfohlene Ausnahmen hinzugefügt.
   - Um Ausnahmen zu importieren, klicken Sie auf **Import** und wählen Sie im folgenden Fenster die Dateien aus, die Kaspersky Embedded Systems Security als vertrauenswürdig betrachten soll.
   - Wenn Sie die Bedingungen, bei deren Vorliegen eine Datei als vertrauenswürdig eingestuft werden soll, manuell angeben möchten, klicken Sie auf **Hinzufügen**.

     Das Fenster **Ausnahme** wird geöffnet.
3. Geben Sie im Abschnitt **Das Objekt wird unter folgenden Bedingungen nicht untersucht**, die Objekte an, die Sie aus dem Schutzbereich bzw. Untersuchungsbereich ausschließen möchten, und die Objekte, die Sie aus der Erkennung ausschließen möchten:
   - Wenn Sie ein Objekt aus dem Schutzbereich oder Untersuchungsbereich ausschließen möchten, gehen Sie wie folgt vor:
     a. Aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt**.

        Fügt eine Datei, einen Ordner, ein Laufwerk oder eine Skriptdatei zu einer Ausnahme hinzu.

        Wenn das Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die festgelegten vordefinierten Bereiche, Dateien, Ordner, Laufwerke oder Skriptdateien während der Ausführung der Untersuchung unter Anwendung der Komponente von Kaspersky Embedded Systems Security, die im Abschnitt **Gültigkeitsbereich der Regel** ausgewählt ist.

        Das Kontrollkästchen ist standardmäßig deaktiviert.

     b. Klicken Sie auf die Schaltfläche **Ändern**.

        Das Fenster **Wählen Sie ein Objekt aus** wird geöffnet.

     c. Geben Sie das Objekt an, das Sie aus dem Untersuchungsbereich ausschließen möchten.

        Sie können die Sonderzeichen ? und * für die Angabe der Objekte verwenden.

     d. Klicken Sie auf **OK**.

     e. Aktivieren Sie das Kontrollkästchen **Auch für Unterordner übernehmen**, wenn Sie alle untergeordneten Dateien und Order des angegebenen Objekts vom Schutzbereich oder Untersuchungsbereich ausschließen möchten.
   - Wenn Sie den Namen eines erkennbaren Objekts angeben wollen:

a. Aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**.

Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen erkennbaren Objekte bei der Untersuchung.

Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security alle Objekte, die im Programm standardmäßig angegeben sind.

Das Kontrollkästchen ist standardmäßig deaktiviert.

b. Klicken Sie auf die Schaltfläche **Ändern**.

Das Fenster **Liste der gefundenen Objekte** wird geöffnet.

c. Geben Sie den Namen oder die Namensmaske des erkennbaren Objekts gemäß der Klassifizierung der Viren-Enzyklopädie an.

d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

e. Klicken Sie auf **OK**.

4. Aktivieren Sie im Abschnitt **Gültigkeitsbereich der Regel** die Kontrollkästchen neben den Namen der Aufgaben, auf die die Ausnahme angewendet werden soll.

Name der Aufgabe von Kaspersky Embedded Systems Security, in der die Regel angewendet wird.

5. Klicken Sie auf **OK**.

Die Ausnahme wird in der Liste in der Registerkarte **Ausnahmen** des Fensters **Vertrauenswürdige Zone** angezeigt.

Vertrauenswürdige Prozesse hinzufügen

► *Um einen oder mehrere Prozesse zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Vertrauenswürdige Zone** (siehe Abschnitt "Programm über das Kaspersky Security Center verwalten" auf Seite 473).
2. Wählen Sie die Registerkarte **Vertrauenswürdige Prozesse** aus.
3. Aktivieren Sie das Kontrollkästchen **Datei-Backup-Operationen nicht untersuchen**, um die Untersuchung von Lesevorgängen für Dateien zu überspringen.

Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung der Lesevorgänge für Dateien, wenn diese Vorgänge von den auf dem Computer installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security bei der Untersuchung die Lesevorgänge für Dateien, die von den auf dem Computer installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security bei der Untersuchung die Lesevorgänge für Dateien, die von den auf dem Computer installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**, um die Untersuchung von Dateivorgängen für vertrauenswürdige Prozesse zu überspringen.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung der Datei-Aktivität vertrauenswürdiger Prozesse.

   Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security bei der Untersuchung die Dateivorgänge vertrauenswürdiger Prozesse.

   Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security die Dateivorgänge vertrauenswürdiger Prozesse.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.
6. Wählen Sie aus dem Kontextmenü der Schaltfläche eine der Einstellungen aus:

   - **Mehrere Prozesse**.

     Nehmen Sie im nächsten Fenster **Hinzufügen von vertrauenswürdigen Prozessen** folgende Einstellungen vor:

     a. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den vollständigen Ordnerpfad, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

        Wenn diese Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

        Das Kontrollkästchen ist standardmäßig deaktiviert.

     b. **Datei-Hash zur Bestimmung der Vertrauenswürdigkeit des Prozesses verwenden**

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den Hashwert der ausgewählten Datei, um den Status der Vertrauenswürdigkeit 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.

        Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     c. Klicken Sie auf die Schaltfläche **Durchsuchen**, um Daten auf der Grundlage ausführbarer Prozesse hinzuzufügen.

     d. Wählen Sie im folgenden Fenster eine ausführbare Datei aus.

        Sie können jeweils nur eine ausführbare Datei hinzufügen. Wiederholen Sie die Schritte c-d, um weitere ausführbare Dateien hinzuzufügen.

     e. Klicken Sie auf die Schaltfläche **Prozesse**, um Daten auf der Grundlage laufender Prozesse hinzuzufügen.

     f. Wählen Sie im folgenden Fenster Prozesse aus. Um mehrere Prozesse auszuwählen, halten Sie die STRG-Taste gedrückt, während Sie auswählen.

     g. Klicken Sie auf **OK**.

Das Benutzerkonto, mit dessen Berechtigungen die Aufgabe zum Echtzeitschutz für Dateien gestartet wird, muss auf dem Computer, auf dem Kaspersky Embedded Systems Security installiert ist, über Administratorrechte verfügen, damit die Liste der aktiven Prozesse angezeigt werden kann. Sie können die Prozesse in der Liste der aktiven Prozesse nach Dateinamen, Prozess-ID (PID) oder Pfad der ausführbaren Prozessdatei auf dem lokalen Computer sortieren. Beachten Sie, dass Sie laufende Prozesse auswählen können, indem Sie auf die Schaltfläche **Prozesse** klicken und nur die Programmkonsole auf einem lokalen Computer oder in den angegebenen Host-Einstellungen über Kaspersky Security Center verwenden.

- **Ein Prozess auf der Grundlage von Dateiname und Pfad.**

  Gehen Sie im nächsten Fenster **Hinzufügen eines Prozesses** wie folgt vor:

  a. Geben Sie einen Pfad zur ausführbaren Datei (inklusive Dateiname) an.

  b. Klicken Sie auf **OK**.

- **Ein Prozess auf der Grundlage von Objekteigenschaften.**

  Nehmen Sie im nächsten Fenster **Hinzufügen eines vertrauenswürdigen Prozesses** folgende Einstellungen vor:

  a. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie einen Prozess aus.

  b. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den vollständigen Ordnerpfad, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

     Wenn diese Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

  c. **Datei-Hash zur Bestimmung der Vertrauenswürdigkeit des Prozesses verwenden**

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den Hashwert der ausgewählten Datei, um den Status der Vertrauenswürdigkeit 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.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  d. Klicken Sie auf **OK**.

  Um den ausgewählten Prozess zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, muss mindestens ein Kriterium für Vertrauenswürdigkeit ausgewählt sein.

7. Klicken Sie im Fenster **Vertrauenswürdige Prozesse hinzufügen** auf die Schaltfläche **OK**.

Die gewählte Datei bzw. der Prozess wird im Fenster **Vertrauenswürdige Zone** zur Liste der vertrauenswürdigen Prozesse hinzugefügt.

Anwenden der Not-a-virus-Maske

Die Not-a-virus-Maske erlaubt es, während der Untersuchung legitime Softwaredateien und Webressourcen, die als schädlich eingestuft werden, zu überspringen. Die Maske wirkt sich auf folgende Aufgaben aus:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl

Wenn die Maske nicht zur Liste mit Ausnahmen hinzugefügt wird, wendet Kaspersky Embedded Systems Security die Aktion an, die in den Aufgabeneinstellungen der Software, die zu dieser Kategorie gehört, festgelegt ist.

► *Um die Not-a-virus-Maske zu verwenden, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Vertrauenswürdige Zone** (siehe Abschnitt "Programm über das Kaspersky Security Center verwalten" auf Seite 473).
2. Scrollen Sie auf der Registerkarte **Ausnahmen** in der Spalte **Zu erkennende Objekte** in der Liste nach unten und wählen Sie die Zeile mit dem Wert **not-a-virus:*** aus, wenn das Kontrollkästchen deaktiviert ist.
3. Klicken Sie auf **OK**.

Die neue Konfiguration wird übernommen.

Vertrauenswürdige Zone über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie durch die Benutzeroberfläche der Programmkonsole navigieren und die vertrauenswürdige Zone auf einem lokalen Computer konfigurieren.

In diesem Abschnitt

Vertrauenswürdige Zone für Aufgaben in der Programmkonsole übernehmen

Die vertrauenswürdige Zone wird standardmäßig in der Aufgabe "Echtzeitschutz für Dateien", in vom Benutzer neu erstellten Aufgaben zur Untersuchung auf Befehl sowie in allen Systemaufgaben zur Untersuchung auf Befehl angewendet. Eine Ausnahme bildet die Aufgabe zur Untersuchung von Quarantäne-Objekten.

Nachdem die vertrauenswürdige Zone aktiviert bzw. deaktiviert wurde, werden die für sie festgelegten Ausnahmen in den laufenden Aufgaben sofort wirksam bzw. unwirksam.

► *Um die Übernahme der vertrauenswürdigen Zone für die Aufgaben von Kaspersky Embedded Systems Security zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü der Aufgabe, für die Sie die Verwendung der vertrauenswürdigen Zone anpassen möchten.

2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

3. Wählen Sie im nächsten Fenster auf der Registerkarte **Allgemein** eine der folgenden Aktionen aus:

   - Wenn Sie die vertrauenswürdige Zone in der Aufgabe übernehmen möchten, aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**.
   - Wenn Sie die Übernahme der vertrauenswürdige Zone in der Aufgabe deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**.

4. Wenn Sie die Einstellungen der vertrauenswürdigen Zone anpassen möchten, klicken Sie auf den Link im Namen des Kontrollkästchens **Vertrauenswürdige Zone anwenden**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

5. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**, um die Änderungen zu speichern.

Einstellungen der vertrauenswürdigen Zone in der Programmkonsole konfigurieren

Um die Einstellungen der vertrauenswürdigen Zone anzupassen, gehen Sie wie folgt vor:

1. Zu überspringende Objekte festlegen (siehe Abschnitt "Ausnahme zur vertrauenswürdigen Zone hinzufügen" auf Seite 480), mithilfe von Kaspersky Embedded Systems Security während der Aufgabenausführung auf der Registerkarte **Ausnahmen**.
2. Zu überspringende Prozesse festlegen (siehe Abschnitt "Vertrauenswürdige Prozesse " auf Seite 482) mithilfe von Kaspersky Embedded Systems Security während der Aufgabenuntersuchung auf der Registerkarte **Vertrauenswürdige Prozesse**.
3. Vertrauenswürdige Zone für die Programmaufgaben übernehmen (siehe Abschnitt "Vertrauenswürdige Zone für Aufgaben in der Programmkonsole übernehmen" auf Seite 479).
4. Not-a-virus-Maske anwenden (siehe Abschnitt "Anwenden der Not-a-virus-Maske" auf Seite 485).

In diesem Abschnitt

Ausnahme zur vertrauenswürdigen Zone hinzufügen

► *Um eine Ausnahme über die Programmkonsole manuell zur vertrauenswürdigen Zone hinzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
2. Wählen Sie die Menüoption **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

3. Wählen Sie die Registerkarte **Ausnahmen** aus.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Ausnahme** wird geöffnet.
5. Geben Sie im Abschnitt **Das Objekt wird unter folgenden Bedingungen nicht untersucht**, die Objekte an, die Sie aus dem Schutzbereich bzw. Untersuchungsbereich ausschließen möchten, und die Objekte, die Sie aus der Erkennung ausschließen möchten:

   - Wenn Sie ein Objekt aus dem Schutzbereich oder Untersuchungsbereich ausschließen möchten, gehen Sie wie folgt vor:

     a. Aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt**.

        Fügt eine Datei, einen Ordner, ein Laufwerk oder eine Skriptdatei zu einer Ausnahme hinzu.

        Wenn das Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die festgelegten vordefinierten Bereiche, Dateien, Ordner, Laufwerke oder Skriptdateien während der Ausführung der Untersuchung unter Anwendung der Komponente von Kaspersky Embedded Systems Security, die im Abschnitt **Gültigkeitsbereich der Regel** ausgewählt ist.

        Das Kontrollkästchen ist standardmäßig deaktiviert.

     b. Klicken Sie auf die Schaltfläche **Ändern**.

        Das Fenster **Wählen Sie ein Objekt aus** wird geöffnet.

     c. Geben Sie das Objekt an, das Sie aus dem Untersuchungsbereich ausschließen möchten.

        > Sie können die Sonderzeichen ? und * für die Angabe der Objekte verwenden.

     d. Klicken Sie auf **OK**.

     e. Aktivieren Sie das Kontrollkästchen **Auch für Unterordner übernehmen**, wenn Sie alle untergeordneten Dateien und Order des angegebenen Objekts vom Schutzbereich oder Untersuchungsbereich ausschließen möchten.

   - Wenn Sie den Namen eines erkennbaren Objekts angeben wollen:

     a. Aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**.

        Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie.

        Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security die angegebenen erkennbaren Objekte bei der Untersuchung.

        Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security alle Objekte, die im Programm standardmäßig angegeben sind.

        Das Kontrollkästchen ist standardmäßig deaktiviert.

     b. Klicken Sie auf die Schaltfläche **Ändern**.

        Das Fenster **Liste der gefundenen Objekte** wird geöffnet.

     c. Geben Sie den Namen oder die Namensmaske des erkennbaren Objekts gemäß der Klassifizierung der Viren-Enzyklopädie an.

d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

e. Klicken Sie auf **OK**.

6. Aktivieren Sie im Abschnitt **Gültigkeitsbereich der Regel** die Kontrollkästchen neben den Namen der Aufgaben, auf die die Ausnahme angewendet werden soll.

   Name der Aufgabe von Kaspersky Embedded Systems Security, in der die Regel angewendet wird.

7. Klicken Sie auf **OK**.

Die Ausnahme wird in der Liste in der Registerkarte **Ausnahmen** des Fensters **Vertrauenswürdige Zone** angezeigt.

Vertrauenswürdige Prozesse

Ein Prozess kann der Liste der vertrauenswürdigen Prozesse auf zwei Arten hinzugefügt werden:

- Prozess aus der Liste der Prozesse auswählen, die auf dem geschützten Computer aktiv sind.
- Die ausführbare Datei des Prozesses auswählen, unabhängig davon, ob der Prozess gerade aktiv ist oder nicht.

Wenn die ausführbare Datei eines Prozesses verändert wird, löscht Kaspersky Embedded Systems Security den Prozess aus der Liste der vertrauenswürdigen Prozesse.

► *Um einen oder mehrere Prozesse zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
2. Wählen Sie die Menüoption **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
3. Wählen Sie die Registerkarte **Vertrauenswürdige Prozesse** aus.
4. Aktivieren Sie das Kontrollkästchen **Datei-Backup-Operationen nicht untersuchen**, um die Untersuchung von Lesevorgängen für Dateien zu überspringen.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung der Lesevorgänge für Dateien, wenn diese Vorgänge von den auf dem Computer installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

   Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security bei der Untersuchung die Lesevorgänge für Dateien, die von den auf dem Computer installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

   Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security bei der Untersuchung die Lesevorgänge für Dateien, die von den auf dem Computer installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

5. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**, um die Untersuchung von Dateivorgängen für vertrauenswürdige Prozesse zu überspringen.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung der Datei-Aktivität vertrauenswürdiger Prozesse.

   Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security bei der Untersuchung die Dateivorgänge vertrauenswürdiger Prozesse.

   Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security die Dateivorgänge vertrauenswürdiger Prozesse.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

6. Klicken Sie auf die Schaltfläche **Hinzufügen**.
7. Wählen Sie aus dem Kontextmenü der Schaltfläche eine der Einstellungen aus:

   - **Mehrere Prozesse**.

     Nehmen Sie im nächsten Fenster **Hinzufügen von vertrauenswürdigen Prozessen** folgende Einstellungen vor:

     a. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den vollständigen Ordnerpfad, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

        Wenn diese Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

        Das Kontrollkästchen ist standardmäßig deaktiviert.

     b. **Datei-Hash zur Bestimmung der Vertrauenswürdigkeit des Prozesses verwenden**

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den Hashwert der ausgewählten Datei, um den Status der Vertrauenswürdigkeit 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.

        Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     c. Klicken Sie auf die Schaltfläche **Durchsuchen**, um Daten auf der Grundlage ausführbarer Prozesse hinzuzufügen.

     d. Wählen Sie im folgenden Fenster eine ausführbare Datei aus.

        Sie können jeweils nur eine ausführbare Datei hinzufügen. Wiederholen Sie die Schritte c-d, um weitere ausführbare Dateien hinzuzufügen.

     e. Klicken Sie auf die Schaltfläche **Prozesse**, um Daten auf der Grundlage laufender Prozesse hinzuzufügen.

     f. Wählen Sie im folgenden Fenster Prozesse aus. Um mehrere Prozesse auszuwählen, halten Sie die STRG-Taste gedrückt, während Sie auswählen.

     g. Klicken Sie auf **OK**.

Das Benutzerkonto, mit dessen Berechtigungen die Aufgabe zum Echtzeitschutz für Dateien gestartet wird, muss auf dem Computer, auf dem Kaspersky Embedded Systems Security installiert ist, über Administratorrechte verfügen, damit die Liste der aktiven Prozesse angezeigt werden kann. Sie können die Prozesse in der Liste der aktiven Prozesse nach Dateinamen, Prozess-ID (PID) oder Pfad der ausführbaren Prozessdatei auf dem lokalen Computer sortieren. Beachten Sie, dass Sie laufende Prozesse auswählen können, indem Sie auf die Schaltfläche **Prozesse** klicken und nur die Programmkonsole auf einem lokalen Computer oder in den angegebenen Host-Einstellungen über Kaspersky Security Center verwenden.

