KASPERSKY lab

Kaspersky Embedded Systems Security

Administratorhandbuch

Produktversion: 2.2.0.605

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: 16.10.2018

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

Inhalt

Über dieses Handbuch

Kaspersky Embedded Systems Security 2.2.0.605 Das Administratorhandbuch (im Weiteren "Kaspersky Embedded Systems Security 2.2", "das Programm") richtet sich an die Experten, die für die Installation und die Verwaltung von Kaspersky Embedded Systems Security 2.2 auf allen geschützten Geräten zuständig sind, sowie an die Experten für den technischen Support der Unternehmen, die Kaspersky Embedded Systems Security 2.2 verwenden.

Dieses Handbuch enthält Informationen über die Konfiguration und Verwendung von Kaspersky Embedded Systems Security 2.2.

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 2.2 enthält folgende Abschnitte.

Informationsquellen über Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt beschreibt Funktionen, Komponenten und Lieferumfang von Kaspersky Embedded Systems Security 2.2 sowie die Hard- und Software-Voraussetzungen für Kaspersky Embedded Systems Security 2.2.

Programm installieren und deinstallieren

Dieser Abschnitt enthält schrittweise Anleitungen zur Installation und Deinstallation von Kaspersky Embedded Systems Security 2.2.

Programmoberfläche

Dieser Abschnitt enthält Informationen zu den Elementen der Programmoberfläche von Kaspersky Embedded Systems Security 2.2.

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 2.2

Dieser Abschnitt enthält Informationen zum Start und Stoppen des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security 2.2 (im Weiteren "Verwaltungs-Plug-in") sowie von Kaspersky Security Service.

Über Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt enthält Informationen über die Rechte zur Verwaltung von Kaspersky Embedded Systems Security 2.2 und der Windows®-Dienste, die das Programm registriert, sowie eine Anleitung zur Konfiguration dieser Rechte.

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt enthält Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Embedded Systems Security 2.2 auf mehreren Computern.

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Embedded Systems Security 2.2, 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 2.2 in Kaspersky Security Center.

Echtzeitschutz des Computers

Dieser Abschnitt informiert über die Aufgaben zum Echtzeitschutz des Computers: Echtzeitschutz für Dateien und Verwendung von KSN, sowie Exploit-Prävention. Darüber hinaus enthält er Anweisungen zum Anpassen der Einstellungen für Aufgaben zum Echtzeitschutz sowie zum Anpassen der Sicherheitseinstellungen des geschützten Computers.

Überwachung der Server-Aktivitäten

Dieser Abschnitt enthält Informationen über die Funktionen von Kaspersky Embedded Systems Security 2.2 zur Kontrolle der Starts und Verbindungen von Apps durch externe Geräte über USB.

Netzwerküberwachung

Dieser Abschnitt enthält Informationen über die Aufgaben zur Firewall-Verwaltung.

System-Diagnose

Dieser Abschnitt enthält Informationen über die Aufgabe zur Überwachung der Datei-Integrität und die Möglichkeiten der Analyse des Systemprotokolls des Betriebssystems.

Integration mit Drittanbietersystemen

Dieser Abschnitt beschreibt die Integration von Kaspersky Embedded Systems Security 2.2 mit Drittanbieterfunktionen und -technologien.

Arbeiten mit Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Embedded Systems Security 2.2 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.
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 einen Pfeil 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. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

Informationsquellen über Kaspersky Embedded Systems Security 2.2

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 2.2 stehen Ihnen folgende Informationsquellen zur Verfügung:

- Seite von Kaspersky Embedded Systems Security 2.2 auf der Website von Kaspersky Lab
- Seite von Kaspersky Embedded Systems Security 2.2 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 2.2 auf der Website von Kaspersky Lab

Auf der Seite von Kaspersky Embedded Systems Security 2.2 https://www.kaspersky.com/small-to-medium-business-security/windows-server-security stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

Auf der Seite für Kaspersky Embedded Systems Security 2.2 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 2.2 in der Wissensdatenbank

Die Wissensdatenbank ist ein spezieller Bereich auf der Website des Technischen Supports.

Auf der Seite von Kaspersky Embedded Systems Security 2.2 in der Wissensdatenbank http://support.kaspersky.com/de/ksws10 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 2.2, 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 2.2

Das Administratorhandbuch von Kaspersky Embedded Systems Security 2.2 enthält Informationen über die Installation, Deinstallation, Konfiguration und Nutzung des Programms.

Diskussion über die Programme von Kaspersky Lab im Forum

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum http://forum.kaspersky.com/ diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen zur Diskussion stellen.

Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt beschreibt Funktionen, Komponenten und Lieferumfang von Kaspersky Embedded Systems Security 2.2 sowie die Hard- und Software-Voraussetzungen für Kaspersky Embedded Systems Security 2.2.

In diesem Kapitel

Über Kaspersky Embedded Systems Security 2.2

Mit Kaspersky Embedded Systems Security 2.2 werden Computer und andere integrierte Systeme unter Microsoft® Windows vor Viren und anderen Computerbedrohungen geschützt. Als Benutzer von Kaspersky Embedded Systems Security 2.2 gelten Netzwerkadministratoren des Unternehmens und Mitarbeiter, die für den Antiviren-Schutz des Unternehmensnetzwerks zuständig sind.