- **Ein Prozess auf der Grundlage von Dateiname und Pfad.**

  Gehen Sie im nächsten Fenster **Hinzufügen eines Prozesses** wie folgt vor:

  a. Geben Sie einen Pfad zur ausführbaren Datei (inklusive Dateiname) an.

  b. Klicken Sie auf **OK**.

- **Ein Prozess auf der Grundlage von Objekteigenschaften.**

  Nehmen Sie im nächsten Fenster **Hinzufügen eines vertrauenswürdigen Prozesses** folgende Einstellungen vor:

  a. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie einen Prozess aus.

  b. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den vollständigen Ordnerpfad, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

     Wenn diese Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad nicht verwendet, um zu bestimmen, ob der Prozess vertrauenswürdig ist.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

  c. **Datei-Hash zur Bestimmung der Vertrauenswürdigkeit des Prozesses verwenden**

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security den Hashwert der ausgewählten Datei, um den Status der Vertrauenswürdigkeit 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.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  d. Klicken Sie auf **OK**.

  Um den ausgewählten Prozess zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, muss mindestens ein Kriterium für Vertrauenswürdigkeit ausgewählt sein.

8. Klicken Sie im Fenster **Vertrauenswürdige Prozesse hinzufügen** auf die Schaltfläche **OK**.

Die gewählte Datei bzw. der Prozess wird im Fenster **Vertrauenswürdige Zone** zur Liste der vertrauenswürdigen Prozesse hinzugefügt.

Anwenden der Not-a-virus-Maske

Die Not-a-virus-Maske erlaubt es, während der Untersuchung legitime Softwaredateien und Webressourcen, die als schädlich eingestuft werden, zu überspringen. Die Maske wirkt sich auf folgende Aufgaben aus:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl

Wenn die Maske nicht zur Liste mit Ausnahmen hinzugefügt wird, wendet Kaspersky Embedded Systems Security die Aktion an, die in den Aufgabeneinstellungen der Software oder der Webressource, die zu dieser Kategorie gehört, festgelegt ist.

► *Um die Not-a-virus-Maske zu verwenden, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.
2. Wählen Sie die Menüoption **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
3. Wählen Sie die Registerkarte **Ausnahmen** aus.
4. Scrollen Sie in der Liste nach unten und wählen Sie die Zeile mit dem Wert **not-a-virus:*** aus, wenn das Kontrollkästchen deaktiviert ist.
5. Klicken Sie auf **OK**.

Die neue Konfiguration wird übernommen.

Exploit-Prävention

Dieser Abschnitt enthält eine Anleitung für die Konfiguration des Schutzes des Prozess-Speichers vor der Ausnutzung von Schwachstellen.

In diesem Kapitel

Über die Exploit-Prävention

Kaspersky Embedded Systems Security bietet eine Möglichkeit zum Schutz des Prozess-Speichers vor Exploits. Diese Funktion ist in der Komponente "Exploit-Prävention" implementiert. Sie können den Status der Aktivität der Komponente ändern und die Schutzeinstellungen des Prozess-Speichers vor der Ausnutzung von Schwachstellen anpassen.

Die Komponente schützt den Prozess-Speicher vor Exploits mithilfe der Einschleusung eines externen Prozess-Schutz-Agenten (im Weiteren "Agent") in den geschützten Prozess.

Der externe Schutz-Agent ist ein dynamisch ladendes Modul von Kaspersky Embedded Systems Security, das in die geschützten Prozesse eingeschleust 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 wenn ein Prozess aus der Liste der geschützten Prozesse entfernt wurde, kann der Agent nur dann aus ihm entladen werden, wenn der Prozess neu gestartet wird.

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 der Computer 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

Kaspersky Security Exploit Prevention Service

Um eine möglichst effektive Nutzung der Funktionen der Komponente "Exploit-Prävention" zu gewährleisten, muss auf dem geschützten Computer Kaspersky Security Exploit Prevention Service vorhanden sein. Dieser Dienst ist zusammen mit der Komponente "Exploit-Prävention" Bestandteil der empfohlenen Installation. Während der Installation des Dienstes auf dem geschützten Computer wird der Prozess "kavfswh" erstellt und gestartet. Auf diese Art werden Informationen über geschützte Prozesse von der Komponente an den Security Agenten gesendet

Nach dem Beenden von Kaspersky Security Exploit Prevention Service schützt Kaspersky Embedded Systems Security auch weiterhin die Prozesse, die zur Liste der geschützten Prozesse hinzugefügt wurden. Darüber hinaus wird das Programm in neu hinzugefügte Prozesse geladen und wendet alle verfügbaren Verfahren zur Exploit-Prävention an, um den Prozess-Speicher zu schützen.

Wenn Ihr Computer unter dem Betriebssystem Windows 10 oder höher läuft, wird das Programm nach dem Beenden von Kaspersky Security Exploit Prevention Service die Prozesse und den Prozess-Speicher nicht länger schützen.

Sollte Kaspersky Security Exploit Prevention Service beendet werden, erhält das Programm nicht länger Daten zu Ereignissen, die für geschützte Prozesse auftreten (darunter auch Daten über Exploit-Angriffe und das Beenden von Prozessen). Der Agent kann auch nicht länger Daten über neue Schutzeinstellungen und über das Hinzufügen neuer Prozesse zur Liste der geschützten Prozesse erhalten.

Modus der Exploit-Prävention

Sie können die Aktionen zur Minderung der Risiken einer Ausnutzung von Schwachstellen in geschützten Prozessen anpassen, indem Sie einen von zwei Modi auswählen:

- **Bei Exploit beenden**: Wenden Sie diesen Modus an, um den Prozess beim Versuch der Ausnutzung einer Schwachstelle zu beenden.

  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.

- **Nur informieren**: Wenden Sie diesen Modus an, um mithilfe von Ereignissen im Sicherheitsprotokoll Daten über Exploits in geschützten Prozessen zu erhalten.

  In diesem Modus protokolliert Kaspersky Embedded Systems Security alle Exploit-Versuche in Form von Ereignissen.

Exploit-Prävention über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Komponenteneinstellungen für einen oder alle Computer im Netzwerk konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Richtlinieneinstellungen für die Exploit-Prävention öffnen

► *Um die Einstellungen der Exploit-Prävention über die Richtlinie von Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
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.
5. Wählen Sie im nächsten Fenster **Richtlinien: <Name der Richtlinie>** den Abschnitt **Echtzeit-Computerschutz** aus.
6. Klicken Sie im Unterabschnitt **Exploit-Prävention** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Exploit-Prävention** wird geöffnet.

Konfigurieren Sie die Exploit-Prävention nach Bedarf.

Einstellungsfenster der Exploit-Prävention öffnen

► *Um das Fenster **Eigenschaften: <Servername>** zu öffnen, gehen Sie wie folgt vor:*

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des geschützten Computers.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Computers aus.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
5. Wählen Sie im Abschnitt **Programme** die Option **Kaspersky Embedded Systems Security** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Einstellungen für Kaspersky Embedded Systems Security** wird geöffnet.
7. Wählen Sie den Abschnitt **Echtzeit-Computerschutz** aus.
8. Klicken Sie im Unterabschnitt **Exploit-Prävention** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Exploit-Prävention** wird geöffnet.

Konfigurieren Sie die Exploit-Prävention nach Bedarf.

Einstellungen zum Schutz des Prozess-Speichers anpassen

► *Um die Einstellungen zum Schutz des Prozess-Speichers für die Prozesse anzupassen, die zur Liste mit geschützten Prozessen hinzugefügt wurden, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Exploit-Prävention** (siehe Abschnitt "**Richtlinieneinstellungen für die Exploit-Prävention öffnen**" auf Seite 488).
2. Konfigurieren Sie im Block **Modus der Exploit-Prävention** die folgenden Einstellungen:
   - **Exploit von Prozessen mit Schwachstellen verhindern**.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Embedded Systems Security die Risiken der Ausnutzung von Schwachstellen von Prozessen, die sich in der Liste der geschützten Prozesse befinden.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Computer-Prozesse von Kaspersky Embedded Systems Security nicht vor Exploits geschützt.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - **Bei Exploit beenden**.

     In diesem Modus beendet Kaspersky Embedded Systems Security einen geschützten Prozess beim Fund eines Exploit-Versuchs, wenn ein aktives Verfahren zur Risikominderung angewendet wird.

- **Nur informieren**.

  In diesem Modus benachrichtigt Kaspersky Embedded Systems Security anhand eines Terminalfensters über Exploits. Der missbräuchlich verwendete Prozess wird auch weiterhin ausgeführt.

  Wenn Kaspersky Embedded Systems Security während der Ausführung des Programms im Modus **Bei Exploit beenden** einen Exploit in einem kritischen Prozess findet, wechselt die Komponente zwangsläufig in den Modus **Nur informieren**.

3. Konfigurieren Sie im Block **Aktionen zur Vorbeugung** die folgenden Einstellungen:

   - **Mittels Terminaldienst über missbräuchlich verwendete Prozesse benachrichtigen.**

     Wenn dieses Kontrollkästchen aktiviert ist, zeigt Kaspersky Embedded Systems Security ein Terminalfenster mit einer Beschreibung der Ursache für das Auslösen des Schutzes und der Angabe des Prozesses, in dem der Exploit-Versuch gefunden wurde, an.

     Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Embedded Systems Security kein Terminalfenster an, wenn ein Exploit-Versuch gefunden oder ein missbräuchlich verwendeter Prozess beendet wurde. Das Terminalfenster wird unabhängig vom Status von Kaspersky Security Exploit Prevention Service angezeigt. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - **Exploit von Prozessen mit Schwachstellen auch verhindern, wenn Kaspersky Security Service deaktiviert ist**.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Embedded Systems Security die Risiken der Ausnutzung von Schwachstellen von bereits gestarteten Prozessen unabhängig davon, ob der Dienst Kaspersky Security Service läuft. Kaspersky Embedded Systems Security schützt keine Prozesse, die nach dem Beenden von Kaspersky Security Service hinzugefügt wurden. Nach dem Start des Dienstes wird die Minderung der Exploit-Risiken für alle Prozesse beendet.

     Wenn dieses Kontrollkästchen deaktiviert ist, schützt Kaspersky Embedded Systems Security keine Prozesse vor Exploits, wenn Kaspersky Security Service beendet wurde.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

4. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security speichert und übernimmt die angepassten Einstellungen zum Schutz des Prozess-Speichers.

Hinzufügen eines Prozesses zum Schutz

Die Komponente "Exploit-Prävention" schützt einige Prozesse standardmäßig. Sie können diesen Prozess vom Schutzbereich ausschließen, indem Sie die entsprechenden Kontrollkästchen in der Liste deaktivieren.

► *Um einen Prozess zur Liste mit geschützten Prozessen hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Exploit-Prävention** (siehe Abschnitt "**Richtlinieneinstellungen für die Exploit-Prävention öffnen**" auf Seite 488).
2. Klicken Sie auf der Registerkarte **Geschützte Prozesse** auf die Schaltfläche **Durchsuchen**.

   Das Microsoft-Windows-Explorer-Fenster wird geöffnet.
3. Wählen Sie den Prozess aus, den Sie zur Liste hinzufügen möchten.

4. Klicken Sie auf **Öffnen**.

   Der Prozessname wird in der Zeile angezeigt.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der angegebene Prozess wird zur Liste der geschützten Prozesse hinzugefügt.

6. Wählen Sie den hinzugefügten Prozess aus.
7. Klicken Sie auf **Verfahren zur Exploit-Prävention angeben**.

   Das Fenster **Verfahren zur Exploit-Prävention** wird geöffnet.

8. Wählen Sie eine der Varianten zur Anwendung der Verfahren zur Risikominderung aus:

   - **Alle verfügbaren Methoden zur Exploit-Prävention anwenden**.

     Wenn diese Einstellung ausgewählt ist, kann die Liste nicht geändert werden. Alle für einen Prozess verfügbaren Techniken werden standardmäßig angewendet.

   - **Folgende Verfahren zur Exploit-Prävention anwenden**.

     Wenn diese Variante ausgewählt ist, können Sie die Liste der angewendeten Verfahren zur Risikominderung bearbeiten:

     a. Aktivieren Sie die Kontrollkästchen der Verfahren, die Sie zum Schutz des ausgewählten Prozesses anwenden möchten.

     b. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Attack Surface Reduction anwenden**.

9. Passen Sie die Einstellungen der Technik "Attack Surface Reduction" an:

   - Geben Sie die Namen der Module, die nicht aus dem geschützten Prozess gestartet werden dürfen, im Feld **Module verbieten** ein.
   - Aktivieren Sie im Feld **Module nicht verbieten, wenn der Start in folgender Netzwerkzone erfolgt** die Kontrollkästchen neben jenen Optionen, in denen Sie den Start von Modulen erlauben möchten:
     - Internet
     - Lokales Intranet
     - Vertrauenswürdige Websites
     - Websites mit eingeschränktem Zugriff
     - Computer

     Diese Einstellungen gelten nur für den Internet Explorer®.

10. Klicken Sie auf **OK**.

Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Exploit-Prävention über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und die Komponenteneinstellungen auf einem lokalen Computer konfigurieren.

In diesem Abschnitt

Navigation

Erfahren Sie, wie Sie über die Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

In diesem Abschnitt

Allgemeine Einstellungen der Exploit-Prävention öffnen

► *Um das Fenster **Einstellungen zur Exploit-Prävention** zu öffnen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security**.
2. Öffnen Sie das Kontextmenü und wählen Sie die Option **Exploit-Prävention: Allgemeine Schutzeinstellungen**.

   Das Fenster **Einstellungen zur Exploit-Prävention** wird geöffnet.

Passen Sie die allgemeinen Einstellungen für die Exploit-Prävention nach Bedarf an.

Einstellungen der Exploit-Prävention für den Schutz von Prozessen öffnen

► *Um das Fenster **Einstellungen zum Schutz von Prozessen** zu öffnen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security**.
2. Öffnen Sie das Kontextmenü und wählen Sie die Option **Exploit-Prävention: Einstellungen für den Schutz von Prozessen**.

   Das Fenster **Einstellungen zum Schutz von Prozessen** wird geöffnet.

Passen Sie die Einstellungen der Exploit-Prävention für den Schutz von Prozessen nach Bedarf an.

Einstellungen zum Schutz des Prozess-Speichers anpassen

► *Um einen Prozess zur Liste mit geschützten Prozessen hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Einstellungsfenster der Exploit-Prävention.
2. Konfigurieren Sie im Block **Modus der Exploit-Prävention** die folgenden Einstellungen:
   - **Exploit von Prozessen mit Schwachstellen verhindern**.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Embedded Systems Security die Risiken der Ausnutzung von Schwachstellen von Prozessen, die sich in der Liste der geschützten Prozesse befinden.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Computer-Prozesse von Kaspersky Embedded Systems Security nicht vor Exploits geschützt.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - **Bei Exploit beenden**.

     In diesem Modus beendet Kaspersky Embedded Systems Security einen geschützten Prozess beim Fund eines Exploit-Versuchs, wenn ein aktives Verfahren zur Risikominderung angewendet wird.

   - **Nur informieren**.

     In diesem Modus benachrichtigt Kaspersky Embedded Systems Security anhand eines Terminalfensters über Exploits. Der missbräuchlich verwendete Prozess wird auch weiterhin ausgeführt.

     Wenn Kaspersky Embedded Systems Security während der Ausführung des Programms im Modus **Bei Exploit beenden** einen Exploit in einem kritischen Prozess findet, wechselt die Komponente zwangsläufig in den Modus **Nur informieren**.
3. Konfigurieren Sie im Block **Aktionen zur Vorbeugung** die folgenden Einstellungen:
   - **Mittels Terminaldienst über missbräuchlich verwendete Prozesse benachrichtigen.**

     Wenn dieses Kontrollkästchen aktiviert ist, zeigt Kaspersky Embedded Systems Security ein Terminalfenster mit einer Beschreibung der Ursache für das Auslösen des Schutzes und der Angabe des Prozesses, in dem der Exploit-Versuch gefunden wurde, an.

     Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Embedded Systems Security kein Terminalfenster an, wenn ein Exploit-Versuch gefunden oder ein missbräuchlich verwendeter Prozess beendet wurde. Das Terminalfenster wird unabhängig vom Status von Kaspersky Security Exploit Prevention Service angezeigt. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - **Exploit von Prozessen mit Schwachstellen auch verhindern, wenn Kaspersky Security Service deaktiviert ist**.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Embedded Systems Security die Risiken der Ausnutzung von Schwachstellen von bereits gestarteten Prozessen unabhängig davon, ob der Dienst Kaspersky Security Service läuft. Kaspersky Embedded Systems Security schützt keine Prozesse, die nach dem Beenden von Kaspersky Security Service hinzugefügt wurden. Nach dem Start des Dienstes wird die Minderung der Exploit-Risiken für alle Prozesse beendet.

     Wenn dieses Kontrollkästchen deaktiviert ist, schützt Kaspersky Embedded Systems Security keine Prozesse vor Exploits, wenn Kaspersky Security Service beendet wurde.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
4. Klicken Sie im Fenster **Einstellungen zur Exploit-Prävention** auf **OK**.

Kaspersky Embedded Systems Security speichert und übernimmt die angepassten Einstellungen zum Schutz des Prozess-Speichers.

Hinzufügen eines Prozesses zum Schutz

Die Komponente "Exploit-Prävention" schützt einige Prozesse standardmäßig. Prozesse in der Liste der geschützten Prozesse, die Sie nicht schützen wollen, können Sie deaktivieren.

► *Um einen Prozess zur Liste mit geschützten Prozessen hinzuzufügen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Einstellungsfenster für den Schutz von Prozessen.
2. Um einen Prozess hinzuzufügen, um sie vor Missbrauch zu schützen und die möglichen Auswirkungen des Exploits zu beschränken, gehen Sie wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Durchsuchen**.

      Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.

   b. Wählen Sie im folgenden Fenster den Prozess aus, den Sie zur Liste hinzufügen möchten.
   c. Klicken Sie auf **Öffnen**.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Der angegebene Prozess wird zur Liste der geschützten Prozesse hinzugefügt.
3. Wählen Sie einen hinzugefügten Prozess in der Liste aus.
4. Auf der Registerkarte **Einstellungen zum Schutz des Prozesses** wird die aktuelle Konfiguration angezeigt:
   - **Prozessname**.
   - **Wird ausgeführt**.
   - **Angewendete Verfahren zur Exploit-Prävention**.
   - **Einstellungen für Attack Surface Reduction (ASR)**.
5. Um die auf den gegebenen Prozess angewendeten Verfahren zur Exploit-Prävention zu bearbeiten, wählen Sie die Registerkarte **Verfahren zur Exploit-Prävention**.
6. Wählen Sie eine der Varianten zur Anwendung der Verfahren zur Risikominderung aus:
   - **Alle verfügbaren Methoden zur Exploit-Prävention anwenden**.

     Wenn diese Einstellung ausgewählt ist, kann die Liste nicht geändert werden. Alle für einen Prozess verfügbaren Techniken werden standardmäßig angewendet.
   - **Angeführte Verfahren zur Exploit-Prävention für den Prozess anwenden**.

     Wenn diese Variante ausgewählt ist, können Sie die Liste der angewendeten Verfahren zur Risikominderung bearbeiten:

     a. Aktivieren Sie die Kontrollkästchen der Verfahren, die Sie zum Schutz des ausgewählten Prozesses anwenden möchten.

7. Passen Sie die Einstellungen der Technik "Attack Surface Reduction" an:
   - Geben Sie die Namen der Module, die nicht aus dem geschützten Prozess gestartet werden dürfen, im Feld **Module verbieten** ein.
   - Aktivieren Sie im Feld **Module nicht verbieten, wenn der Start in folgender Netzwerkzone erfolgt** die Kontrollkästchen neben jenen Optionen, in denen Sie den Start von Modulen erlauben möchten:
     - Internet
     - Lokales Intranet
     - Vertrauenswürdige Websites
     - Websites mit eingeschränktem Zugriff
     - Computer

     Diese Einstellungen gelten nur für den Internet Explorer®.
8. Klicken Sie auf **OK**.

Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Exploit-Präventionstechniken

Tabelle 62. Exploit-Präventionstechniken

Verfahren zur Exploit-Prävention	Beschreibung
Data Execution Prevention (DEP)	Verhinderung einer Ausführung von Daten – Verbot der Ausführung eines zufälligen Codes im geschützten Speicherbereich.
Address Space Layout Randomization (ASLR)	Zufallsgestaltung der Datenstruktur im Adressraum des Prozesses.
Structured Exception Handler Overwrite Protection (SEHOP)	Auswechslung des Eintrags in der Struktur der Ausnahmen oder Auswechslung des Ausnahmehandlers.
Null Page Allocation	Verhinderung der Umorientierung des Nullregisters.
LoadLibrary Network Call Check (Anti ROP)	Schutz vor dem Download dynamischer Bibliotheken von Netzwerkpfaden.
Executable Stack (Anti ROP)	Verbot der unbefugten Verwendung des Stapelbereichs.
Anti RET Check (Anti ROP)	Untersuchung des sicheren Aufrufs von Funktionen durch eine CALL-Anweisung.
Anti Stack Pivoting (Anti ROP)	Schutz vor einer Verschiebung des ESP-Registerstapels zur exploitierten Adresse.
Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Schutz vor Lesezugriff auf die Exportadresstabelle (Export Address Table) für die Module kernel32.dll, kernelbase.dll, ntdll.dll

Verfahren zur Exploit-Prävention	Beschreibung
Heapspray Allocation (Heapspray)	Schutz vor Speicherbelegung unter Verwendung von schädlichem Code.
Execution Flow Simulation (Anti Return Oriented Programming)	Erkennen verdächtiger Anweisungsketten (mögliches ROP-Gadget) in der Komponente Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Schutz vor der Ausweitung von Privilegien durch eine Schwachstelle im AFD-Treiber (Ausführen eines zufälligen Codes auf dem Nullring durch den Anruf von QueryIntervalProfile).
Attack Surface Reduction (ASR)	Blockierung des Starts von Modulen mit etwaigen Schwachstellen über den geschützten Prozess.
Anti Process Hollowing (Hollowing)	Schutz gegen das Erstellen und Ausführen von schädlichen Kopien vertrauenswürdiger Prozesse.
Anti AtomBombing (APC)	Globaler Atomtabellen-Exploit über Asynchrone Prozeduraufrufe (APC).
Anti CreateRemoteThread (RThreadLocal)	Ein anderer Prozess hat einen Thread in einem geschützten Prozess erstellt.
Anti CreateRemoteThread (RThreadRemote)	Ein geschützter Prozess hat einen Thread in einem anderen Prozess erstellt.

Integration mit Dritthersteller-Systemen

Dieser Abschnitt beschreibt die Integration von Kaspersky Embedded Systems Security mit Funktionen und Technologien von Drittherstellern.

In diesem Kapitel

Leistungskontrolle. Indikatoren in Kaspersky Embedded Systems Security

Dieser Abschnitt informiert über die Indikatoren von Kaspersky Embedded Systems Security: Leistungsindikatoren für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps.

In diesem Abschnitt

Leistungsindikatoren für das Programm Systemmonitor

Dieser Abschnitt enthält Informationen über Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows, die von Kaspersky Embedded Systems Security während der Installation registriert werden.

In diesem Abschnitt

Über Leistungsindikatoren in Kaspersky Embedded Systems Security

Die Komponente **Leistungsindikatoren** gehört zu den standardmäßig installierten Komponenten von Kaspersky Embedded Systems Security. Während der Installation registriert Kaspersky Embedded Systems Security seine Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows.

Mit den Indikatoren von Kaspersky Embedded Systems Security können Sie die Leistung des Programms bei der Ausführung von Echtzeitschutz-Aufgaben kontrollieren. Sie können Engstellen beim Zusammenwirken mit anderen Anwendungen und bei ungenügenden Ressourcen überwachen. Außerdem können Sie nicht so optimale Einstellungen von Kaspersky Embedded Systems Security und Abstürze diagnostizieren.

Sie können die Leistungsindikatoren für Kaspersky Embedded Systems Security aufrufen, indem Sie die Konsole **Optimierung** im Element **Administration** der Windows-Systemsteuerung öffnen.

Die folgenden Abschnitte erklären die Indikatoren, nennen die empfohlenen Intervalle für das Ablesen der Werte und entsprechende Grenzwerte. Außerdem werden Empfehlungen zur Konfiguration von Kaspersky Embedded Systems Security bei Grenzwertüberschreitungen gegeben.

Gesamtzahl der abgelehnten Anfragen

Tabelle 63. Gesamtzahl der abgelehnten Anfragen

Name	Gesamtzahl der abgelehnten Anfragen (Total number of requests denied)
Definition	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, deren Verarbeitungsanfragen von aktiven Prozessen durch Kaspersky Embedded Systems Security zurückgewiesen werden.
Ziel	Ein Indikator kann überwachen: • Qualitätsverluste beim Echtzeitschutz wegen hoher Belastung der Arbeitsprozesse von Kaspersky Embedded Systems Security • Unterbrechung des Echtzeitschutzes wegen Abweisungen vom File-Interception-Dispatcher

Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Summe der abgelehnten Anfragen für die Verarbeitung entspricht der Summe der übersprungenen Objekte Folgende Situationen sind abhängig vom "Verhalten" des Indikators möglich: • Der Indikator zeigt mehrere abgelehnte Anfrage im Laufe einer längeren Zeit: Alle Prozesse von Kaspersky Embedded Systems Security waren vollständig ausgelastet, deshalb konnte Kaspersky Embedded Systems Security die Objekte nicht untersuchen. Um das Überspringen von Objekten auszuschließen, erhöhen Sie die Menge an Programmprozessen für Aufgaben des Echtzeitschutzes. Sie können die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** von Kaspersky Embedded Systems Security verwenden. • 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 beim Öffnen. Kaspersky Embedded Systems Security neu starten

Gesamtzahl der übersprungenen Anfragen

Tabelle 64. Gesamtzahl der übersprungenen Anfragen

Name	Gesamtzahl der übersprungenen Anfragen (Total number of requests skipped).
Definition	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 vom File-Interception-Dispatcher überwachen.

Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Ein Indikatorwert, 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.

Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Tabelle 65. Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Name	Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden (Number of requests not processed due to lack of resources)
Definition	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 Objekte, deren Verarbeitungsanfragen vom File-Interceptor-Treiber zurückgewiesen werden.
Ziel	Der Indikator kann mögliche Qualitätsverluste des Echtzeitschutzes erkennen und beseitigen, die aufgrund nicht genügender Systemressourcen eintreten.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert ungleich Null ist, brauchen die Prozesse von Kaspersky Embedded Systems Security für die Anfragenbearbeitung einen größeren Arbeitsspeicher. Es ist möglich, dass es andere aktive Prozesse gibt, die den ganzen Arbeitsspeicher in Anspruch nehmen.

Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Tabelle 66. Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Name	Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden (Number of requests sent to be processed).
Definition	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 Computer zu überwachen.
Normalwert / Grenzwert	Der Indikatorwert kann schwanken, je nach Stufe der Dateiaktivität auf dem Computer.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Nein

Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

Tabelle 67. Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

Name	Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers (Average number of file interception dispatcher streams).
Definition	Anzahl der Datenströme des File-Interception-Dispatchers in einem Arbeitsprozess. Mittelwert für alle Prozesse, die momentan an Echtzeitschutz-Aufgaben beteiligt sind.
Ziel	Dieser Indikator erlaubt es, mögliche Qualitätsverluste des Echtzeitschutzes zu erkennen und zu beseitigen, die auf vollständige Auslastung der Prozesse von Kaspersky Embedded Systems Security zurückgehen.
Normalwert / Grenzwert	Variiert / 40.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	In jedem aktiven Prozess können bis zu 60 Datenströme des File-Interception-Dispatchers angelegt werden. Wenn sich der Indikatorwert der Zahl 60 nähert, besteht das Risiko, dass kein aktiver Prozess mehr die Verarbeitung einer in der Warteschlange stehenden Anfrage vom File-Interception-Treiber abnimmt und Kaspersky Embedded Systems Security überspringt das Objekt. Vergrößern Sie die Anzahl der Prozesse von Kaspersky Embedded Systems Security für die Aufgaben des Echtzeitschutzes. Sie können die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** von Kaspersky Embedded Systems Security verwenden.

Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Tabelle 68. Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Name	Maximale Anzahl der Datenströme des File-Interception-Dispatchers (Maximum number of file interception dispatcher streams)
Definition	Anzahl der Datenströme des File-Interception-Dispatchers in einem Arbeitsprozess. Höchstwert für alle Prozesse, die momentan an Echtzeitschutz-Aufgaben beteiligt sind.
Ziel	Der Indikator kann einen Produktivitätsverlust wegen ungleichmäßiger Belastungsverteilung in den ausgeführten Arbeitsprozessen erkennen und beseitigen.
Normalwert / Grenzwert	Variiert / 40.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Wert dieses Indikators dauerhaft und erheblich von dem Indikatorwert **Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers** abweicht, verteilt Kaspersky Embedded Systems Security die Belastung ungleichmäßig auf die ausführenden Prozesse. Kaspersky Embedded Systems Security neu starten

Anzahl der Elemente in der Warteschlange der infizierten Objekte

Tabelle 69. Anzahl der Elemente in der Warteschlange der infizierten Objekte

Name	Anzahl der Elemente in der Warteschlange der infizierten Objekte (Number of items in the infected object queue)
Definition	Anzahl der infizierten Objekte, die momentan auf die Verarbeitung (Desinfektion oder Löschen) warten.
Ziel	Ein Indikator kann überwachen: • Unterbrechung des Echtzeitschutzes wegen möglichen Abweisungen vom File-Interception-Dispatcher • 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 • Es steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Computerbelastung durch andere Anwendungen senken). • Es ist eine Virenepidemie eingetreten. Vom Eintreten einer Virenepidemie zeugt außerdem eine große Menge an gefundenen infizierten oder möglicherweise infizierten Objekten in der Aufgabe Echtzeitschutz für Dateien. Informationen über die Anzahl der gefundenen Objekte können Sie der Aufgabenstatistik oder dem Protokoll der Aufgabenausführung entnehmen.

Anzahl der pro Sekunde verarbeiteten Objekte

Tabelle 70. Anzahl der pro Sekunde verarbeiteten Objekte

Name	Anzahl der pro Sekunde verarbeiteten Objekte (Number of objects processed per second).
Definition	Anzahl der verarbeiteten Objekte geteilt durch die Zeit, in der diese Objekte verarbeitet wurden. Wird in gleichmäßigen Zeitabständen berechnet.
Ziel	Dieser Indikator zeigt das Tempo der Objektverarbeitung. So können Produktivitätsverluste des Computers erkannt und beseitigt werden, die wegen der Zuweisung zu geringer Prozessorzeit an die Arbeitsprozesse von Kaspersky Embedded Systems Security oder wegen Fehler bei der Ausführung von Kaspersky Embedded Systems Security eingetreten sind.
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 Computers durch Prozesse anderer Programme ab. Beobachten Sie längere Zeit das mittlere Anzeige-Niveau des Indikators. Wenn das Durchschnittsniveau des Indikators gesunken ist, kann diese auf eine der folgenden Situationen hinweisen: • Den aktiven Prozessen von Kaspersky Embedded Systems Security steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Computerbelastung durch andere Anwendungen senken). • Kaspersky Embedded Systems Security ist abgestürzt (mehrere Datenströme stehen still). Kaspersky Embedded Systems Security neu starten

SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zu den Indikatoren und Traps in Kaspersky Embedded Systems Security.

In diesem Abschnitt

Über SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security

Wenn Sie SNMP-Indikatoren und -Traps zu den Komponenten von Anti-Virus hinzugefügt haben, die installiert werden sollen, können Sie Indikatoren und Traps für Kaspersky Embedded Systems Security mithilfe des SNMP-Protokolls (Simple Network Management Protocol) anzeigen.

Um die Indikatoren und Traps für Kaspersky Embedded Systems Security am Administrator-Arbeitsplatz anzuzeigen, starten Sie auf dem geschützten Computer 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 eine Tabelle mit einer Beschreibung der Einstellungen der SNMP-Indikatoren von Kaspersky Embedded Systems Security.

In diesem Abschnitt

Leistungsindikatoren

Tabelle 71. Leistungsindikatoren

Indikatoren	Definition
currentRequestsAmount	Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden (auf Seite 500)
currentInfectedQueueLength	Anzahl der Elemente in der Warteschlange für infizierte Objekte (siehe Abschnitt "Anzahl der Elemente in der Warteschlange der infizierten Objekte" auf Seite 502)
currentObjectProcessingRate	Anzahl der pro Sekunde verarbeiteten Objekte (auf Seite 503)
currentWorkProcessesNumber	Aktuelle Anzahl von Arbeitsprozessen, die von Kaspersky Embedded Systems Security genutzt werden

Indikatoren für Quarantäne

Tabelle 72. Indikatoren für Quarantäne

Indikatoren	Definition
totalObjects	Anzahl der Objekte, die sich momentan im Quarantäne-Ordner befinden.
totalSuspiciousObjects	Anzahl der möglicherweise infizierten Objekte, die sich momentan im Quarantäne-Ordner befinden
currentStorageSize	Volumen der Daten im Quarantäne-Ordner (MB)

Backup-Indikatoren

Tabelle 73. Backup-Indikatoren

Indikatoren	Definition
currentBackupStorageSize	Volumen der Daten im Backup-Ordner (MB)

Allgemeine Indikatoren

Tabelle 74. Allgemeine Indikatoren

Indikatoren	Definition
lastCriticalAreasScanAge	Der seit der letzten vollständigen Untersuchung der wichtigen Computerbereiche vergangene Zeitraum (in Sekunden angegebener Zeitraum seit dem letzten Abschluss der *Aufgabe zur Untersuchung wichtiger Bereiche*)

Indikatoren	Definition
licenseExpirationDate	Gültigkeitsdauer der Lizenz. Wenn ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt wurden, wird die Gültigkeitsdauer der Lizenz des Reserveschlüssels angezeigt.
currentApplicationUptime	Ausführungszeit von Kaspersky Embedded Systems Security seit dem letzten Start, in Hundertstelsekunden
currentFileMonitorTaskStatus	Status der Aufgabe Echtzeitschutz für Dateien: **On** – wird ausgeführt; **Off** – wurde beendet oder angehalten.

Update-Indikatoren

Tabelle 75. Update-Indikatoren

Indikatoren	Definition
avBasesAge	"Alter" der Datenbanken (in Hundertstelsekunden angegebener Zeitraum zwischen Veröffentlichungsdatum der zuletzt installierten Datenbanken-Updates und dem gegenwärtigen Zeitpunkt).

Indikatoren für den Echtzeitschutz

Tabelle 76. Indikatoren für den Echtzeitschutz

Indikatoren	Definition
totalObjectsProcessed	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien untersuchten Objekte
totalInfectedObjectsFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen infizierten und anderen Objekte
totalSuspiciousObjectsFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen möglicherweise infizierten Objekte
totalVirusesFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen Objekte
totalObjectsQuarantined	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien.
totalObjectsNotQuarantined	Anzahl der infizierten oder möglicherweise infizierten Objekte, die Kaspersky Embedded Systems Security erfolglos versuchte, in die Quarantäne zu verschieben. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsDisinfected	Anzahl der infizierten Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien

Indikatoren	Definition
totalObjectsNotDisinfected	Anzahl der infizierten und anderen Objekte, deren Desinfektion durch Kaspersky Embedded Systems Security fehlgeschlagen ist. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsDeleted	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotDeleted	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die Kaspersky Embedded Systems Security erfolglos zu desinfizieren versuchte. Gezählt seit dem letzten Start der zum Aufgabe Echtzeitschutz für Dateien
totalObjectsBackedUp	Anzahl der infizierten oder anderen Objekte, die von Kaspersky Embedded Systems Security ins Backup verschoben wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotBackedUp	Anzahl der infizierten oder anderen Objekte, die Kaspersky Embedded Systems Security erfolglos versuchte, ins Backup zu verschieben. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien

SNMP-Traps in Kaspersky Embedded Systems Security

Die Optionen von SNMP-Traps in Kaspersky Embedded Systems Security sind wie folgt zusammengefasst:

- eventThreatDetected: Objekt gefunden.