Sie können Kaspersky Embedded Systems Security 2.2 auf einer Vielzahl von integrierten Systemen unter Windows installieren, u. a. auf den folgenden Typen von Geräten:

- GAA (Geldausgabeautomaten)
- Kassensysteme

Kaspersky Embedded Systems Security 2.2 kann auf folgende Arten verwaltet werden:

- Über die Programmkonsole, die auf einem Computer mit Kaspersky Embedded Systems Security 2.2 oder auf einem anderen Computer installiert ist.
- Mithilfe eines Befehls in der Befehlszeile.
- Mithilfe der 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 ein Exemplar von Kaspersky Embedded Systems Security 2.2 installiert ist.

Sie können die Leistungsindikatoren von Kaspersky Embedded Systems Security 2.2 für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps analysieren.

Komponenten und Funktionen von Kaspersky Embedded Systems Security 2.2

Im Lieferumfang des Programms sind folgende Komponenten enthalten:

- **Echtzeitschutz für Dateien**. Kaspersky Embedded Systems Security 2.2 untersucht Objekte, wenn darauf zugegriffen wird. Kaspersky Embedded Systems Security 2.2 untersucht die folgenden Objekte:

  - Dateien
  - Alternative Datenströme der Dateisysteme (NTFS-Streams)
  - MBR und Bootsektoren von lokalen Festplatten und Wechseldatenträgern.
- **Untersuchung auf Befehl**. Kaspersky Embedded Systems Security 2.2 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 ermöglicht eine Kontrolle der Registrierung und der Verwendung von Massenspeichergeräten und CD-/DVD-Geräten, um den Computer vor Gefahren für die Computersicherheit zu schützen, die während des Dateiaustausches mit angeschlossenen 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 2.2 erkennt Änderungen in Dateien im in den Aufgabeneinstellungen festgelegten Überwachungsbereich. Diese Änderungen können auf eine Sicherheitsverletzung auf dem geschützten Computer 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 2.2 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 2.2 als möglicherweise infiziert eingestuft wurden, werden unter Quarantäne gestellt, d. h. die Objekte werden von ihrem ursprünglichen Speicherort in die *Quarantäne* verschoben. Aus Sicherheitsgründen werden Objekte in der Quarantäne in verschlüsselter Form gespeichert.
- **Backup**. Bevor ein Objekt mit dem Status *Infiziert* oder *Möglicherweise infiziert* desinfiziert oder gelöscht wird, speichert Kaspersky Embedded Systems Security 2.2 eine verschlüsselte Sicherungskopie 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 2.2 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 2.2 in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Embedded Systems Security 2.2 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 2.2 verwenden.
- **Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security**. Sie können die Rechte für die Verwaltung von Kaspersky Embedded Systems Security 2.2 und der Windows-Dienste, die das Programm registriert, für Benutzer und Benutzergruppen konfigurieren.
- **Protokollieren von Ereignissen im Ereignisprotokoll des Programms**. Kaspersky Embedded Systems Security 2.2 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 2.2 sowie Informationen, die für die Fehlerdiagnose in Kaspersky Embedded Systems Security 2.2 erforderlich sind.
- **Vertrauenswürdige Zone**. Sie können eine Liste mit Ausnahmen aus dem Schutzbereich bzw. Untersuchungsbereich anlegen, die Kaspersky Embedded Systems Security 2.2 bei der Ausführung der Aufgaben zur Untersuchung auf Befehl und zum Echtzeitschutz für Dateien 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 2.2 verfügt über die folgenden neuen Funktionen und Verbesserungen:

- Unterstützung für neue Versionen von Microsoft-Windows-Betriebssystemen.

  Auf ELAM- und PPL-Technologien basierende Selbstschutzmechanismen: Beim Installieren des Programms wird nun automatisch ein ELAM-Treiber registriert, mit dem der Kaspersky Security Service (kavfs.exe) mit dem Attribut "Protected Process Light" gestartet werden kann. Somit kann der Selbstschutz des Programms unterstützt und ein breites Spektrum von Angriffen vermieden werden.

  Die Funktionalität ist verfügbar, wenn das Programm auf Computern installiert wurde, auf denen Microsoft Windows Server™ 10 RS2 (build 15063) und höher ausgeführt wird.
- Unterstützung für die Prüfung und Verarbeitung von Cloud-Dateien, die in Microsoft OneDrive gespeichert werden.
- Die Möglichkeiten des Subsystems "Kontrolle für Installationspakete" wurden verbessert.

  Sie können jetzt angeben, welche Installationsdateien das Attribut für ein vertrauenswürdiges Installationspaket übergeben können. Das gilt für die gesamte Menge von Dateien, die aus ihnen extrahiert werden können. Somit besteht jetzt die Möglichkeit, die Stabilität der Softwareinstallationsprozesse auf einem Server mit aktivierter Kontrolle des Programmstarts zu erhöhen. Allerdings erweitert sich hierdurch aber auch die Möglichkeit eines Angriffs, weil die Anzahl der autorisierten Programmstarts erhöht wird. Wir empfehlen, den Parameter bei komplexen Softwarebereitstellungen zu verwenden. Dazu gehören u. a. Situationen, in denen der Server während eines Installationspaketprozesses neu gestartet werden muss.
- Integration mit WMI-Tools.