  Es gibt folgende Trap-Optionen:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - UserName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- eventBackupStorageSizeExceeds: Maximale Größe des Backups überschritten.Das Gesamtvolumen der Daten im Backup-Ordner hat den Wert überschritten, der durch die Einstellung **Maximale Größe des Backups (MB)** festgelegt ist. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

Es gibt folgende Trap-Optionen:

- eventDateAndTime
- eventSeverity
- eventSource

- eventThresholdBackupStorageSizeExceeds: Maximale Größe des Backups ist erreicht. Größe des freien Speicherplatzes im Backup, die in der Einstellung **Grenzwert für verfügbaren Speicherplatz (MB)** eingegeben wurde, ist gleich dem angegebenen Wert oder liegt darunter. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

  Es gibt folgende Trap-Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: Die maximale Größe der Quarantäne wurde überschritten. Das Gesamtvolumen der Daten im Quarantäne-Ordner hat den Wert überschritten, der durch die Einstellung **Maximale Größe der Quarantäne (MB)** festgelegt ist. Kaspersky Embedded Systems Security verschiebt möglicherweise infizierte Objekte weiterhin in die Quarantäne.

  Es gibt folgende Trap-Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: Quarantäne-Fehler.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - UserName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped: Fehler beim Speichern einer Kopie des Objekts im Backup.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - UserName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError: Interner Quarantäne-Fehler.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError: Backup-Fehler.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated: Antiviren-Datenbanken sind veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Update der Programm-Datenbanken zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventAVBasesTotallyOutdated: Antiviren-Datenbanken sind stark veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Update der Programm-Datenbanken zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventApplicationStarted: Kaspersky Embedded Systems Security läuft

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventApplicationShutdown: Kaspersky Embedded Systems Security wurde beendet

  Es gibt folgende Trap-Optionen:

  - eventSeverity

  - eventDateAndTime
  - eventSource
- eventCriticalAreasScanWasntPerformForALongTime: Untersuchung wichtiger Bereiche liegt lange zurück. Berechnet als Anzahl der Tage seit dem letzten Abschluss der Aufgabe zur Untersuchung wichtiger Bereiche

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventLicenseHasExpired: Lizenz ist abgelaufen.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
- eventLicenseExpiresSoon: Lizenz läuft bald ab. Es werden die Tage gezählt, die bis zum Ablauf der Lizenz verbleiben.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days
- eventTaskInternalError: Fehler bei Ausgabenausführung.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName
- eventUpdateError: Fehler bei Ausführung der Update-Aufgabe.

  Es gibt folgende Trap-Optionen:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Die Beschreibungen der Trap-Optionen und deren mögliche Parameter lauten wie folgt:

- eventDateAndTime: Datum und Uhrzeit des Ereignisses.
- eventSeverity: Prioritätsstufe.

  Diese Option kann folgende Werte annehmen:

  - critical (1) – kritisch
  - warning (2) – Warnung
  - info (3) – informativ
- userName: Ein Benutzername (z. B. des Benutzers, der versucht hat, Zugriff auf eine infizierte Datei zu erhalten).
- computerName: Computername (beispielsweise Name des Computers, von dem ein Benutzer versucht hat, Zugriff auf eine infizierte Datei zu bekommen)
- eventSource: Ereignisquelle: funktionalen Komponente, bei der ein Ereignis aufgetreten ist.

  Diese Option kann folgende Werte annehmen:

  - unknown (0) – Die Komponente ist 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 nichts mit einzelnen Komponenten, sondern mit Kaspersky Embedded Systems Security als Ganzem zu tun hat
  - systemAudit (8) – Systemaudit-Protokoll
- eventReason: Ereignisauslöser: Grund für Ereigniseintritt.

  Diese Option kann folgende Werte annehmen:

  - reasonUnknown(0) – der Grund ist unbekannt
  - reasonInvalidSettings (1) – nur für Ereignisse des Backups und der Quarantäne; Wird angezeigt, wenn der Quarantäne-Ordner oder der Backup-Ordner nicht verfügbar sind (unzureichende Zugriffsrechte oder Ordner wurde in den Quarantäneparametern falsch angegeben, z.B. ein Netzwerkpfad wurde angegeben). In diesem Fall verwendet Kaspersky Embedded Systems Security den Standardordner für Backup oder Quarantäne.
- objectName: Objektname (beispielsweise Name der Datei, in der eine Bedrohung gefunden wurde).
- threatName: Name des gefundenen Objekts gemäß der Klassifizierung der Viren-Enzyklopädie https://encyclopedia.kaspersky.de/knowledge/classification/. Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Embedded Systems Security beim Fund eines Objekts zurückgibt. Sie können den vollständigen Namen eines gefundenen Objekts im Protokoll der Aufgabenausführung einsehen (siehe Abschnitt "Protokolleinstellungen anpassen" auf Seite 106).
- detectType: Typ des gefundenen Objekts.

Diese Option kann folgende Werte annehmen:

- undefined (0) – nicht definiert
- virware – klassische Viren und Netzwerkwürmer
- trojware – Trojaner
- malware – sonstige Schadsoftware
- adware – Adware
- pornware – pornografische Programme
- riskware – legale Programmen, die von Angreifern genutzt werden können, um den Computer oder persönliche Daten zu schädigen

- detectCertainty: Gewissheit für 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 bekanntem Schadcode übereinstimmt.
  - Sure (infiziert)– Kaspersky Embedded Systems Security hat erkannt, dass ein Codeabschnitt des Objekts vollständig mit einem bekanntem Schadcode übereinstimmt.
- days: Anzahl von Tagen (z. B. Anzahl der Tage bis zum Ablauf einer Lizenz).
- errorCode: Ein Fehlercode.
- knowledgeBaseId: Adresse des Artikels in der Wissensdatenbank (beispielsweise Adresse des Artikels, der einen Fehler beschreibt).
- taskName: Ein Aufgabenname.
- updaterErrorEventReason: Ein Grund, aus dem das Update nicht übernommen wurde.

  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 – Das Objekt ist beschädigt;
  - reasonConnectionReset – Verbindungstrennung;
  - reasonTimeOut – Zeitüberschreitung bei Verbindung;
  - reasonProxyAuthError – Fehler bei Authentifizierung auf dem Proxyserver;
  - reasonServerAuthError – Fehler bei Authentifizierung auf dem Server;
  - reasonHostNotFound – Der Computer wurde nicht gefunden;
  - reasonServerBusy – Server nicht verfügbar;

- reasonConnectionError – Verbindungsfehler;
- reasonModuleNotFound – Das Objekt wurde nicht gefunden;
- reasonBlstCheckFailed(16) – Fehler beim Überprüfen der schwarzen Schlüsselliste. Möglicherweise wurde während des Updatevorgangs Datenbanken-Updates veröffentlicht. Wiederholen Sie bitte das Update in einigen Minuten.

- storageObjectNotAddedEventReason: Der Grund für das Nichtverschieben eines Objektes in das Backup oder die Quarantäne.

  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 – Ein-/Ausgabefehler: a) Kaspersky Embedded Systems Security ist beschädigt, Kaspersky Embedded Systems Security muss wiederhergestellt werden; b) das Laufwerk mit Kaspersky Embedded Systems Security ist beschädigt.
  - reasonStorageCorrupted – Speicher ist beschädigt; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
  - reasonStorageFull – Datenbank ist voll; es wird Speicherplatz benötigt.
  - 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 nicht auf dem Datenträger 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 Platz auf dem Datenträger.

Integration mit WMI

Kaspersky Embedded Systems Security unterstützt die Integration mit Windows-Verwaltungsinstrumentation (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 seine Komponenten zu sammeln.

Wenn Kaspersky Embedded Systems Security installiert ist, werden eigene Module im System registriert, wodurch die Erstellung eines Namensraums von Kaspersky Embedded Systems Security, des WMI-Stammnamensraums auf dem lokalen Computer erleichtert wird. 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 dauernd ausgeführt oder beendet werden kann. Für solche Aufgaben gibt es keinen Ausführungsfortschritt. Die Ergebnisse der Aufgabenausführung 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 die Richtlinien von Kaspersky Security Center verwaltet.

Eine *Periodische Aufgabe* ist eine Programmaufgabe, die zeitlich beschränkt ist und einen Ausführungsfortschritt aufweist, der als Prozentsatz angezeigt wird. Die Aufgabenergebnisse werden beim Abschluss der Aufgabe erzeugt und als ein einzelnes Element oder geänderten Programmstatus dargestellt (beispielsweise Update der Programm-Datenbanken abgeschlossen, Konfigurationsdateien für die Aufgaben zum Erstellen von Regeln erzeugt). Eine Anzahl von periodischen Aufgaben desselben Typs kann auf einem einzelnen Computer 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 und das Empfangen von dynamischen Daten aus WMI-Namensräume in Ihrem Unternehmensnetzwerk verwenden, haben Sie die Möglichkeit, Informationen über den aktuellen Zustand des Programms zu empfangen (siehe Tabelle unten).

Tabelle 77. Informationen über den Zustand des Programms

Eigenschaft der Exemplarklasse	Beschreibung	Werte
ProductName	Name des installierten Programms.	Vollständiger Name des Programms ohne Versionsnummer.
ProductVersion	Vollständige Version des installierten Programms.	Vollständige Versionsnummer des Programms einschließlich Nummer des Builds
InstalledPatches	Matrix von Patch-Anzeigenamen, die für das Programm bereitgestellt sind.	Liste von kritischen Fehlerbehebungen, die für das Programm installiert wurden.
IsLicenseInstalled	Aktivierungsstatus des Programms.	Status des Schlüssels, der zur Aktivierung des Programms verwendet wurde. Mögliche Werte: • Falsch – Es wurde kein Schlüssel oder Aktivierungscode im Programm festgelegt. • Wahr – Es wurde ein Schlüssel oder Aktivierungscode zum Programm hinzugefügt.

Eigenschaft der Exemplarklasse	Beschreibung	Werte
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 auf der Grundlage einer schwarzen Liste für Schlüssel gesperrt ist).
AVBasesDatetime	Zeitstempel für eine 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 "Nicht installiert" auf.
IsExploitPreventionEnabled	Komponentenstatus der "Exploit-Prävention".	Status der Komponente "Exploit-Prävention". Mögliche Werte: • Wahr – Die Komponente "Exploit-Prävention" ist aktiviert und bietet Schutz. • Falsch – Die Komponente "Exploit-Prävention" bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
ProtectionTasksRunning	Matrix 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 einzige nicht periodische Aufgabe ausgeführt wird, weist das Feld den Wert "Keine" auf.

Eigenschaft der Exemplarklasse	Beschreibung	Werte
IsAppControlRunning	Aufgabenstatus der zur Kontrolle des Programmstarts.	Status der Aufgabe zur Kontrolle des Programmstarts. • Wahr – Die Aufgabe zur Kontrolle des Programmstarts wird derzeit nicht ausgeführt. • Falsch – Die Kontrolle des Programmstarts wird derzeit nicht ausgeführt oder die Komponente "Kontrolle des Programmstarts" ist nicht installiert.
AppControlMode	Aufgabenstatus der Kontrolle des Programmstarts.	Beschreibung des aktuellen Status der Komponente "Kontrolle des Programmstarts" und beschreibt den ausgewählten Modus für die zugehörige Aufgabe. Mögliche Werte: • Aktiv – In den Aufgabeneinstellungen ist der Modus **Aktiv** ausgewählt. • Nur Statistik – In den Aufgabeneinstellungen ist der Modus **Nur Statistik** ausgewählt. • Nicht installiert – Die Komponente "Kontrolle des Programmstarts" ist nicht installiert.
AppControlRulesNumber	Gesamtanzahl der Regeln für die Kontrolle des Programmstarts.	Anzahl der derzeit in den Einstellungen der Kontrolle des Programmstarts festgelegten Regeln.
AppControlLastBlocking	Zeitstempel für den letzten von der Aufgabe zur 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 Aufgabenmodus. Wenn zum Zeitpunkt der Verarbeitung der WMI-Abfrage keine Exemplarklassen von blockierten Programmstarts registriert sind, wird dem Feld der Wert "Keine" zugewiesen.

Eigenschaft der Exemplarklasse	Beschreibung	Werte
PeriodicTasksRunning	Matrix 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 "Keine" auf.
ConnectionState	Status der Verbindung zwischen der WMI-Anbieterkomponente und dem Kaspersky Security Service (KAVFS).	Informationen über den Status der Verbindung zwischen dem WMI-Anbietermodul und dem Kaspersky Security Service. Mögliche Werte: • Erfolg – Die Verbindung wurde erfolgreich hergestellt: der WMI-Client kann Informationen über den Programmstatus empfangen. • Fehler. Fehlercode: <code> – Die Verbindung konnte aufgrund eines Fehlers mit dem angegebenen Code nicht hergestellt werden.

Diese Daten repräsentieren Eigenschaften von Exemplarklassen vom Typ "KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security", wobei:

- "KasperskySecurity_ProductInfo" der Name der Klasse von Kaspersky Embedded Systems Security ist
- ".ProductName=Kaspersky Embedded Systems Security" der Schlüsselparameter für Kaspersky Embedded Systems Security ist

Die Exemplarklasse wird im Namensraum ROOT\Kaspersky\Security erstellt.

Arbeiten mit Kaspersky Embedded Systems Security aus der Befehlszeile

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Embedded Systems Security aus der Befehlszeile.

In diesem Kapitel

Befehle der Befehlszeile

Sie können die Basisbefehle zur Verwaltung von Kaspersky Embedded Systems Security aus der Befehlszeile des geschützten Computers erteilen, wenn Sie bei der Installation von Kaspersky Embedded Systems Security den Punkt Befehlszeilen-Tool zur Installation ausgewählt haben.

Mit Hilfe der Befehlszeile können Sie nur Funktionen steuern, für die Sie in Kaspersky Embedded Systems Security zugriffsberechtigt sind.

Bestimmte Befehle von Kaspersky Embedded Systems Security werden in folgenden Modi ausgeführt:

- Synchronmodus: Die Kontrolle kehrt sofort nach Abschluss der Befehlsausführung zur Konsole zurück.
- Asynchronmodus: Die Kontrolle kehrt sofort nach dem Befehlsstart zur Konsole zurück.

► *Um die Ausführung eines synchronen Befehls zu unterbrechen,*

drücken Sie die Tasten **Strg+C**.

Gehen Sie entsprechend der folgenden Regeln vor, wenn Sie Befehle für Kaspersky Embedded Systems Security eingeben:

- Beachten Sie bei der Eingabe von Schlüsseln und Befehlen die Groß- und Kleinschreibung.
- Trennen Sie Schlüssel durch Leerzeichen voneinander.
- Wenn der Name einer Datei, den Sie als Wert für einen Schlüssel angeben, ein Leerzeichen enthält, setzen Sie den Dateinamen (und den entsprechenden Pfad) in Anführungszeichen, z. B.: "`C:\TEST\test cpp.exe`".
- Bei Bedarf können Sie in Masken für Dateinamen oder Pfade Platzhalterzeichen verwenden. Beispiele: "`C:\Temp\Temp*\`", "`C:\Temp\Temp???.doc`", "`C:\Temp\Temp*.doc`"

Mithilfe der Befehlszeile können Sie das gesamte Spektrum an Operationen zur Steuerung und Verwaltung von Kaspersky Embedded Systems Security ausführen (siehe Tabelle unten).

Tabelle 78. Befehle für Kaspersky Embedded Systems Security

Befehl	Beschreibung
KAVSHELL APPCONTROL (siehe Abschnitt "Ergänzen der Regelliste für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL" auf Seite 533)	Ergänzt die Liste der gebildeten Regeln für die Kontrolle des Programmstarts entsprechend dem ausgewählten Prinzip für das Hinzufügen.
KAVSHELL APPCONTROL /CONFIG (siehe Abschnitt "Verwaltung der Aufgabe Kontrolle des Programmstarts. KAVSHELL APPCONTROL /CONFIG" auf Seite 530).	Verwaltung des Ausführungsmodus der Aufgabe zur Kontrolle des Programmstarts.
KAVSHELL APPCONTROL /GENEARTE (siehe Abschnitt "Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL /GENERATE" auf Seite 531).	Erstellt eine Aufgabe zum automatischen Erstellen von Erlaubnisregeln für die Kontrolle des Programmstarts.
KAVSHELL VACUUM (siehe Abschnitt "Log-Dateien für Kaspersky Embedded Systems Security defragmentieren.KAVSHELL VACUUM" auf Seite 541)	Defragmentiert die Log-Dateien für Kaspersky Embedded Systems Security.
KAVSHELL PASSWORD	Verwaltet die Einstellungen für den Kennwortschutz.
KAVSHELL HELP (siehe Abschnitt "Hilfe für Befehle in Kaspersky Embedded Systems Security anzeigen.KAVSHELL HELP" auf Seite 521)	Zeigt die Hilfe für Befehle in Kaspersky Embedded Systems Security an.
KAVSHELL START (siehe Abschnitt "Kaspersky Security Service starten und anhalten. KAVSHELL START, KAVSHELL STOP" auf Seite 521)	Startet den Dienst von Kaspersky Embedded Systems Security.
KAVSHELL STOP (siehe Abschnitt "Kaspersky Security Service starten und anhalten. KAVSHELL START, KAVSHELL STOP" auf Seite 521)	Stoppt den Dienst von Kaspersky Embedded Systems Security.

Befehl	Beschreibung
KAVSHELL SCAN (siehe Abschnitt "Ausgewählten Bereich untersuchen.KAVSHELL SCAN" auf Seite 522)	Erstellt und startet eine temporäre Aufgabe zur Untersuchung auf Befehl mit einem Untersuchungsbereich und Sicherheitsparametern, die durch Befehlsschlüssel vorgegeben werden.
KAVSHELL SCANCRITICAL (siehe Abschnitt "Aufgabe zur Untersuchung wichtiger Bereiche starten.KAVSHELL SCANCRITICAL" auf Seite 526)	Startet die Systemaufgabe Untersuchung wichtiger Bereiche.
KAVSHELL TASK (siehe Abschnitt "Angegebene Aufgabe asynchron verwalten.KAVSHELL TASK" auf Seite 527)	Startet , Hält an / Setzt fort , Beendet die angegebene Aufgabe im asynchronen Modus , Gibt den aktuellen Aufgabenstatus / eine Statistik für die Aufgabe zurück.
KAVSHELL RTP (siehe Abschnitt "Aufgaben zum Echtzeitschutz starten und stoppen.KAVSHELL RTP" auf Seite 529)	Startet oder beendet alle Echtzeitschutz-Aufgaben.
KAVSHELL UPDATE (siehe Abschnitt "Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security starten.KAVSHELL UPDATE" auf Seite 535)	Startet die Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security mit den festgelegten Befehlszeilenparametern.
KAVSHELL ROLLBACK (siehe Abschnitt "Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security.KAVSHELL ROLLBACK" auf Seite 539)	Kehrt zur vorherigen Version der Datenbanken zurück.
KAVSHELL LICENSE	Fügt die Schlüssel hinzu bzw. löscht diese. Zeigt Informationen über die hinzugefügten Schlüssel an.
KAVSHELL TRACE (siehe Abschnitt "Protokoll zur Ablaufverfolgung aktivieren, anpassen und deaktivieren.KAVSHELL TRACE" auf Seite 539)	Aktiviert oder deaktiviert das Protokoll zur Ablaufverfolgung, Verwalten der Parameter für das Protokoll zur Ablaufverfolgung.
KAVSHELL DUMP (siehe Abschnitt "Anlegen von Dump-Dateien ein- und ausschalten.KAVSHELL DUMP" auf Seite 543)	Aktiviert bzw. deaktiviert die Erstellung von Dump-Dateien für Prozesse von Kaspersky Embedded Systems Security bei einem Absturz von Prozessen.

Befehl	Beschreibung
KAVSHELL IMPORT (siehe Abschnitt "Einstellungen importieren.KAVSHELL IMPORT" auf Seite 544)	Importiert die allgemeinen Einstellungen, Funktionen und Aufgaben für Kaspersky Embedded Systems Security aus einer zuvor erstellten Konfigurationsdatei.
KAVSHELL EXPORT (siehe Abschnitt "Einstellungen exportieren.KAVSHELL EXPORT" auf Seite 544)	Exportiert alle Einstellungen und vorhandene Aufgaben von Kaspersky Embedded Systems Security in eine Konfigurationsdatei.
KAVSHELL DEVCONTROL (siehe Abschnitt "Liste der Regeln für die Gerätekontrolle ergänzen.KAVSHELL DEVCONTROL" auf Seite 534)	Ergänzt die Liste der erstellten Regeln für die Gerätekontrolle entsprechend dem ausgewählten Prinzip für das Hinzufügen.

Hilfe für Befehle in Kaspersky Embedded Systems Security anzeigen. KAVSHELL HELP

Um eine Liste aller Befehle für Kaspersky Embedded Systems Security zu öffnen, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Um die Beschreibung und Syntax eines Befehls zu erhalten, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL HELP <Befehl>

KAVSHELL <Befehl> /?
```

Beispiele für den Befehl KAVSHELL HELP

Um ausführliche Informationen zu dem Befehl KAVSHELL SCAN zu erhalten, führen Sie folgenden Befehl aus:

```
KAVSHELL HELP SCAN
```

Kaspersky Security Service starten und anhalten KAVSHELL START, KAVSHELL STOP

Um Kaspersky Security Service zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL START
```

Wenn Kaspersky Security Service gestartet wird, werden standardmäßig folgende Aufgaben gestartet: Echtzeitschutz für Dateien und Untersuchung bei Systemstart, sowie andere Aufgaben, für deren Zeitplan die Startfrequenz **Bei Programmstart** gilt.

Um Kaspersky Security Service anzuhalten, führen Sie folgenden Befehl aus:

```
KAVSHELL STOP
```

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Angegebenen Bereich untersuchen. KAVSHELL SCAN

Um eine Untersuchung für bestimmte Bereich des geschützten Computers zu starten, verwenden Sie den Befehl `KAVSHELL SCAN`. Die Schlüssel dieses Befehls legen die Einstellungen des Untersuchungsbereichs und die Sicherheitseinstellungen des ausgewählten Knotens fest.

Eine Aufgabe zur Untersuchung auf Befehl, die mit dem Befehl `KAVSHELL SCAN` gestartet wurde, ist temporär. Sie wird nur während ihrer Ausführung in der Programmkonsole angezeigt (die Aufgabeneinstellungen können nicht in der Programmkonsole angezeigt werden). Das Protokoll über die Leistung der Aufgabe wird gleichzeitig erzeugt. Es wird in den **Protokollen der Aufgabenausführung** der Programmkonsole angezeigt.

Wenn Sie den Pfad in einer Aufgabe zur Untersuchung bestimmter Bereiche angeben, können Sie Umgebungsvariable verwenden. Wenn Sie eine Umgebungsvariable verwenden, die einem Benutzer zugeordnet ist, führen Sie den Befehl `KAVSHELL SCAN` mit den Rechten dieses Benutzers aus.

Der Befehl `KAVSHELL SCAN` wird synchron ausgeführt.

Um eine bestehenden Aufgabe zur Untersuchung auf Befehl aus der Befehlszeile zu starten, verwenden Sie den Befehl KAVSHELL TASK (siehe Abschnitt "Angegebene Aufgabe asynchron verwalten.KAVSHELL TASK" auf Seite 527).

Syntax des Befehls KAVSHELL SCAN

```
KAVSHELL SCAN <Untersuchungsbereiche> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< Name der Datei mit einer Liste der Untersuchungsbereiche >] [/F<A|C|E>] [/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"Masken">] [/ES:<Größe>] [/ET:<Dauer in Sekunden>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<Tage>] [NORECALL]>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<Dateiname für Protokoll der Aufgabenausführung>] [/ANSI] [/ALIAS:<Alias des Aufgabenamens>]
```

Der Befehl KAVSHELL SCAN enthält sowohl obligatorische als auch Reserveschlüssel, deren Verwendung optional ist (s. Tabelle unten).

Beispiele für den Befehl KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Tabelle 79. Schlüssel des Befehls KAVSHELL SCAN.

Schlüssel	Beschreibung
Untersuchungsbereich. Obligatorischer Schlüssel.	
<Dateien> <Ordner> <Netzwerkpfad>	Untersuchungsbereich – Liste mit Dateien, Ordnern, Netzwerkpfaden und vordefinierten Bereichen. Geben Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) an. Im folgenden Beispiel wird der Ordner Folder4 ohne Pfad angegeben. Er befindet sich im Ordner, aus dem der Befehl KAVSHELL ausgeführt wird: KAVSHELL SCAN Folder4 Wenn der Name des Objektes, das Sie untersuchen möchten, ein Leerzeichen enthält, muss dieser Name in Klammern stehen. Wenn Sie einen Ordner ausgewählt haben, untersucht Kaspersky Embedded Systems Security auch alle eingebetteten Unterordner für diesen Ordner. Um eine Gruppe der Datei zu untersuchen, können Sie die Zeichen * und ? verwenden.
/MEMORY	Objekte im Arbeitsspeicher untersuchen.
/SHARED	Freigegebene Ordner auf dem Computer untersuchen.
/STARTUP	Autostart-Objekte untersuchen
/REMDRIVES	Wechseldatenträger untersuchen.
/FIXDRIVES	Festplatten untersuchen.
/MYCOMP	Alle Bereiche des geschützten Computers untersuchen.

Schlüssel	Beschreibung
/L: <Name einer Datei mit einer Liste der Untersuchungsbereiche>	Name einer Datei mit einer Liste der Untersuchungsbereiche, einschließlich dem vollständigen Dateipfad. Trennen Sie die Untersuchungsbereiche in der Datei durch ein Zeilenwechselsymbol. Sie können vordefinierte Untersuchungsbereiche angeben, wie unten am Beispiel einer Datei mit einer Liste von Untersuchungsbereichen gezeigt wird: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Zu untersuchende Objekte (File types). Wenn Sie keine Werte für diesen Schlüssel angeben, untersucht Kaspersky Embedded Systems Security die Objekte nach Format.	
/FA	Alle Objekte untersuchen.
/FC	Objekte, die nach Format untersucht werden (Standard). Kaspersky Embedded Systems Security untersucht nur Objekte, die dem Format nach als infizierbar gelten.
/FE	Objekte nach Erweiterung untersuchen. Kaspersky Embedded Systems Security untersucht nur Objekte, die der Erweiterung nach als infizierbar gelten.
/NEWONLY	Nur neue und veränderte Dateien untersuchen. Wenn Sie diesen Schlüssel nicht angeben, untersucht Kaspersky Embedded Systems Security alle Objekte.
/AI: **Aktion für infizierte und andere Objekte**. Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Embedded Systems Security die Aktion **Überspringen** aus.	
DISINFECT	Desinfizieren, irreparable Objekte überspringen Die Einstellungen DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Embedded Systems Security beibehalten, um die Kompatibilität mit den vorherigen Versionen zu gewährleisten. Diese Einstellungen können anstelle der Befehle /AI und /AS verwendet werden: In diesem Fall werden möglicherweise infizierte Objekte von Kaspersky Embedded Systems Security nicht bearbeitet.
DISINFDEL	Desinfizieren, irreparable Objekte überspringen
DELETE	Löschen Die Einstellungen DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Embedded Systems Security beibehalten, um die Kompatibilität mit den vorherigen Versionen zu gewährleisten. Diese Einstellungen können anstelle der Befehle /AI und /AS verwendet werden: In diesem Fall werden möglicherweise infizierte Objekte von Kaspersky Embedded Systems Security nicht bearbeitet.
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
/AS: **Aktion für möglicherweise infizierte Objekte**/ Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Embedded Systems Security die Aktion **Überspringen** aus.	
QUARANTINE	Quarantäne
DELETE	Löschen

Schlüssel	Beschreibung
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
Ausnahmen	
/E:ABMSPO	Dieser Schlüssel schließt zusammengesetzte Objekte der folgenden Typen aus: A – SFX-Archive B – E-Mail-Datenbanken M – Dateien mit E-Mailformaten S – Archive (SFX-Archive einschließlich) P – gepackte Objekte O – eingebettete OLE-Objekte
/EM:<"Masken">	Dateien nach Maske ausschließen Sie können mehrere Masken angeben, z. B. EM:"*.txt;*.png; C\Videos*.avi".
/ET:<Anzahl der Sekunden>	Verarbeitung eines Objektes abbrechen, wenn sie länger dauert, als der in Sekunden festgelegte Wert. In der Grundeinstellung ist die Untersuchungsdauer nicht beschränkt.
/ES:<Größe>	Zusammengesetzte Objekte, deren Größe den in MB festgelegten Wert <size> überschreitet, von Untersuchung ausschließen. Kaspersky Embedded Systems Security untersucht standardmäßig alle Objektgrößen.
/TZOFF	Ausnahmen der vertrauenswürdigen Zone verschieben.
Erweiterte Einstellungen (Options)	
/NOICHECKER	iChecker-Technologie deaktivieren (standardmäßig aktiviert).
/NOISWIFT	iSwift-Technologie deaktivieren (standardmäßig aktiviert).
/ANALYZERLEVEL:<Analysestufe>	Verwendung der heuristische Analyse aktivieren, Analyseniveau einstellen. Die folgenden Ebenen der heuristischen Analyse verfügbar: 1 – oberflächlich; 2 – mittel; 3 – tief Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Embedded Systems Security die heuristische Analyse nicht.
/ALIAS:<Alias des Aufgabenamens>	Dieser Schlüssel weist einer Aufgabe zur Untersuchung auf Befehl einen temporären Namen zu, mit dem auf die Aufgabe zugegriffen werden kann, während sie ausgeführt wird, z.B. um mit dem Befehl TASK eine Statistik anzuzeigen. Der Alias des Aufgabenamens muss unter den alternativen Namen für die Aufgaben aller Funktionalkomponenten von Kaspersky Embedded Systems Security einmalig sein. Wenn dieser Schlüssel nicht vorgegeben ist, erhält die Aufgabe den alternativen Name scan_<kavshell_pid> (z.B. scan_1234). In der Programmkonsole erhält die Aufgabe den Namen Scan objects (<Datum und Uhrzeit>), z. B. Scan objects 8/16/2007 05:13:14 PM.
Einstellungen für Protokolle über Aufgabenausführung (Report settings)	

Schlüssel	Beschreibung
/W:<Name des Protokolls der Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Embedded Systems Security das Protokoll der Aufgabenausführung mit dem durch diesen Schlüssel vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse in der Aufgabe. Im Protokoll werden die Ereignisse aufgezeichnet, die durch die Einstellungen für die Protokolle der Aufgabenausführung und das Ereignisprotokoll von Kaspersky Embedded Systems Security in der Ereignisanzeige festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten "Protokolle der Aufgabenausführung" der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen, es erfolgt aber eine Fehlermeldung.
/ANSI	Der Schlüssel erlaubt es, die Ereignisse in das Protokoll der Aufgabenausführung in der ANSI-Codierung zu schreiben. Der ANSI Schlüssel wird nicht verwendet, wenn der W Schlüssel nicht angegeben wird. Wenn der ANSI Schlüssel nicht angegeben wird, wird das Protokoll der Aufgabenausführung in der ANSI-Codierung geführt.

Aufgabe Untersuchung wichtiger Bereiche starten. KAVSHELL SCANCRITICAL

Verwenden Sie den Befehl `KAVSHELL SCANCRITICAL`, um die Systemaufgabe zur Untersuchung wichtiger Bereiche auf Befehl mit den Einstellungen zu starten, die in der Programmkonsole festgelegt wurden.

Syntax des Befehls KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<Dateiname für das Protokoll der Aufgabenausführung>]
```

Beispiele für den Befehl KAVSHELL SCANCRITICAL

Um die Aufgabe zur Untersuchung auf Befehl Untersuchung wichtiger Bereiche auszuführen und das Protokoll der Aufgabenausführung im aktuellen Ordner in der Datei scancritical.log zu speichern, führen Sie folgenden Befehl aus:

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

Sie können den Speicherort des Protokolls der Aufgabenausführung je nach Syntax des Schlüssels /W einstellen (s. Tabelle unten).

Tabelle 80. Syntax des Schlüssels /W des Befehls KAVSHELL SCANCRITICAL

Schlüssel	Beschreibung
/W:<Name des Protokolls der Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Embedded Systems Security das Protokoll der Aufgabenausführung mit dem durch diesen Schlüssel vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse in der Aufgabe. Im Protokoll werden die Ereignisse aufgezeichnet, die durch die Einstellungen für das Protokoll der Aufgabenausführung und das Ereignisprotokoll des Programms in der Ereignisanzeige festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten **Protokolle der Aufgabenausführung** der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen, es erfolgt aber eine Fehlermeldung.

Asynchrone Aufgabenverwaltung. KAVSHELL TASK

Mit dem Befehl `KAVSHELL TASK` können Sie eine bestimmte Aufgabe verwalten: Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe, sowie Anzeigen des aktuelles Status und einer Statistik der Aufgabe. Der Befehl wird asynchron ausgeführt.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL TASK

```
KAVSHELL TASK [<Alias des Aufgabenamens> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Beispiele für den Befehl KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

Der Befehl `KAVSHELL TASK` kann sowohl mit einem oder mehreren Schlüsseln als auch ohne Schlüssel ausgeführt werden (s. Tabelle unten).

Tabelle 81. Schlüssel des Befehls KAVSHELL TASK

Schlüssel	Beschreibung
Ohne Schlüssel	Gibt eine Liste aller vorhandenen Serveraufgaben in Kaspersky Embedded Systems Security zurück. Die Liste enthält die Felder: Alias des Aufgabennamens, Aufgabenkategorie (Systemaufgabe oder benutzerdefinierte Aufgabe) und den aktuellen Aufgabenstatus.
<Alias des Aufgabenamens>	Verwenden Sie anstatt des Aufgabennamens im Befehl SCAN TASK einen alternativen Namen (Task alias). Dies ist ein zusätzlicher Kurzname, den Kaspersky Embedded Systems Security an Aufgaben vergibt. Um die alternativen Namen der Aufgaben von Kaspersky Embedded Systems Security anzuzeigen, führen Sie den Befehl KAVSHELL TASK ohne einen Schlüssel aus.
/START	Die angegebene Aufgabe im asynchronen Modus starten.
/STOP	Beenden einer angegebenen Aufgabe.
/PAUSE	Anhalten einer angegebenen Aufgabe.
/RESUME	Asynchrones Fortsetzen einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (zum Beispiel, *Läuft*, *Abgeschlossen*, *Angehalten*, *Beendet*, *Fehlgeschlagen*, *Wird gestartet*, *Wird wiederhergestellt*).
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet wurden.

Beachten Sie, dass diese Schlüssel von allen Aufgaben von Kaspersky Embedded Systems Security vollständig unterstützt werden.

Rückgabecodes für den Befehl KAVSHELL TASK (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TASK" auf Seite 548).

KAVFS als systemgeschützten Prozess registrieren. KAVSHELL CONFIG

Mit dem Befehl `KAVSHELL CONFIG` können Sie die Registrierung des Kaspersky Security Service als einen systemgeschützten Prozess (Protected Process Light) mithilfe des ELAM-Treibers steuern, der während der Programminstallation im Betriebssystem installiert wurde.

Syntax des Befehls KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<ON|OFF>
```

Tabelle 82. Schlüssel des Befehls KAVSHELL CONFIG

Schlüssel	Beschreibung
/PPL:ON	Kaspersky Security Service als PPL registrieren.
/PPL:OFF	PPL-Attribut für Kaspersky Security Service entfernen.

Das Programm führt die Deregistrierung des Dienstes automatisch durch, wenn eine der folgenden Aktionen ausgeführt wird:

- Deinstallation des Programms
- Upgrade des Programms
- Installation eines Patches
- Reparatur von Programmkomponenten

Rückgabecodes für den Befehl KAVSHELL CONFIG

Echtzeitschutz-Aufgaben starten und beenden. KAVSHELL RTP

Mit dem Befehl `KAVSHELL RTP` können Sie alle Aufgaben des Echtzeitschutzes starten oder beenden.

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Beispiele für den Befehl KAVSHELL RTP

Um alle Aufgaben zum Echtzeitschutz zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL RTP /START
```

Der Befehl `KAVSHELL RTP` kann einen beliebigen der beiden obligatorischen Schlüssel enthalten (s. Tabelle unten).

Tabelle 83. Schlüssel des Befehls KAVSHELL RTP

Schlüssel	Beschreibung
/START	Startet alle Echtzeitschutz-Aufgaben: "Echtzeitschutz für Dateien" und "Verwendung von KSN".
/STOP	Beenden aller Echtzeitschutz-Aufgaben.