  Bei der Installation des Programms wird jetzt automatisch ein Kaspersky Security Namespace im WMI Root Namespace auf dem lokalen Computer erstellt. Mit Client-Lösungen, die WMI-Abfragen unterstützen, können Sie Daten zum Programm und seinen Komponenten abrufen.

- Das Format zur Anzeige von Informationen zum Programm und seinen Komponenten wurde durch den Befehl KAVSHELL OMSINFO erweitert: Jetzt können Sie Informationen zum Status der Aufgabe "Kontrolle des Programmstarts" sowie Informationen zu installierten kritischen Updates von Programmmodulen abrufen.
- Verbesserte Möglichkeiten der Verwaltung und Überwachung des Programmzustands mittels der kompakten Server-Übersicht:
  - Jetzt können Sie die Statistikindikatoren für die installierten Komponenten auf der Registerkarte "Statistik" in der kompakten Server-Übersicht ansehen.
  - Beim Zugriff auf die kompakte Server-Übersicht ist keine Kennworteingabe erforderlich, selbst wenn der Kennwortschutz aktiviert ist: Das Programm beschränkt den Zugriff auf die in der kompakten Server-Übersicht verfügbaren Informationen und Steuerelemente nur auf Grundlage der festgelegten Benutzerrechte zur Programmverwaltung.
- Ab Version 2.2 implementiert das Programm die Möglichkeit eines Grundschutzes für den Computer während dem Start des Betriebssystems im "Abgesicherten Modus".

  Standardmäßig funktioniert das Programm auf einem Computer im abgesicherten Modus nicht. Um das Programm auch dann zu starten, wenn das sich das Betriebssystem im abgesicherten Modus befindet, setzen Sie den Parameter "LoadInSafeMode" im folgenden Registry-Schlüssel auf " =1 " .

  `HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters`

  Solange ein Computer im abgesicherten Modus läuft, sind die Funktionen des Programms beschränkt.
- Berichte in Kaspersky Security Center werden unterstützt: Sie können nun Berichte einsehen über den Status der Programmkomponenten und zwei Berichtsarten über verbotene Anwendungen. Die Funktionalität wird nur unterstützt, wenn Sie Kaspersky Security Center 11 verwenden.
- Die Zugriffserlaubnis für Nutzer, um den Installationsordner oder wichtige Registry-Pfade der Programmkomponenten zu verändern, ist nun eingeschränkt.

Lieferumfang

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

- Installationsassistent für Kaspersky Embedded Systems Security 2.2 starten
- Installationsassistent für die Konsole für Kaspersky Embedded Systems Security 2.2 starten.
- Starten Sie den Installationsassistenten für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security 2.2, um das Programm über Kaspersky Security Center zu verwalten.
- Das Administratorhandbuch lesen
- Das Benutzerhandbuch lesen
- Wechseln Sie zur Seite von Kaspersky Embedded Systems Security 2.2 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 2.2 lesen.

Der Ordner \console beinhaltet die Installationsdateien für die Programmkonsole (Komponentenpaket "Administrations-Tools für Kaspersky Embedded Systems Security 2.2").

Der Ordner \product enthält Folgendes:

- Dateien für die Installation der Serverkomponenten von Kaspersky Embedded Systems Security 2.2 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 2.2 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 Komponenten und Plug-ins von Kaspersky Embedded Systems Security 2.2 ohne die 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 2.2

Datei	Ziel
autorun.inf	Autostart-Datei des Installationsassistenten von Kaspersky Embedded Systems Security 2.2 bei der Programminstallation von Wechseldatenträgern
ess_admin_guide_en.pdf	Administratorhandbuch.
ess_user_guide_en.pdf	Benutzerhandbuch
release_notes.txt	Datei enthält Ausgabedaten.
setup.exe	Startdatei des Begrüßungsprogramms (startet setup.hta).
\console\esstools_x86(x64).msi	Installationspaket 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	Startdatei des Assistenten zur Installation von Kaspersky Embedded Systems Security 2.2 auf dem geschützten Computer; startet die Datei des Installationspakets ess.msi mit den im Assistenten gewählten Installationsparametern.
\product\ess_x86(x64).msi	Installationspaket des Dienstes Windows Installer; installiert Kaspersky Embedded Systems Security 2.2 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 2.2 über Kaspersky Security Center.

Datei	Ziel
\product\klcfginst.exe	Installationsprogramm für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security 2.2 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 2.2 mit dieser Konsole verwalten möchten.
\product\license.txt	Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
\product\migration.txt	Die Datei beschreibt die Migration von früheren Programmversionen.
\setup\setup.hta	Datei für den Start des Begrüßungsprogramms.

Sie können die im Lieferumfang enthaltenen Dateien von der Installations-CD starten. Wenn Sie die Dateien zuvor auf einen lokalen Datenträger kopieren, stellen Sie sicher, dass die ursprüngliche Dateistruktur erhalten bleibt.

Hard- und Software-Voraussetzungen

Vor der Installation von Kaspersky Embedded Systems Security 2.2 müssen Sie andere Antiviren-Programme vom Computer deinstallieren.

Hardwarevoraussetzungen für den geschützten Computer

Allgemeine Voraussetzungen:

- X86-kompatible Systeme in Einzel- und Mehrprozessor-Konfigurationen.
- x64-kompatible Systeme in Einzel- und Mehrprozessor-Konfigurationen.