Verwaltung der Aufgabe Kontrolle des Programmstarts. KAVSHELL APPCONTROL /CONFIG

Mithilfe des Befehls `KAVSHELL APPCONTROL/CONFIG` können Sie den Ausführungsmodus der Aufgabe Kontrolle des Programmstarts anpassen und den Upload von DLL-Modulen überwachen.

Syntax des Befehls KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<vollständiger Pfad zur xml-Datei>
```

Beispiele für den Befehl KAVSHELL APPCONTROL /CONFIG

► *Um die Aufgabe zur Kontrolle des Programmstarts im Modus **Aktiv** auszuführen, ohne das DLL-Modul zu laden, und die Einstellungen der Aufgabe nach Abschluss zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no> /savetofile:c:\appcontrol\config.xml
```

Sie können die Einstellungen der Aufgabe zur Kontrolle des Programmstarts mithilfe von Schlüsseln anpassen (s. Tabelle unten).

Tabelle 84. Schlüssel des Befehls `KAVSHELL APPCONTROL/CONFIG`

Schlüssel	Beschreibung
`/mode:<applyrules|statistics>`	Funktionsmodus der Aufgabe zur Kontrolle des Programmstarts. Wählen Sie eine der folgenden Ausführungsmodi für die Aufgabe: • Aktiv – Regeln für die Kontrolle des Programmstarts übernehmen • statistics – Nur Statistik
`/dll:<no|yes>`	Deaktivieren oder Aktivieren von "Upload von DLL-Modulen überwachen".
`/savetofile: <vollständiger Pfad der xml-Datei>`	Festgelegte Regeln in die angegebene Datei im xml-Format exportieren.

/savetofile: <vollständiger Name der xml-Datei>	Liste der Regeln in einer Datei speichern.
/savetofile: <vollständiger Name der xml-Datei> /sdc	Liste der Regeln für die Kontrolle für Installationspakete in einer Datei speichern.
/clearsdc	Alle Regeln für die Kontrolle für Installationspakete aus der Liste löschen.

Automatisches Erstellen von Regeln für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL /GENERATE

Mithilfe des Befehls KAVSHELL APPCONTROL/GENERATE können Sie die Listen der Regeln für die Kontrolle des Programmstarts erstellen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel [/pwd:<password>].

Syntax des Befehls KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL/GENERATE <Ordnerpfad> |/source: <Pfad der Datei mit der Ordnerliste> [/masks: <edms>] [/runapp] [/rules: <ch|cp|h>] [/strong] [/user: <Benutzer oder Benutzergruppe>] [/export: <vollständiger Pfad zur xml-Datei>] [/import: <a|r|m>] [/prefix: <Präfix für die Regelnamen>] [/unique]
```

Beispiele für den Befehl KAVSHELL APPCONTROL/GENERATE

► *Um Regeln für die Dateien aus den angegebenen Ordnern zu erstellen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt /export:c:\rules\appctrlrules.xml
```

► *Um im angegebenen Ordner Regeln für ausführbare Dateien aller verfügbaren Erweiterungen zu erstellen und die erstellten Regeln nach Abschluss der Aufgabe in die angegebene xml-Datei zu speichern, führen Sie den folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /GENERATEc:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

Je nach der Syntax der Schlüssel können Sie die Einstellungen für das automatische Erstellen der Regeln für die Kontrolle des Programmstarts anpassen (s. Tabelle unten).

Tabelle 85. Schlüssel des Befehls KAVSHELL APPCONTROL/GENERATE

Schlüssel	Beschreibung
Gültigkeitsbereich der Erlaubnisregeln	
<Ordnerpfad>	Pfad des Ordners, der die ausführbaren Dateien enthält, für die automatisch Erlaubnisregeln erstellt werden sollen.
/source:<Pfad der Datei mit der Ordnerliste>	Pfad der Datei im txt-Format, in der die Liste der Ordner mit den ausführbaren Dateien enthalten ist, für die automatisch Erlaubnisregeln erstellt werden sollen.
/masks: <edms>	Erweiterungen der ausführbaren Dateien, für die Erlaubnisregeln für die Kontrolle des Programmstarts erstellt werden sollen. Sie können Dateien mit den folgenden Erweiterungen zum Gültigkeitsbereich der Regeln einschließen: • e – Dateien mit der Erweiterung exe • d – Dateien mit der Erweiterung dll • m – Dateien mit der Erweiterung msi • s – Skripte
/runapp	Bei der Erstellung von Erlaubnisregeln Programme berücksichtigen, die zum Zeitpunkt der Ausführung der Aufgabe auf dem geschützten Computer gestartet sind.
Verhalten bei der automatischen Erstellung von Erlaubnisregeln	
/rules: <ch|cp|h>	Aktionen angeben, die von der Aufgabe während der Erstellung der Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden: • ch – digitales Zertifikat verwenden. Wenn das Zertifikat fehlt, SHA256-Hash verwenden. • cp – digitales Zertifikat verwenden. Wenn das Zertifikat fehlt, den Wert des Pfades der ausführbaren Datei verwenden. • h – SHA256-Hash verwenden.
/strong	Bei der automatischen Erstellung der Erlaubnisregeln für die Kontrolle des Programmstarts Header und Fingerabdruck des digitalen Zertifikats verwenden. Der Befehl wird ausgeführt, wenn für den Schlüssel /rules folgender Wert angegeben wird: <ch|cp|>.
/user: <Benutzer oder Benutzergruppe>	Benutzername oder Name der Benutzergruppe, für die die Regeln angewendet werden sollen. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer und/oder die angegebene Benutzergruppe.
Verhalten nach Abschluss des automatischen Erstellens von Regeln für die Kontrolle des Programmstarts	
/export: <vollständiger Pfad der xml-Datei>	Erstellte Regeln in einer xml-Datei speichern.

/unique	Informationen über den Computer hinzufügen, für dessen Programme die Erlaubnisregeln für die Kontrolle des Programmstarts erstellt werden.
\prefix: <Präfix für die Regelnamen>	Präfix für den Namen der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts.
/import: <a|r|m>	Erstellte Regeln in die Liste der festgelegten Regeln für die Kontrolle des Programmstarts entsprechend dem angegebenen Ergänzungsprinzip für neue Regeln importieren: • a – **Zu den bestehenden Regeln hinzufügen** (identische Regeln werden verdoppelt) • r – **Bestehende Regeln ersetzen** (bestehende Regeln werden durch neue Regeln ersetzt) • m – **Mit bestehenden Regeln zusammenführen** (neue Regeln, deren Einstellungen nicht mit den Einstellungen schon bestehender Regeln übereinstimmen, werden hinzugefügt)

Ergänzen der Regelliste für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL

Mithilfe des Befehls `KAVSHELL APPCONTROL` können Sie entsprechend dem ausgewählten Prinzip Regeln aus einer xml-Datei zur Regelliste der Aufgabe zur Kontrolle des Programmstarts hinzufügen sowie alle festgelegten Regeln aus der Liste löschen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <vollständiger Pfad zur xml-Datei> | /replace <vollständiger Pfad zur xml-Datei> | /merge <vollständiger Pfad zur xml-Datei> | /clear
```

Beispiel für den Befehl KAVSHELL APPCONTROL

► *Um Regeln aus einer xml-Datei nach dem Prinzip "Zu den bestehenden Regeln hinzufügen" zu den festgelegten Regeln für die Kontrolle des Programmstarts hinzuzufügen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Je nach Syntax der Schlüssel können Sie das Prinzip für das Hinzufügen neuer Regeln aus der angegebenen xml-Datei zur Liste der festgelegten Regeln für die Aufgabe Kontrolle des Programmstarts wählen (s. Tabelle unten).

Tabelle 86. Schlüssel des Befehls KAVSHELL APPCONTROL

Schlüssel	Beschreibung
/append <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts durch Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Zu den bestehenden Regeln hinzufügen** (Regeln mit identischen Einstellungen werden verdoppelt).
/replace <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts durch Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Bestehende Regeln ersetzen** (Regeln mit identischen Einstellungen werden nicht hinzugefügt, die Regel wird hinzugefügt, wenn zumindest eine Regeleinstellung eindeutig ist).
/merge <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts durch Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen: **Mit bestehenden Regeln zusammenführen** (neue Regeln werden nicht dupliziert, wenn identische Regeln bereits vorhanden sind).
/clear	Liste der Regeln für die Kontrolle des Programmstarts leeren

Liste der Regeln zur Gerätekontrolle aus einer Datei ergänzen. KAVSHELL DEVCONTROL

Mithilfe des Befehls `KAVSHELL DEVCONTROL` können Sie entsprechend dem ausgewählten Prinzip Regeln aus einer xml-Datei zur Regelliste der Aufgabe zur Gerätekontrolle hinzufügen sowie alle festgelegten Regeln aus der Liste löschen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <vollständiger Pfad zur xml-Datei> | /replace <vollständiger Pfad zur xml-Datei> | /merge <vollständiger Pfad zur xml-Datei> | /clear
```

Beispiel für den Befehl KAVSHELL DEVCONTROL

► *Um Regeln aus einer xml-Datei nach dem Prinzip **Zu den bestehenden Regeln hinzufügen** zu den festgelegten Regeln zur Gerätekontrolle hinzuzufügen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Je nach Syntax der Schlüssel können Sie das Prinzip für das Hinzufügen neuer Regeln aus der angegebenen xml-Datei zur Liste der festgelegten Regeln für die Aufgabe zur Gerätekontrolle wählen (s. Tabelle unten).

Tabelle 87. Schlüssel des Befehls KAVSHELL DEVCONTROL

Schlüssel	Beschreibung
/append <vollständiger Pfad der xml-Datei>	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Zu den bestehenden Regeln hinzufügen** (Regeln mit identischen Einstellungen werden verdoppelt).
/replace <vollständiger Pfad der xml-Datei>	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Bestehende Regeln ersetzen** (Regeln mit identischen Einstellungen werden nicht hinzugefügt, die Regel wird hinzugefügt, wenn zumindest eine Regeleinstellung eindeutig ist).
/merge <vollständiger Pfad der xml-Datei>	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen: **Mit bestehenden Regeln zusammenführen** (neue Regeln werden nicht dupliziert, wenn identische Regeln bereits vorhanden sind).
/clear	Liste der Regeln zur Gerätekontrolle leeren.

Aufgabe zum Update der Programm-Datenbanken von Kaspersky Embedded Systems Security starten. KAVSHELL UPDATE

Mit dem Befehl `KAVSHELL UPDATE` können Sie die Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security im Synchronmodus starten.

Die Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security, die mit dem Befehl `KAVSHELL UPDATE` gestartet wird, ist temporär. Sie wird nur während ihrer Ausführung in der Programmkonsole angezeigt. Das Protokoll der Aufgabenausführung wird gleichzeitig erzeugt. Es wird in den **Protokollen der Aufgabenausführung** der Programmkonsole angezeigt. Für Update-Aufgaben, die mit dem Befehl `KAVSHELL UPDATE` erstellt und gestartet wurden, sowie für Update-Aufgabe, die in der Programmkonsole angelegt wurden, können die Richtlinien der Anwendung Kaspersky Security Center übernommen werden. Informationen darüber, wie Kaspersky Embedded Systems Security auf Computer mithilfe der Anwendung Kaspersky Security Center verwaltet wird, finden Sie im Abschnitt "Verwaltung von Kaspersky Embedded Systems Security mithilfe von Kaspersky Security Center".

Wenn Sie in dieser Aufgabe den Pfad eine Update-Quelle angeben, können Sie Umgebungsvariable verwenden.

Wenn Sie eine Umgebungsvariable verwenden, die einem Benutzer zugeordnet ist, führen Sie den Befehl KAVSHELL UPDATE mit den Rechten dieses Benutzers aus.

Syntax des Befehls KAVSHELL UPDATE

```
KAVSHELL UPDATE < Update-Quelle | /AK | /KL> [/NOUSEKL] [/PROXY:<Adresse>:<Port>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<Benutzername>] [/PROXYPWD:<Kennwort>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE] [/TIMEOUT:<Sekunden>] [/REG:<Code iso3166>] [/W:<Name des Protokolls der Aufgabenausführung>] [/ALIAS:<Alias des Aufgabennamens>]
```

Der Befehl KAVSHELL UPDATE enthält sowohl obligatorische als auch Reserveschlüssel, deren Verwendung optional ist (s. Tabelle unten).

Beispiel für den Befehl KAVSHELL UPDATE

► *Um eine benutzerdefinierte Aufgabe zum Update der Programm-Datenbanken zu starten, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE
```

► *Um eine Aufgabe zum Update der Programm-Datenbanken zu starten, dessen Updatedateien im Netzwerkordner \\server\bases gespeichert sind, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE \\server\bases
```

► *Um eine Aufgabe zum Update vom FTP-Server ftp://dnl-ru1.kaspersky-labs.com/ zu starten und alle Ereignisse der Aufgabe in die Log-Datei c:\update_report.log zu schreiben, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

► *Stellen Sie zum Herunterladen von Updates der Programm-Datenbanken für Kaspersky Embedded Systems Security vom Update-Server von Kaspersky Lab über einen Proxyserver (Adresse: proxy.company.com, Port: 8080) eine Verbindung zur Update-Quelle her. Um unter Verwendung der integrierten NTLM-Authentifizierung von Microsoft Windows (Benutzername: inetuser, Passwort: 123456) auf den Computer zuzugreifen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456
```

Tabelle 88. Schlüssel des Befehls KAVSHELL UPDATE

Schlüssel	Beschreibung
Update-Quelle (obligatorischer Schlüssel). Geben Sie eine oder mehrere Quellen an. Kaspersky Embedded Systems Security greift der angegebenen Reihenfolge nach auf die Update-Quellen zu. Trennen Sie die Quellen durch Leerzeichen.	
<Pfad im Format UNC>	Benutzerdefinierte Update-Quelle Pfad des Netzwerk-Update-Ordners im UNC-Format.
<URL>	Benutzerdefinierte Update-Quelle Adresse eines HTTP- oder FTP-Servers, auf dem sich der Update-Ordner befindet.

Schlüssel	Beschreibung
<Lokaler Ordner>	Benutzerdefinierte Update-Quelle Ordner auf dem geschützten Computer.
/AK	Kaspersky Security Center-Administrationsserver als Update-Quelle
/KL	Update-Server von Kaspersky Lab als Update-Quelle
/NOUSEKL	Die Kaspersky-Lab-Update-Server nicht verwenden, wenn die anderen angegebenen Update-Quellen nicht verfügbar sind (Quellen, die standardmäßig verwendet werden).
Proxyserver-Einstellungen	
/PROXY:<Adresse>:<Port>	Netzwerkname oder IP-Adresse des Proxyservers und dessen Port. Wenn dieser Schlüssel nicht angegeben ist, verwendet stellt Kaspersky Embedded Systems Security automatisch die Einstellungen des Proxyservers fest, der im lokalen Netzwerk verwendet wird.
/AUTHTYPE:<0-2>	Dieser Schlüssel bestimmt die Authentifizierungsmethode für den Zugriff auf den Proxyserver. Folgende Werte sind möglich: **0** – integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Embedded Systems Security greift unter dem Benutzerkonto **Lokales System** (**SYSTEM**) auf den Proxyserver zu; **1** – integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Embedded Systems Security greift unter dem Benutzerkonto, dessen Login-Daten durch die Schlüssel /PROXYUSER und /PROXYPWD angegeben werden, auf den Proxyserver zu; **2** – Authentifizierung mit Benutzername und Kennwort, die durch die Schlüssel /PROXYUSER und /PROXYPWD (basic authentication) angegeben werden. Wenn für den Zugriff auf den Proxyserver keine Authentifizierung erforderlich ist, muss dieser Schlüssel nicht angeben werden.
/PROXYUSER:<Benutzername>	Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn Sie den Schlüsselwert /AUTHTYPE:0 angeben, werden die Schlüssel /PROXYUSER:<Benutzername> und /PROXYPWD:<Kennwort> ignoriert.
/PROXYPWD:<Kennwort>	Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn Sie den Schlüsselwert /AUTHTYPE:0 angeben, werden die Schlüssel /PROXYUSER:<Benutzername> und /PROXYPWD:<Kennwort> ignoriert. Wenn Sie den Schlüssel /PROXYUSER angeben und den Schlüssel /PROXYPWD auslassen, wird das Kennwort als leer betrachtet.
/NOPROXYFORKL	Proxyserver-Einstellungen für die Verbindung zu den Kaspersky-Lab-Update-Servern nicht verwenden (Sie werden standardmäßig verwendet)
/USEPROXYFORCUSTOM	Proxyserver-Parameter für die Verbindung zu benutzerdefinierten Update-Quellen verwenden (Sie werden standardmäßig nicht verwendet).
/USEPROXYFORLOCAL	Proxyserver-Parameter für die Verbindung zu lokalen Update-Quellen verwenden. Wenn kein Wert angegeben wurde, wird der Wert **Für lokale Adressen keinen Proxyserver verwenden** verwendet.
Allgemeine Parameter eines FTP- und HTTP-Servers	
/NOFTPPASSIVE	Wenn dieser Schlüssel angegeben ist, verwendet Kaspersky Embedded Systems Security den FTP-Server im aktiven Modus für eine Verbindung zum geschützten Computer. Wenn dieser Schlüssel nicht angegeben ist, verwendet Kaspersky Embedded Systems Security nach Möglichkeit den passiven Modus des FTP-Servers.

Schlüssel	Beschreibung
/TIMEOUT:<Anzahl der Sekunden>	Wartezeit für Verbindung mit einem FTP- oder HTTP-Server. Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Embedded Systems Security den voreingestellten Standardwert 10 s. Als Wert für diesen Schlüssel können nur ganze Zahlen eingegeben werden.
/REG:<Code iso3166>	Regionale Einstellungen Dieser Schlüssel wird beim Update-Download von den Update-Servern von Kaspersky Lab verwendet. Kaspersky Embedded Systems Security optimiert den Update-Download auf den geschützten Computer, indem der geografisch am nächsten liegenden Update-Server ausgewählt wird. Geben Sie als Schlüsselwert den Buchstabencode des Landes an, in dem sich der geschützte Computer befindet. Beachten Sie dabei ISO-Standard 3166-1 (z. B. "/REG:gr" oder "/REG:RU"). Wenn dieser Schlüssel nicht angegeben oder ein nicht existierender Landescode angegeben wird, erkennt Kaspersky Embedded Systems Security den Ort des geschützten Computers entsprechend den regionalen Einstellungen des Computers auf dem die Programmkonsole installiert ist.
/ALIAS:<Alias des Aufgabenamens>	Dieser Schlüssel weist der Aufgabe einen temporären Namen zu, mit dem darauf zugegriffen werden kann, während sie ausgeführt wird. Mit dem Befehl TASK können Sie beispielsweise eine Aufgabenstatistik anzeigen lassen. Der Alias des Aufgabenamens muss unter den alternativen Namen für die Aufgaben aller Funktionalkomponenten von Kaspersky Embedded Systems Security einmalig sein. Wenn dieser Schlüssel nicht festgelegt ist, erhält die Aufgabe den alternativen Name update_<kavshell_pid> (z.B. update_1234). In der Programmkonsole erhält die Aufgabe den Namen Update-databases (<Datum und Uhrzeit>) (z. B. Update-databases 8/16/2007 5:41:02 PM).
/W:<Name des Protokolls der Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Embedded Systems Security das Protokoll der Aufgabenausführung mit dem durch diesen Schlüssel vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse in der Aufgabe. Im Protokoll werden die Ereignisse aufgezeichnet, die durch die Einstellungen für die Protokolle der Aufgabenausführung und das Ereignisprotokoll von Kaspersky Embedded Systems Security in der "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten **Protokolle der Aufgabenausführung** der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen oder es erfolgt aber eine Fehlermeldung.

Rückgabecodes für den Befehl KAVSHELL UPDATE (auf Seite 549).

Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security. KAVSHELL ROLLBACK

Mit dem Befehl `KAVSHELL ROLLBACK` können Sie die Systemaufgabe Rollback des Datenbank-Updates von Kaspersky Embedded Systems Security ausführen. Dadurch werden die Datenbanken von Kaspersky Embedded Systems Security mit den zuvor installierten Updates wieder hergestellt. Der Befehl wird synchron ausgeführt.

Syntax des Befehls