Festplattenplatz:

- Für die Installation der Komponente "Kontrolle des Programmstarts": 50 MB.
- Für die Installation aller Komponenten von Kaspersky Embedded Systems Security 2.2: 500 MB.

Arbeitsspeicher:

- 256 MB, um nur die Komponente "Kontrolle des Programmstarts" auf dem Computer unter einem Microsoft® Windows-Betriebssystem zu installieren.
- 512 MB, um alle Komponenten auf dem Computer unter einem Microsoft Windows-Betriebssystem zu installieren.

Mindestvoraussetzungen für den Prozessor:

- für 32-Bit-Betriebssysteme von Microsoft Windows: Intel® Pentium® III.
- für 64-Bit-Betriebssysteme von Microsoft Windows: Intel Pentium IV.

Softwarevoraussetzungen für den geschützten Computer

Sie können Kaspersky Embedded Systems Security 2.2 auf einem Gerät unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows installieren.

Auf einem Computer unter Microsoft Windows XP ist für eine ordnungsgemäße Installation des Programms Windows Installer 3.1 erforderlich.

Um Kaspersky Embedded Systems Security 2.2 auf Geräten mit eingebetteten Betriebssystemen zu installieren und zu verwenden, sind die Komponenten "Filter Manager" und "Administrations-Tools" erforderlich.

Sie können Kaspersky Embedded Systems Security 2.2 auf einem Computer unter einem der folgenden 32-Bit- oder 64-Bit-Betriebssysteme von Microsoft Windows installieren:

- Windows XP Embedded SP3
- Windows XP Pro SP2 / SP3
- Windows Embedded POSReady 2009
- Windows Embedded Standard 7 SP1
- Windows Embedded Enterprise 7 SP1
- Windows Embedded POSReady 7
- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

Programm installieren und deinstallieren

Dieser Abschnitt enthält schrittweise Anleitungen zur Installation und Deinstallation von Kaspersky Embedded Systems Security 2.2.

In diesem Kapitel

Programmkomponenten von Kaspersky Embedded Systems Security 2.2 und ihre Codes für den Dienst Windows Installer

Standardmäßig werden mithilfe der Dateien \server\ess_x86(x64).msi alle Programmkomponenten von Kaspersky Embedded Systems Security 2.2 installiert. Sie können die Installation dieser Komponente bei einer benutzerdefinierten Installation des Programms aktivieren.

Durch die Dateien \client\esstools_x86(x64).msi werden alle Programmkomponenten des Pakets "Administrations-Tools" installiert.

Die folgenden Abschnitte enthalten die Codes der Programmkomponenten von Kaspersky Embedded Systems Security 2.2 für den Dienst Windows Installer. Sie können diese Codes verwenden, um die Liste der zu installierenden Komponenten festzulegen, wenn Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile installiert wird.

In diesem Abschnitt

Programmkomponenten von Kaspersky Embedded Systems Security 2.2

Die folgende Tabelle enthält die Codes und eine Beschreibung der Programmkomponenten von Kaspersky Embedded Systems Security 2.2.

Tabelle 3. Beschreibung der Programmkomponenten von Kaspersky Embedded Systems Security 2.2

Komponente	Code	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 festgelegten 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 gewährleistet den Antiviren-Schutz und beinhaltet die folgenden Komponenten: • Untersuchung auf Befehl • Echtzeitschutz für Dateien
Untersuchung auf Befehl	Ods	Diese Komponente installiert die Systemdateien von Kaspersky Embedded Systems Security 2.2 und Dateien, die die Aufgaben zur Untersuchung auf Befehl (Untersuchung von Objekten des geschützten Computers) umsetzen. Wenn Sie beim Installieren von Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile andere Komponenten von Kaspersky Embedded Systems Security 2.2 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.

Komponente	Code	Ausgeführte Funktion
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 2.2 zu verwalten. Die Komponente wird in der Aufgabe Firewall-Verwaltung umgesetzt.
Modul für die Integration in den Administrationsagenten von Kaspersky Security Center	AKIntegration	Koordination der Verbindung zwischen dem Server von Kaspersky Embedded Systems Security 2.2 und dem Administrationsagenten von Kaspersky Security Center. 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. Die Leistungsindikatoren messen die Leistungsfähigkeit von Kaspersky Embedded Systems Security 2.2 und finden mögliche Engpässe bei gleichzeitiger Ausführung von Kaspersky Embedded Systems Security 2.2 und anderen Programme.
SNMP-Indikator und Traps	SnmpSupport	Die Komponente veröffentlicht die Indikatoren und Traps für Kaspersky Embedded Systems Security 2.2 über den Dienst Simple Network Management Protocol (SNMP) von Microsoft Windows. Sie können diese Komponente nur auf dem geschützten Computer installieren, wenn der Microsoft SNMP auf demselben Computer installiert ist.

Komponente	Code	Ausgeführte Funktion
Symbol für Kaspersky Embedded Systems Security 2.2 im Infobereich	TrayApp	Die Komponente zeigt das Symbol für Kaspersky Embedded Systems Security 2.2 im Infobereich der Taskleiste des geschützten Computers an. Das Symbol für Kaspersky Embedded Systems Security 2.2 zeigt den Status des Schutzes auf dem Computer an und erlaubt, die Konsole für Kaspersky Embedded Systems Security 2.2 in Microsoft Management Console (falls installiert) und das Fenster **Über das Programm** zu öffnen.
Befehlszeilen-Utility	Shell	Verwaltung von Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile des geschützten Computers.

Programmkomponenten des Pakets "Administrations-Tools"

Die folgende Tabelle enthält die Codes und eine Beschreibung der Programmkomponenten des Satzes "Administrationswerkzeuge".

Tabelle 4. Beschreibung der Programmkomponenten des Satzes Administrationswerkzeuge

Komponente	Code	Funktionen der Komponente
Snap-ins von Kaspersky Embedded Systems Security 2.2	MmcSnapin	Die Komponente installiert das Microsoft Management Console Snap-in für die Verwaltung über die Konsole für Kaspersky Embedded Systems Security 2.2. Wenn Sie beim Installieren eines Satzes der Administrationswerkzeuge aus der Befehlszeile andere Satz-Komponenten angeben, ohne die MmcSnapin-Komponente zu nennen, wird die MmcSnapin-Komponente automatisch installiert.
Help	Help	chm-Hilfedatei; wird im Ordner mit den Dateien der Administrations-Tools für Kaspersky Embedded Systems Security 2.2 gespeichert. 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 2.2 fügt eine Verknüpfung zur Kaspersky Lab-Web-Ressource hinzu, wo das Administratorhandbuch und das Benutzerhandbuch im PDF-Format verfügbar sind. Sie können alle Handbücher aus dem Menü **Start** öffnen.

Systemänderungen nach der Installation von Kaspersky Embedded Systems Security 2.2

Bei der Installation von Kaspersky Embedded Systems Security 2.2 und der Programmkonsole (aus dem Paket "Administrations-Tools") nimmt der Dienst von Windows Installer auf dem 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 2.2 erstellt.
- Die Dienste von Kaspersky Embedded Systems Security 2.2 werden registriert
- Eine Benutzergruppe für Kaspersky Embedded Systems Security 2.2 wird erstellt
- In der Systemregistrierung werden die Schlüssel für Kaspersky Embedded Systems Security 2.2 registriert.

Diese Veränderungen sind in der Tabelle unten beschrieben.

Ordner für Kaspersky Embedded Systems Security 2.2

Tabelle 5. Ordner für Kaspersky Embedded Systems Security 2.2 auf einem geschützten Computer

Ordner	Dateien für Kaspersky Embedded Systems Security 2.2
Standardinstallationsordner für Kaspersky Embedded Systems Security 2.2: In der 32-Bit-Version von Microsoft Windows – %Programme%\Kaspersky Lab\Kaspersky Embedded Systems Security\ In der 64-Bit-Version von Microsoft Windows – %Programme (x86)%\Kaspersky Embedded Systems Security\	Ausführbare Dateien für Kaspersky Embedded Systems Security 2.2 (Zielordner wird während der Installation angegeben).
Ordner %Kaspersky Embedded Systems Security%\mibs	Dateien für die Management Information Base (MIB). Diese Dateien enthalten eine Beschreibung der Indikatoren und Traps, die von Kaspersky Embedded Systems Security 2.2 mit dem SNMP-Protokoll veröffentlicht werden.
Ordner %Kaspersky Embedded Systems Security%\x64	64-Bit-Version der ausführbaren Dateien von Kaspersky Embedded Systems Security 2.2 (der Ordner wird nur erstellt, wenn Kaspersky Embedded Systems Security 2.2 unter einer 64-Bit-Version von Microsoft Windows installiert wird.)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\	Dienstdateien für Kaspersky Embedded Systems Security 2.2
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\	Dateien mit Einstellungen für die Update-Quellen.

Ordner	Dateien für Kaspersky Embedded Systems Security 2.2
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\	Datenbanken-Updates und Updates der Programm-Module, die mithilfe der Aufgabe Update-Verteilung empfangen wurden (Der Ordner wird erstellt, wenn zum ersten Mal Updates mithilfe der Aufgabe Update-Verteilung empfangen werden).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Reports\	Protokolle über Aufgabenausführung und Systemaudit-Protokoll.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\	Satz der Datenbanken, die im Moment verwendet werden.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\	Backup-Kopie der Datenbanken; wird bei jedem Datenbanken-Update überschrieben
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\	Temporäre Dateien, die beim Ausführen der Update-Aufgabe angelegt werden.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\	Objekte in der Quarantäne (standardmäßiger Ordner).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\	Objekte im Backup (standardmäßiger Ordner).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\	Objekte, die aus Backup oder Quarantäne wiederhergestellt wurden (standardmäßiger Ordner für die Wiederherstellung von Objekten).

Tabelle 6. Ordner, die bei der Installation der Programmkonsole erstellt werden

Ordner	Dateien der Konsole für Kaspersky Embedded Systems Security 2.2
Standardinstallationsordner für die Programm-Konsole: • In der 32-Bit-Version von Microsoft Windows – %Programme%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ • In der 64-Bit-Version von Microsoft Windows – %Programme (x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\	Dateien für "Administrations-Tools" (Zielordner, der bei der Installation der Konsole für Kaspersky Embedded Systems Security 2.2 angegeben wird).

Dienste von Kaspersky Embedded Systems Security 2.2

Die Dienste von Kaspersky Embedded Systems Security 2.2 werden unter dem Systemkonto (SYSTEM) gestartet.