```
KAVSHELL ROLLBACK
```

Rückgabecode für den Befehl KAVSHELL ROLLBACK (auf Seite 549)

Verwalten der Protokollanalyse. KAVSHELL TASK LOG-INSPECTOR

Der Befehl `KAVSHELL TASK LOG-INSPECTOR` kann verwendet werden, um die Integrität der Umgebung auf der Grundlage der Windows-Ereignisprotokollanalyse zu überwachen.

Syntax des Befehls

```
KAVSHELL TASK LOG-INSPECTOR
```

Befehlsbeispiele

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Tabelle 89. KAVSHELL TASK LOG-INSPECTOR zum Ändern des Befehls

Schlüssel	Beschreibung
/START	Die angegebene Aufgabe im asynchronen Modus starten.
/STOP	Beenden einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (zum Beispiel, *Läuft*, *Abgeschlossen*, *Angehalten*, *Beendet*, *Fehlgeschlagen*, *Wird gestartet*, *Wird wiederhergestellt*).
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet wurden.

Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR" auf Seite 547).

Erstellung eines Protokolls zur Ablaufverfolgung aktivieren, anpassen und deaktivieren. KAVSHELL TRACE

Mit dem Befehl `KAVSHELL TRACE` können Sie das Anlegen eines Ablaufverfolgungsprotokolls für alle Subsysteme von Kaspersky Embedded Systems Security aktivieren oder deaktivieren, und die entsprechende Protokollierungsstufe festlegen.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet.

Syntax des Befehls KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<Ordner mit Dateien des Ablaufverfolgungsprotokolls>
[/S:<maximale Größe einer Log-Datei in MB>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Wenn ein Protokoll zur Ablaufverfolgung geführt wird und Sie seine Parameter ändern möchten, geben Sie den Befehl `KAVSHELL TRACE` mit dem Schlüssel /ON ein und geben Sie die Parameter für das Protokoll zur Ablaufverfolgung mit den Schlüsselwerten /S und /LVL an (s. Tabelle unten).

Tabelle 90. Schlüssel des Befehls KAVSHELL TRACE

Schlüssel	Beschreibung
/ON	Führen eines Protokolls zur Ablaufverfolgung aktivieren
/F:<Ordner für Log-Dateien des Ablaufverfolgungsprotokolls>	Dieser Schlüssel gibt den vollständigen Pfad des Ordners an, in dem die Log-Dateien des Ablaufverfolgungsprotokolls gespeichert werden (obligatorischer Schlüssel). Wenn Sie den Pfad eines nicht vorhandenen Ordners angeben, wird kein Protokoll zur Ablaufverfolgung erstellt. Pfade zu Ordnern auf Netzlaufwerken von anderen Computern können nicht angegeben werden. Wenn der Name eines Ordners, dessen Pfad Sie als Schlüsselwert angeben, ein Leerzeichen enthält, schreiben Sie den Pfad in Anführungszeichen (z. B. /F:"C\Trace Folder"). Wenn Sie den Pfad von Log-Dateien des Ablaufverfolgungsprotokolls angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariablen sind dagegen nicht zulässig.
/S:<maximale Größe einer Log-Datei in MB>	Dieser Schlüssel bestimmt die maximale Größe einer Log-Datei des Ablaufverfolgungsprotokolls. Sobald eine Log-Datei den Grenzwert erreicht, beginnt Kaspersky Embedded Systems Security, die Daten in eine neue Datei zu schreiben. Die bisherige Log-Datei wird gespeichert. Wenn Sie diesen Schlüssel nicht angeben, beträgt die maximale Größe für eine Log-Datei 50 MB.
/LVL:debug|info|warning|error|critical	Dieser Schlüssel legt die Genauigkeitsstufe des Protokolls fest. Auf der maximalen Stufe (**Alle Debug-Informationen**) werden alle Ereignisse protokolliert, auf der minimalen Stufe (**Kritische Ereignisse**) nur kritische Ereignisse. Wenn dieser Schlüssel nicht angegeben ist, werden Ereignisse mit der Genauigkeitsstufe **Alle Debug-Informationen** im Protokoll zur Ablaufverfolgung aufgezeichnet.
/OFF	Dieser Schlüssel deaktiviert das Führen des Protokolls zur Ablaufverfolgung.

Beispiel für den Befehl KAVSHELL TRACE

► *Um das Anlegen eines Protokolls zur Ablaufverfolgung mit der Genauigkeitsstufe **Alle Debug-Informationen** und einer maximalen Größe der Log-Datei von 200 MB zu aktiveren und die Log-Datei im Ordner C:\Trace Folder zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Um das Anlegen eines Protokolls zur Ablaufverfolgung mit der Genauigkeitsstufe **Wichtige Ereignisse** zu aktiveren und die Log-Datei im Ordner C:\Trace Folder zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Um die Erstellung eines Protokolls zur Ablaufverfolgung zu aktivieren, führen Sie folgenden Befehl aus:*

```
KAVSHELL TRACE /OFF
```

Rückgabecodes für den Befehl KAVSHELL TRACE (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TRACE" auf Seite 550).

Log-Dateien für Kaspersky Embedded Systems Security defragmentieren. KAVSHELL VACUUM

Mithilfe des Befehls `KAVSHELL VACUUM` können Sie Log-Dateien für Ereignisse des Programms defragmentieren. Dadurch können System- und Programmfehler aufgrund der Speicherung einer großen Anzahl von Log-Dateien, die aufgrund von Programmereignissen erzeugt wurden, vermieden werden.

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Es wird empfohlen, den Befehl `KAVSHELL VACUUM` für die Optimierung der Speicherung von Log-Dateien bei häufigen Starts der Aufgaben zur Untersuchung auf Befehl oder der Update-Aufgabe zu verwenden. Bei der Ausführung des Befehls erneuert Kaspersky Embedded Systems Security die logische Struktur der Log-Dateien des Programms, die auf dem geschützten Computer im angegebenen Pfad gespeichert sind.

Standardmäßig werden die Log-Dateien der Ereignisse bei der Ausführung des Programms im Pfad C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\2.3\Reports gespeichert. Wenn Sie manuell einen anderen Pfad zum Speichern von Protokollen angegeben haben, defragmentiert der Befehl `KAVSHELL VACUUM` die Dateien im Ordner, der in den Einstellungen der Protokolle von Kaspersky Embedded Systems Security angegeben ist.

> Eine große Anzahl von zu defragmentierenden Log-Dateien für Ereignisse verlängert die Zeit für die Ausführung des Befehls `KAVSHELL VACUUM`.

Während der Ausführung des Befehls `KAVSHELL VACUUM` ist die Ausführung der Aufgaben Echtzeitschutz und Computer-Kontrolle unmöglich. Der Defragmentierungsvorgang sperrt den Zugang auf das Protokoll von Kaspersky Embedded Systems Security und verbietet ein Protokollieren von Ereignissen. Damit die Sicherheitsstufe des Computers nicht verringert wird, wird empfohlen, die Ausführung des Befehls `KAVSHELL VACUUM` im Voraus zur arbeitsfreien Zeit zu planen.

► *Um eine Defragmentierung der Log-Dateien für Ereignisse bei der Ausführung von Kaspersky Embedded Systems Security durchzuführen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL VACUUM
```

Der Befehl kann beim Start mit Berechtigungen des Benutzerkontos des lokalen Administrators ausgeführt werden.

iSwift-Datenbank leeren. KAVSHELL FBRESET

Kaspersky Embedded Systems Security verwendet die iSwift-Technologie, um eine erneute Untersuchung einer Datei zu vermeiden, wenn die Datei seit der vorherigen Untersuchung nicht verändert wurde (**iSwift-Technologie verwenden**).

Kaspersky Embedded Systems Security erstellt im Ordner %SYSTEMDRIVE%\System Volume Information die Dateien klamfb.dat und klamfb2.dat, die Informationen über bereits untersuchte, virenfreie Objekte enthalten. Je größer die Anzahl der Dateien, die von Kaspersky Embedded Systems Security untersucht worden sind, desto größer ist die Datei klamfb.dat (klamfb2.dat). Diese Datei enthält nur aktuelle Informationen über die tatsächlich im System vorhandenen Dateien: Wenn eine Datei im System gelöscht wird, löscht Kaspersky Embedded Systems Security die entsprechenden Informationen aus der Datei klamfb.dat.

Um diese Datei zu leeren, verwenden Sie den Befehl `KAVSHELL FBRESET`.

Berücksichtigen Sie folgende Besonderheiten bei der Arbeit mit dem Befehl `KAVSHELL FBRESET`:

- Wenn die Datei klamfb.dat mithilfe des Befehls KAVSHELL FBRESET geleert wird, hält Kaspersky Embedded Systems Security den Schutz nicht an (im Gegensatz zum manuellen Löschen der Datei klamfb.dat).
- Nachdem die Datei klamfb.dat geleert wurde, kann sich die durch Kaspersky Embedded Systems Security verursachte Belastung des Computers erhöhen. Dabei untersucht Kaspersky Embedded Systems Security alle Dateien, auf die nach dem Leeren der Datei klamfb.dat zum ersten Mal zugegriffen wird. Nach der Untersuchung trägt Kaspersky Embedded Systems Security erneut Informationen über ein untersuchtes Objekt in die Datei klamfb.dat ein. Bei einem erneuten Zugriff auf dieses Objekt erlaubt die iSwift-Technologie es, die Datei nicht erneut zu scannen, falls sie nicht verändert wurde.

Zur Ausführung des Befehls `KAVSHELL FBRESET` muss die Befehlszeile im Benutzerkonto SYSTEM gestartet werden.

Anlegen von Dump-Dateien ein- und ausschalten. KAVSHELL DUMP

Mit dem Befehl `KAVSHELL DUMP` können Sie das Erstellen von Speicherauszügen (Dump-Dateien), die bei Abstürzen für die Prozesse von Kaspersky Embedded Systems Security erstellt werden, aktivieren oder deaktivieren (siehe folgende Tabelle). Außerdem können Sie jederzeit Speicher-Images der von Kaspersky Embedded Systems Security ausgeführten Prozesse anfertigen.

Damit die Dump-Datei erfolgreich erstellt werden kann, muss der Befehl `KAVSHELL DUMP` unter dem lokalen Systemkonto (SYSTEM) ausgeführt werden.

Syntax des Befehls KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<Ordner mit Dump-Datei>|/SNAPSHOT /F:<Ordner mit Dump-Datei>
/ P:<pid> | /OFF>
```

Tabelle 91. Schlüssel des Befehls KAVSHELL DUMP

Schlüssel	Beschreibung
/ON	Aktiviert die Erstellung einer Dump-Datei für einen Prozess im Falle seines Absturzes.
/F:<Pfad der Dump-Dateien>	Dieser Schlüssel ist obligatorisch. Er gibt den Pfad des Ordners an, in dem die Dump-Datei gespeichert wird. Pfade zu Ordnern auf Netzlaufwerken von anderen nicht geschützten Computern können nicht angegeben werden. Wenn Sie einen Pfad für Dump-Dateien angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariable sind dagegen nicht zulässig.
/SNAPSHOT	Fertigt ein Speicher-Image des laufenden Prozesses mit PID an und speichert die Dump-Datei im Ordner, dessen Pfad durch den Schlüssel /F definiert wird.
/P	Prozess-PID, die im Task-Manager von Microsoft Windows angezeigt wird.
/OFF	Deaktiviert die Erstellung einer Dump-Datei im Falle seines Absturzes.

Rückgabecodes für den Befehl KAVSHELL DUMP (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL DUMP" auf Seite 551).

Beispiel für den Befehl KAVSHELL DUMP

► *Um die Erstellung einer Dump-Datei zu aktivieren und die erstellte Dump-Datei im Ordner C:\Dump Folder zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

► *Um ein Speicherabbild eines Prozesses mit dem Bezeichner 1234 anzufertigen und im Ordner C:/Dumps zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /F:1234
```

► *Um die Erstellung einer Dump-Datei zu aktivieren, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /OFF
```

Einstellungen importieren. KAVSHELL IMPORT

Mit dem Befehl `KAVSHELL IMPORT` können Sie Einstellungen, Funktionen und Aufgaben von Kaspersky Embedded Systems Security aus einer Konfigurationsdatei in Kaspersky Embedded Systems Security auf den geschützten Computer importieren. Mit dem Befehl `KAVSHELL EXPORT` können Sie eine Konfigurationsdatei erstellen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL IMPORT

```
KAVSHELL IMPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiel für den Befehl KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tabelle 92. Schlüssel des Befehls KAVSHELL IMPORT

Schlüssel	Beschreibung
<Name und Pfad der Konfigurationsdatei>	Name der Konfigurationsdatei, aus der die Parameter importiert werden. Wenn Sie einen Dateipfad angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariablen sind dagegen nicht zugelassen.

Rückgabecodes für den Befehl KAVSHELL IMPORT (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL IMPORT" auf Seite 551).

Einstellungen exportieren. KAVSHELL EXPORT

Mit dem Befehl `KAVSHELL EXPORT` können Sie alle Einstellungen von Kaspersky Embedded Systems Security und die aktuellen Aufgaben in eine Konfigurationsdatei exportieren, um sie auf anderen Computern in Kaspersky Embedded Systems Security zu importieren.

Syntax des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiel für den Befehl KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tabelle 93. Schlüssel des Befehls KAVSHELL EXPORT

Schlüssel	Beschreibung
<Name und Pfad der Konfigurationsdatei>	Name der Konfigurationsdatei, in der die Parameter gespeichert werden. Sie können der Konfigurationsdatei eine beliebige Erweiterung zuweisen. Wenn Sie einen Dateipfad angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariablen sind dagegen nicht zugelassen.

Rückgabecodes für den Befehl KAVSHELL EXPORT (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL EXPORT" auf Seite 552).

Integration in Microsoft Operation Management Suite. KAVSHELL OMSINFO

Mithilfe des Befehls KAVSHELL OMSINFO können Sie den Programmstatus sowie Informationen über die von den Antiviren-Datenbanken und dem KSN-Dienst gefundenen Bedrohungen anzeigen. Die Informationen über Bedrohungen werden den verfügbaren Ereignisprotokollen entnommen.