Tabelle 7. Dienste von Kaspersky Embedded Systems Security 2.2

Dienst	Ziel
Kaspersky Security Service (KAVFS)	Wichtiger Dienst von Kaspersky Embedded Systems Security 2.2, der Aufgaben und Workflows in Kaspersky Embedded Systems Security 2.2 verwaltet.
Dienst von Kaspersky Security Management Service (KAVFSGT)	Der Dienst ist für die Programmverwaltung von Kaspersky Embedded Systems Security 2.2 mithilfe der Programmkonsole vorgesehen.

Gruppen von Kaspersky Embedded Systems Security 2.2

Tabelle 8. Gruppen von Kaspersky Embedded Systems Security 2.2

Gruppe	Ziel
ESS Administrators	Die Benutzer aus dieser Gruppe besitzen auf dem geschützten Computer Vollzugriff auf Kaspersky Security Management Service sowie Zugriff auf alle Funktionen von Kaspersky Embedded Systems Security 2.2.

Schlüssel der Systemregistrierung

Tabelle 9. Schlüssel der Systemregistrierung

Schlüssel	Ziel
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Eigenschaften des Dienstes für Kaspersky Embedded Systems Security 2.2
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Einstellungen des Ereignisprotokolls für Kaspersky Embedded Systems Security 2.2 (Kaspersky Event Log).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Eigenschaften des Dienstes zur Verwaltung von Kaspersky Embedded Systems Security 2.2
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 Leistungsindikatoren

Schlüssel	Ziel
In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent] In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent]	Parameter für die Komponente Unterstützung des SNMP-Protokolls.
In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump] In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump]	Einstellungen für Einträge in die Dump-Datei.
In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace] In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace]	Einstellungen für Protokolldateien.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment]	Konfiguration der Aufgaben und Funktionen der Anwendung.

Prozesse von Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 startet die in der folgenden Tabelle beschriebenen Prozesse.

Tabelle 10. Prozesse von Kaspersky Embedded Systems Security 2.2

Dateiname	Ziel
kavfswp.exe	Workflow von Kaspersky Embedded Systems Security 2.2
kavtray.exe	Prozess für das Taskleistensymbol
kavshell.exe	Prozess der Befehlszeilen-Utility
kavfsrcn.exe	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security 2.2
kavfs.exe	Dienstprozess von Kaspersky Security Service
kavfsgt.exe	Prozess des Verwaltungsdienstes Kaspersky Security Management Service
kavfswh.exe	Prozess des Verwaltungsdienstes Kaspersky Security-Exploit-Prävention

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

In den folgenden Tabellen werden die Einstellungen für die Installation und Deinstallation von Kaspersky Embedded Systems Security 2.2 und deren Standardwerte beschrieben. Außerdem werden die Schlüssel für die Änderung der Einstellungswerte und mögliche Werte dieser Schlüssel erläutert. Sie können diese Schlüssel gemeinsam mit den Standardschlüsseln des Befehls msiexec des Dienstes Windows Installer verwenden, wenn Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile installiert wird.

Tabelle 11. Installationseinstellungen und deren Schlüssel in Windows Installer

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert	Beschreibung
Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren	EULA=<Wert> 0 – Sie lehnen die Bedingungen des Endbenutzer-Lizenzvertrags ab. 1 – Sie akzeptieren die Bedingungen des Endbenutzer-Lizenzvertrags.	0	Um Kaspersky Embedded Systems Security 2.2 installieren zu installieren, müssen Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren.
Bedingungen der Datenschutzrichtlinie akzeptieren	PRIVACYPOLICY=<Wert> 0 – Sie lehnen die Bedingungen der Datenschutzrichtlinie ab. 1 – Sie akzeptieren die Bedingungen der Datenschutzrichtlinie.	0	Um Kaspersky Embedded Systems Security 2.2 zu installieren, müssen Sie die Bedingungen der Datenschutzrichtlinie akzeptieren.
Zielordner	INSTALLDIR=<Vollständiger Pfad zum Ordner>	Kaspersky Embedded Systems Security 2.2: %Programme%\Kaspersky Lab\Kaspersky Embedded Systems Security Administrations-Tools: %Programme%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools In der 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%	Ordner, in dem die Dateien für Kaspersky Embedded Systems Security 2.2 bei der Installation gespeichert werden. Sie können einen anderen Ordner angeben.

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert	Beschreibung
Echtzeitschutz für Dateien beim Start von Kaspersky Embedded Systems Security 2.2 starten (**Echtzeitschutz nach der Installation des Programms aktivieren**)	RUNRTP=<Wert> 1 – starten 0 – nicht starten	1	Aktivieren Sie diese Einstellung, damit der Echtzeitschutz für Dateien beim Start von Kaspersky Embedded Systems Security 2.2 gestartet wird (empfohlen).
Untersuchungsausnahmen, die von der Firma Microsoft empfohlen werden (**Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**)	ADDMSEXCLUSION=<Wert> 1 – ausschließen 0 – nicht ausschließen	1	In der Aufgabe Echtzeitschutz für Dateien werden jene Objekte auf dem Computer vom Schutzbereich ausgenommen, deren Ausnahme die Firma Microsoft empfiehlt. Einige Anwendungen auf dem Computer laufen möglicherweise nicht stabil, wenn Antiviren-Anwendungen Dateien abfangen oder ändern, auf die diese Programme zugreifen. Zu solchen Programmen zählt Microsoft beispielsweise einige Anwendungen wie Domain-Controller.
Untersuchungsausnahmen, die von Kaspersky Lab empfohlen werden (**Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen**)	ADDKLEXCLUSION=<Wert> 1 – ausschließen 0 – nicht ausschließen	1	In der Aufgabe zum Echtzeitschutz für Dateien werden Objekte auf dem Computer in Übereinstimmung mit der Empfehlung von Kaspersky Lab aus dem Schutzbereich ausgeschlossen.

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert	Beschreibung
Remote-Verbindung zur Programmkonsole erlauben.	ALLOWREMOTECON=<Wert> 1 – erlauben 0 – verbieten	0	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 2.2 erstellt Erlaubnisregeln für den Prozess kavfsgt.exe gemäß TCP-Protokoll für alle Ports.
Pfad der Schlüsseldatei (**Schlüssel**)	LICENSEKEYPATH=<Pfad der Schlüsseldatei>	Ordner im Lieferumfang \product	Das Installationsprogramm sucht standardmäßig in dem im Lieferumfang enthaltenen Ordner \product nach einer Datei mit der Erweiterung .key Wenn der Ordner \product mehrere Schlüsseldateien enthält, wählt das Installationsprogramm 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.

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert	Beschreibung
			Sie können den Schlüssel während der Installation von Kaspersky Embedded Systems Security 2.2 hinzufügen, mithilfe der von Ihnen gewählten Administrationswerkzeuge, zum Beispiel mit der Programmkonsole. Wenn Sie während der Programminstallation keinen Programmschlüssel hinzufügen, funktioniert Kaspersky Embedded Systems Security 2.2 nach Abschluss der Installation nicht.
Pfad der Konfigurations datei	CONFIGPATH=<Pfad der Schlüsseldatei>	Nicht festgelegt	Kaspersky Embedded Systems Security 2.2 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 2.2 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.

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert	Beschreibung
Netzwerkverbindungen für die Konsole erlauben	ADDWFEXCLUSION=<Wert> **1** – erlauben **0** – verbieten	0	Verwenden Sie diese Option, um Kaspersky Embedded Systems Security 2.2 installieren auf einem anderen Computer zu installieren. Mit der Konsole für Kaspersky Embedded Systems Security 2.2 können Sie den Computerschutz über ein anderes Gerät ferngesteuert verwalten. Auf dem Computer wird in der Firewall von Microsoft Windows der TCP-Port 135 geöffnet, Netzwerkverbindungen für die ausführbare Datei kavfsrcn.exe werden erlaubt (Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security 2.2) und der Zugriff auf DCOM-Programme wird zugelassen.
			Fügen Sie nach Abschluss der Installation die Benutzer, die das Programm ferngesteuert verwalten werden, zur Gruppe ESS Administrators auf dem Computer hinzu und erlauben Sie darauf Netzwerkverbindungen für den Dienst Kaspersky Security Management Service (Datei kavfsgt.exe). Mehr zur weiteren Konfiguration bei Installation der Konsole für Kaspersky Embedded Systems Security 2.2 auf einem anderen Computer finden Sie im Abschnitt "Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Computer" auf Seite 44.

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert	Beschreibung
Untersuchung auf nicht kompatible Software deaktivieren	SKIPINCOMPATIBLESW = <Wert> 0 – Untersuchung auf nicht kompatible Software wird ausgeführt 1 – Untersuchung auf nicht kompatible Software wird nicht ausgeführt	0	Verwenden Sie diese Einstellung, um die Untersuchung auf nicht kompatible Software bei der Installation des Programms auf dem Gerät im Hintergrundmodus zu aktivieren bzw. deaktivieren. Unabhängig vom Wert dieser Einstellung warnt das Programm bei der Installation von Kaspersky Embedded Systems Security 2.2 immer vor anderen auf diesem Gerät installierten Programmversionen.

Tabelle 12. Deinstallationsparameter und Optionen für die Befehlszeile für den Dienst Windows Installer

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert
Wiederherstellung von Objekten aus der Quarantäne	RESTOREQTN =<Wert> **0** – Quarantäne-Inhalt entfernen; **1** – Inhalt der Quarantäne in dem Unterordner \Quarantine im Ordner wiederherstellen, der mit der Einstellung RESTOREPATH vorgegeben ist.	0 – Löschen
Wiederherstellen des Backup-Inhalt	RESTOREBCK =<Wert> **0** – Backup-Inhalt entfernen; **1** – Inhalt des Backups in dem Unterordner \Backup im Ordner wiederherstellen, der mit der Einstellung RESTOREPATH vorgegeben ist.	0 – Löschen

Einstellung	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Standardwert
Eingabe des aktuellen Kennworts für die Bestätigung des Löschvorgangs (wenn die Verwendung eines Kennworts aktiv ist)	UNLOCK_PASSWORD=<festgelegtes Kennwort>	Nicht festgelegt
Ordner für wiederhergestellte Objekte	RESTOREPATH=<vollständiger Pfad des Ordners> Wiederhergestellte Objekte werden im angegebenen Ordner gespeichert.	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored

Installations- und Deinstallationsprotokoll für Kaspersky Embedded Systems Security 2.2

Wenn Sie die Installation oder Deinstallation von Kaspersky Embedded Systems Security 2.2 mit Hilfe des Assistenten zur Installation (Deinstallation) starten, erstellt der Dienst Windows Installer ein Protokoll über die Installation (Deinstallation). Die Log-Datei mit dem Namen ess_install_<uid>.log (wobei <uid> für die individuelle achtstellige ID des Protokolls steht) wird im Ordner %temp% des Benutzers gespeichert, mit dessen Rechten der Installationsassistent gestartet wurde.