Syntax des Befehls KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <vollständiger Pfad zur erstellten Datei samt Dateiname>
```

Beispiel für den Befehl KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabelle 94. Schlüssel des Befehls KAVSHELL OMSINFO

Schlüssel	Beschreibung
<Pfad zur erstellten Datei samt Dateiname>	Name der erstellten Datei, die Informationen über den Programmstatus und die erkannten Bedrohungen enthalten wird.

Rückgabecodes der Befehlszeile

In diesem Abschnitt

Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP

Tabelle 95. Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist der Dienst von Kaspersky Embedded Systems Security bereits gestartet oder schon beendet)
-7	Service ist nicht registriert
-8	Der automatische Start des Dienstes ist deaktiviert
-9	Versuch zum Starten des Dienstes unter einem anderen Benutzerkonto war erfolglos (in der Grundeinstellung arbeitet der Dienst von Kaspersky Embedded Systems Security unter dem Systemkonto).
-99	Unbekannter Fehler

Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL

Tabelle 96. Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt (Es wurden keine Bedrohungen gefunden)
1	Vorgang abgebrochen
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (Datei mit Liste der Untersuchungsbereiche nicht gefunden)
-5	Ungültige Befehlssyntax oder Untersuchungsbereich nicht festgelegt
-80	Infizierte und andere gefundene Objekte
-81	Möglicherweise infizierte Objekte gefunden
-82	Es wurden Verarbeitungsfehler erkannt
-83	Es wurden nicht untersuchte Objekte gefunden
-84	Es wurden beschädigte Objekte gefunden
-85	Das Erstellen eines Protokolls der Aufgabenausführung ist fehlgeschlagen.
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR

Tabelle 97. Rückgabecode für den Befehl KAVSHELL TASK LOG-INSPECTOR

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-6	Ungültiger Vorgang (zum Beispiel ist der Dienst von Kaspersky Embedded Systems Security bereits gestartet oder schon beendet)
402	Aufgabe ist schon gestartet (für Schlüssel /STATE)

Rückgabecodes für den Befehl KAVSHELL TASK

Tabelle 98. Rückgabecodes für den Befehl KAVSHELL TASK

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (Aufgabe nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist die Aufgabe nicht gestartet, schon gestartet oder kann nicht angehalten werden)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel
401	Aufgabe nicht gestartet (für Schlüssel /STATE)
402	Aufgabe ist schon gestartet (für Schlüssel /STATE)
403	Aufgabe ist schon angehalten (für Schlüssel /STATE)
-404	Fehler bei Vorgangsausführung (Ändern des Aufgabenstatus führte zum Absturz)

Rückgabecodes für den Befehl KAVSHELL RTP

Tabelle 99. Rückgabecodes für den Befehl KAVSHELL RTP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keine bzw. alle Aufgaben des Echtzeitschutzes nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel Aufgabe ist schon gestartet oder schon beendet)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL UPDATE

Tabelle 100. Rückgabecodes für den Befehl KAVSHELL UPDATE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
200	Alle Objekte sind aktuell (Datenbanken oder Programm-Komponenten sind in einem aktuellen Zustand)
-2	Service nicht gestartet
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-99	Unbekannter Fehler
-206	Updatedateien sind nicht vorhanden oder falsches Format
-209	Fehler bei Verbindung mit Update-Quelle
-232	Authentifizierungsfehler bei Verbindung mit dem Proxyserver
-234	Fehler bei Verbindung zum Programm Kaspersky Security Center
-235	Kaspersky Embedded Systems Security hat die Authentifizierungsprüfung beim Verbinden mit der Update-Quelle nicht bestanden
-236	Die Datenbanken von Kaspersky Embedded Systems Security sind beschädigt
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Tabelle 101. Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-99	Unbekannter Fehler
-221	Backup-Kopie der Datenbanken nicht gefunden
-222	Backup-Kopie der Datenbanken ist beschädigt

Rückgabecodes für den Befehl KAVSHELL LICENSE

Tabelle 102. Rückgabecodes für den Befehl KAVSHELL LICENSE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Unzureichende Rechte für die Schlüsselverwaltung
-4	Kein Schüssel mit der angegebenen Nummer gefunden
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Schlüssel nicht hinzugefügt)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel
-303	Die Lizenz erstreckt sich auf ein anderes Programm

Rückgabecodes für den Befehl KAVSHELL TRACE

Tabelle 103. Rückgabecodes für den Befehl KAVSHELL TRACE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keinen Pfad gefunden, der als Pfad zum Ordner mit den Log-Dateien für das Ablaufverfolgungsprotokoll führt)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch, den Befehl KAVSHELL TRACE/OFF auszuführen, wenn Erstellen des Protokolls zur Ablaufverfolgung schon deaktiviert ist)
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL FBRESET

Tabelle 104. Rückgabecodes für den Befehl KAVSHELL FBRESET

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL DUMP

Tabelle 105. Rückgabecodes für den Befehl KAVSHELL DUMP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keinen Pfad gefunden, der als Pfad zum Ordner mit der Dump-Datei führt; keinen Prozess mit PID gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch, den Befehl KAVSHELL DUMP /OFF auszuführen, wenn Erstellen der Dump-Datei deaktiviert ist)
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL IMPORT

Tabelle 106. Rückgabecodes für den Befehl KAVSHELL IMPORT

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (zu importierende Konfigurationsdatei nicht gefunden)
-5	Ungültige Syntax
-99	Unbekannter Fehler
501	Der Vorgang wurde erfolgreich ausgeführt. Bei der Befehlsausführung ist jedoch ein Fehler bzw. Kommentar aufgetreten (z. B. Kaspersky Embedded Systems Security hat die Einstellungen einer bestimmten funktionellen Komponente nicht importiert).
-502	Zu importierende Datei ist nicht vorhanden oder hat ein unbekanntes Format

Feedback-Code	Beschreibung
-503	Inkompatible Einstellungen (Konfigurationsdatei aus einem anderen Programm oder einer höhere oder inkompatiblen Version von Kaspersky Embedded Systems Security exportiert)

Rückgabecodes für den Befehl KAVSHELL EXPORT

Tabelle 107. Rückgabecodes für den Befehl KAVSHELL EXPORT

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-5	Ungültige Syntax
-10	Konfigurationsdatei konnte nicht erstellt werden (beispielsweise kein Zugang zum Ordner, welcher im Pfad vorgegeben wurde)
-99	Unbekannter Fehler
501	Der Vorgang wurde erfolgreich ausgeführt. Bei der Befehlsausführung ist jedoch ein Fehler bzw. Kommentar aufgetreten (z. B. Kaspersky Embedded Systems Security hat die Einstellungen einer bestimmten funktionellen Komponente nicht exportiert).

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Informationen darüber, wie und zu welchen Bedingungen Sie technischen Support erhalten.

In diesem Kapitel

Wie Sie technischen Support erhalten

Wenn Sie in der Dokumentation oder in anderen Informationsquellen zum Programm keine Lösung für Ihr Problem gefunden haben, empfehlen wir Ihnen, den Technischen Support zu kontaktieren. Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Der Technische Support steht nur den Benutzern zur Verfügung, die eine kommerzielle Lizenz für die Programmnutzung gekauft haben. Benutzer, die eine Testlizenz verwenden, können den Technischen Support nicht nutzen.

Bevor Sie sich an unseren Technischen Support wenden, machen Sie sich bitte mit unseren Support-Regeln vertraut.

Eine Kontaktaufnahme mit den Experten des Technischen Supports ist auf folgende Weise möglich:

- Technischen Support anrufen
- Versand einer Anfrage an den Technischen Support von Kaspersky Lab über das Portal Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Hotline des Technischen Supports

Der Technische Support ist in vielen Ländern telefonisch erreichbar. Informationen darüber, wie und wo Sie in Ihrer Region technischen Support erhalten können, finden Sie auf der Website des Technischen Supports von Kaspersky Lab (https://support.kaspersky.com/b2b/de).

Bevor Sie sich an unseren Technischen Support wenden, machen Sie sich bitte mit unseren Support-Regeln (https://support.kaspersky.com/support/rules#de_de) vertraut.

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) ist ein Portal für Unternehmen, die Programme von Kaspersky Lab verwenden. Über das Portal Kaspersky CompanyAccount können Benutzer mit Kaspersky-Lab-Experten mithilfe von Online-Anfragen kommunizieren. Über das Portal Kaspersky CompanyAccount kann der Status der Verarbeitung elektronischer Anfragen durch Kaspersky Lab-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 Lab 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 http://support.kaspersky.com/de/faq/companyaccount_help.

Protokolldatei und AVZ-Skript verwenden

Wenn Sie sich mit einem Problem an die Experten des Technischen Supports von Kaspersky Lab wenden, werden Sie möglicherweise darum gebeten, einen Bericht über Kaspersky Embedded Systems Security zu erstellen und den Bericht an den Technischen Support von Kaspersky Lab zu schicken. Zusätzlich können die Experten des Technischen Supports von Kaspersky Lab eine Protokolldatei anfordern. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Experten des Technischen Supports von Kaspersky Lab ein AVZ-Skript erstellen, das dann an Sie geschickt wird. Mit Hilfe von AVZ-Skripten können die laufenden Prozesse auf Bedrohungen analysiert, der Computer auf Bedrohungen untersucht, infizierte Dateien desinfiziert oder entfernt und ein Bericht über die Ergebnisse der Untersuchung des Computers erstellt werden.

Für eine effektivere Unterstützung im Falle des Auftretens von Fragen zur Arbeit des Programms können die Fachleute des Technischen Supports Sie bitten, zur Fehlersuche für den Zeitraum der Diagnose die Programmeinstellungen zu ändern. Hierzu können die folgenden Maßnahmen erforderlich werden:

- Aktivierung der Funktion zur Verarbeitung und Speicherung erweiterter Diagnosedaten.
- Feineinstellung verschiedener Programmkomponenten, die mithilfe der auf der Benutzeroberfläche standardmäßig zur Verfügung stehenden Mittel nicht möglich ist.
- Änderung der Einstellungen für die Speicherung und den Versand verarbeiteter Diagnosedaten.
- Konfiguration der Überwachung und Protokollierung des Netzwerkverkehrs in einer Datei.

Glossar

A

Administrationsserver

Programmkomponente von Kaspersky Security Center, mit der die zentralisierte Speicherung von Informationen über die im Unternehmensnetzwerk installierten Programme von Kaspersky Lab realisiert wird. Die Verwaltung dieser Programme erfolgt ebenfalls über diese Komponente.

Aktiver Schlüssel

Der Schlüssel, der momentan vom Programm verwendet wird.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die Kaspersky Lab zum Zeitpunkt der Veröffentlichung der Antiviren-Datenbanken bekannt waren. Mithilfe der Einträge in den Antiviren-Datenbanken wird in den Untersuchungsobjekten schädlicher Code identifiziert. Die Antiviren-Datenbanken werden von den Experten von Kaspersky Lab gepflegt und stündlich aktualisiert.

Archiv

Eine oder mehrere Dateien, die komprimiert und in einer einzigen Datei zusammengefasst wurden. Ein spezielles Archivierungsprogramm ist zum Komprimieren und Entpacken der Daten erforderlich.

Aufgabe

Das Kaspersky-Lab-Programm führt seine Funktionen in Form von Aufgaben aus, zum Beispiel: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers und Update der Programm-Datenbanken.

Aufgabeneinstellungen

Programmeinstellungen, die für den jeweiligen Aufgabentyp gelten.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die ordnungsgemäße Ausführung des auf dem Computer installierten Betriebssystems und der Software benötigt wird. Diese Objekte werden bei jedem Start des Betriebssystems ausgeführt. Es gibt Viren, die genau diese Objekte infizieren können, was beispielsweise dazu führen kann, dass das Betriebssystem nicht gestartet wird.

B

Backup

Ein spezieller Speicher für Backup-Kopien von Dateien, die vor dem Desinfektionsversuch oder dem Löschen der Dateien erstellt werden.

D

Dateimaske

Darstellung eines Dateinamens mithilfe von Platzhaltern. Die Standard-Platzhalter, die in Dateimasken verwendet werden, sind * und ?, wobei * eine beliebige Anzahl an Zeichen und ? ein beliebiges Einzelzeichen ersetzt.

Desinfektion

Verarbeitungsmethode für infizierte Objekte, die eine vollständige oder teilweise Wiederherstellung der Daten zum Ergebnis hat. Nicht alle infizierten Objekte können desinfiziert werden.

E

Echtzeitschutz

Ausführungsmodus des Programms, in dem Objekte in Echtzeit auf das Vorhandensein von schädlichem Code untersucht werden.

Das Programm fängt alle Versuche ab, ein Objekt zu öffnen (lesen, schreiben oder ausführen), und untersucht die Objekte auf Bedrohungen. Nicht infizierte Objekte werden an den Benutzer weitergegeben, während Objekte, die Bedrohungen enthalten oder möglicherweise infiziert sind, gemäß den Aufgabeneinstellungen verarbeitet werden (desinfiziert, gelöscht oder in Quarantäne verschoben).

Ereignispriorität

Eigenschaft eines Ereignisses, das während der Ausführung eines Kaspersky-Lab-Programms aufgetreten ist. Dem Ereignis wird eine von vier Signifikanzen zugewiesen:

- Kritisches Ereignis
- Fehler
- Warnung
- Info

Ereignisse vom gleichen Typ können je nach der Situation, in der sie auftreten, unterschiedliche Signifikanzen haben.

F

Fehlalarm

Eine Situation, in der ein Programm von Kaspersky Lab ein nicht infiziertes Objekt als infiziert betrachtet, weil dessen Code dem eines Virus ähnelt.

H

Heuristische Analyse

Technologie zur Erkennung von Bedrohungen, über die noch keine Informationen in den Datenbanken von Kaspersky Lab enthalten sind. Die heuristische Analyse erkennt Objekte, deren Verhalten eine Sicherheitsbedrohung für das Betriebssystem darstellen kann. Objekte, die mithilfe der heuristischen Analyse gefunden werden, werden als möglicherweise infiziert eingestuft. Als möglicherweise infiziert kann beispielsweise ein Objekt gelten, das eine Befehlsfolge enthält, die für schädliche Objekte als charakteristisch gilt (Datei öffnen, in Datei schreiben).

I

Infizierbare Datei

Datei, die aufgrund ihrer Struktur bzw. ihres Formates von Betrügern als "Behälter" für die Aufbewahrung und Verteilung von schädlichem Code verwendet werden kann. In der Regel handelt es sich dabei um ausführbare Dateien mit den Erweiterungen com, exe und dll. Das Risiko für das Einschleusen von bösartigem Code in solche Dateien ist recht hoch.

infiziertes Objekt

Objekt mit einem Abschnitt im Code, der vollständig mit dem Abschnitt im Code einer bekannten Schadsoftware übereinstimmt. Kaspersky Lab empfiehlt nicht, auf solche Objekte zuzugreifen.

K

Kaspersky Security Network (KSN)

Infrastruktur aus Cloud-Diensten, die Zugriff auf die Kaspersky Lab-Datenbank bietet. Diese Datenbank enthält laufend aktualisierte Informationen über die Reputation von Dateien, Webressourcen und Software. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Programme von Kaspersky Lab auf neue Bedrohungen, erhöht die Effektivität der Arbeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

L

Laufzeit der Lizenz

Der Zeitraum, in dem Sie Zugriff auf die Programmfunktionen sowie das Recht zur Verwendung zusätzlicher Dienste haben. Die Dienste, die Sie verwenden können, sind vom Lizenztyp abhängig.

Lokale Aufgabe

Eine Aufgabe, die auf einem einzelnen Client-Computer festgelegt wurde und ausgeführt wird.

O

OLE-Objekt

Objekt, das mithilfe der Technologie "Object Linking and Embedding (OLE)" an eine andere Datei angehängt oder in dieser eingebettet ist. Beispiel für ein OLE-Objekt ist eine Tabelle von Microsoft Office Excel®, die in einem Microsoft Office Word-Dokument eingebettet ist.

Q

Quarantäne

Ordner, in den die Programme von Kaspersky Lab erkannte möglicherweise infizierte Objekte verschieben. Objekte werden in der Quarantäne in verschlüsselter Form gespeichert, um eine Einwirkung auf den Computer zu vermeiden.

R

Richtlinie

Eine Richtlinie bestimmt die Einstellungen eines Programms und verwaltet die Möglichkeiten zum Konfigurieren dieses Programms auf Computern innerhalb einer Administrationsgruppe. Für jedes Programm muss eine separate Richtlinie erstellt werden. Sie können für Programme, die auf Computern in jeder Administrationsgruppe installiert sind, eine unbegrenzte Anzahl an unterschiedlichen Richtlinien erstellen; allerdings kann jeweils nur eine Richtlinie gleichzeitig für ein Programm innerhalb einer Administrationsgruppe übernommen werden.

S

Schutzstatus

Aktueller Schutzstatus, der die Stufe der Computersicherheit anzeigt.

Schwachstelle

Unzulänglichkeit im Betriebssystem oder Programm, die von den Herstellern von Schadsoftware zum Eindringen in das Betriebssystem oder Programm und zur Beschädigung dessen Integrität verwendet werden kann. Eine große Anzahl von Schwachstellen in einem System macht dieses unzuverlässig, da Viren, die in das System eingedrungen sind, zu Ausführungsfehlern im System selbst sowie in den installierten Programmen führen können.

Sicherheitsstufe

Die Sicherheitsstufe ist ein vorkonfiguriertes Set an Einstellungen der Programmkomponenten.

SIEM

Eine Technologie, die Sicherheitsereignisse analysiert, die auf verschiedenen Geräten und Programmen im Netzwerk eintreten.

U

Update

Vorgang zum Ersetzen bestehender bzw. Hinzufügen neuer Dateien (Datenbanken oder Programm-Module), die von den Kaspersky-Lab-Update-Servern heruntergeladen wurden.

AO Kaspersky Lab

Kaspersky Lab ist ein weltweit anerkannter Hersteller von Systemen zum Schutz von Computern vor digitalen Bedrohungen, einschließlich Viren und anderer Schadsoftware, unerwünschten E-Mails (Spam) sowie Netzwerk- und Hacking-Angriffen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach Angaben der IDC ist Kaspersky Lab in Russland der beliebteste Hersteller von Computerschutzsystemen für Heimanwender (IDC Endpoint Tracker 2014).

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern, der in 33 verschiedenen Ländern über insgesamt 38 Niederlassungen verfügt. Das Unternehmen beschäftigt über 3.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die persönliche Produktpalette umfasst Sicherheitsanwendungen für Desktop-, Laptop- und Tablet-Computer, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Schutz- und Steuerungslösungen und -technologien für Workstations und mobile Geräte, virtuelle Maschinen, File- und Webserver, Mail-Gateways und Firewalls. Zum Portfolio des Unternehmens gehören auch spezialisierte Produkte zum Schutz vor DDoS-Angriffen, zum Schutz von industriellen Steuerungssystemen und zur Verhinderung von Finanzbetrug. In Verbindung mit zentralisierten Management-Tools gewährleisten diese Lösungen einen effektiven, automatisierten Schutz für Unternehmen und Organisationen jeder Größe vor Computerbedrohungen. Die Produkte von Kaspersky Lab sind von großen Testlabors zertifiziert, mit Software verschiedener Hersteller kompatibel und für den Einsatz auf vielen Hardware-Plattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Jeden Tag decken sie Hunderttausende neuer Computerbedrohungen auf, erstellen Werkzeuge zur Erkennung und Desinfektion und fügen ihre Signaturen in Datenbanken ein, die von Kaspersky Lab-Anwendungen verwendet werden.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Software-Hersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu und ZyXEL. Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So erhielt Kaspersky Lab 2014 bei Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives neben einem anderen Hersteller die meisten "Advanced+"-Zertifikate und wurde schließlich mit dem "Top Rated"-Zertifikat ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 400 Millionen Anwender und über 270.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	https://www.kaspersky.de	
Viren-Enzyklopädie:	https://de.securelist.com/	
Kaspersky VirusDesk:	https://virusdesk.kaspersky.com/de verdächtiger Dateien und Webseiten)	(zur Untersuchung
Webcommunity von Kaspersky Lab:	https://community.kaspersky.com	

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in der Datei legal_notices.txt, die sich im Installationsverzeichnis des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Marken und Dienstleistungszeichen sind Eigentum der jeweiligen Rechteinhaber.

Intel und Pentium sind Markenzeichen der Intel Corporation in den USA und/oder anderen Ländern.

Linux ist ein registriertes Warenzeichen von Linus Torvalds in den USA und anderen Ländern.

Microsoft, Active Directory, Excel, Internet Explorer und Windows sind Handelsmarken von Microsoft Corporation, die in den USA und anderen Ländern eingetragen sind.

UNIX ist ein registriertes Warenzeichen in den Vereinigten Staaten und anderen Ländern, das ausschließlich über X/Open Company Limited lizenziert ist.

Sachregister

A

B

D

E

F

H

I

K

M

O

P

Q

R

S

U

V

W