Wenn Sie für die Programmkonsole oder für Kaspersky Embedded Systems Security 2.2 über **Start** die Option **Ändern oder Löschen** ausführen, wird die Datei ess_2.2_maintenance.log automatisch im Ordner %temp% erstellt.

Wenn Sie die Installation oder Deinstallation von Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile ausführen, wird in der Grundeinstellung kein Installationsprotokoll erstellt.

► *Geben Sie einen der folgenden Befehle ein, damit bei der Installation von Kaspersky Embedded Systems Security 2.2 die Log-Datei auf dem Laufwerk C:\ angelegt wird:*

- `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 enthält eine Beschreibung der Administrations-Tools für Kaspersky Embedded Systems Security 2.2 und der besonderen Aspekte bei der Installation und Deinstallation von Kaspersky Embedded Systems Security 2.2 mithilfe eines Assistenten (siehe Abschnitt "Installation und Deinstallation des Programms mit dem Assistenten" auf Seite 40), der Befehlszeile (siehe Abschnitt "Installation und Deinstallation des Programms aus der Befehlszeile" auf Seite 53), über Kaspersky Security Center (siehe Abschnitt "Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center" auf Seite 59) und mittels Active Directory®-Gruppenrichtlinie (siehe Abschnitt "Installation und Deinstallation mittels Active Directory-Gruppenrichtlinien" auf Seite 64).

Bevor Sie mit der Installation von Kaspersky Embedded Systems Security 2.2 installieren beginnen, sollten Sie die wichtigsten Installationsetappen planen.

1. Wählen Sie die Administrations-Tools aus, die Sie zur Verwaltung und Konfiguration von Kaspersky Embedded Systems Security 2.2 einsetzen möchten.
2. Legen Sie fest, welche Programmkomponenten für die Installation erforderlich sind (siehe Abschnitt "Programmkomponenten von Kaspersky Embedded Systems Security 2.2 und ihre Codes für den Dienst Windows Installer" auf S. 22).
3. Wählen Sie eine Installationsmethode aus.

In diesem Abschnitt

Administrations-Tools auswählen

Entscheiden Sie, welche Administrations-Tools Sie für die Konfiguration der Einstellungen von Kaspersky Embedded Systems Security 2.2 und dessen Verwaltung einsetzen möchten. Als Administrations-Tools für Kaspersky Embedded Systems Security 2.2 können die Programmkonsole, das Befehlszeilen-Tool sowie die Verwaltungskonsole von Kaspersky Security Center dienen.

Konsole für Kaspersky Embedded Systems Security 2.2

Die Konsole für Kaspersky Embedded Systems Security 2.2 ist ein isoliertes Snap-in, das in die Microsoft Management Console eingefügt wird. Sie können Kaspersky Embedded Systems Security 2.2 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 2.2 hinzufügen, um mit ihr den Schutz mehrerer Computer zu verwalten, auf denen Kaspersky Embedded Systems Security 2.2 installiert ist.

Die Programmkonsole gehört zu den Programmkomponenten "Administrations-Tools".

Befehlszeilen-Utility

Sie können Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile eines geschützten Computers verwalten.

Das Befehlszeilen-Tool gehört zum Paket der Programmkomponenten von Kaspersky Embedded Systems Security 2.2.

Kaspersky Security Center

Wenn Sie zur zentralisierten Verwaltung des Antiviren-Schutzes für die Computer in Ihrem Unternehmen das Programm Kaspersky Security Center verwenden, können Sie Kaspersky Embedded Systems Security 2.2 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 2.2. Sie gewährleistet die Kommunikation zwischen Kaspersky Embedded Systems Security 2.2 und dem Administrationsagenten. 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 2.2 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 2.2**. Installieren Sie auf den Computer, auf dem die Verwaltungskonsole für Kaspersky Embedded Systems Security 2.2 installiert ist, zusätzlich das Verwaltungs-Plug-in für den Kaspersky Security Center-Administrationsserver. Das Plug-In bietet die Oberfläche zur Verwaltung des Programms über Kaspersky Security Center. Die Installationsdatei für das Plug-In \product\klcfginst.exe gehört zum Lieferumfang von Kaspersky Embedded Systems Security 2.2.

Installationstyp auswählen

Nachdem Sie die Softwarekomponenten für die Installation von Kaspersky Embedded Systems Security 2.2 (siehe Abschnitt "Programmkomponenten von Kaspersky Embedded Systems Security 2.2 und ihre Codes für den Dienst Windows Installer" auf S. 22) angegeben haben, müssen Sie die Installationsmethode des Programms auswählen.

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

- Ob spezielle Installationseinstellungen für Kaspersky Embedded Systems Security 2.2 festgelegt werden sollen oder ob die empfohlenen Installationseinstellungen verwendet werden (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 30).
- Ob die Installationseinstellungen für alle Computer einheitlich oder für jeden Computer individuell sind

Sie können Kaspersky Embedded Systems Security 2.2 mit dem Installationsassistenten sowie ohne Benutzereingriff installieren, indem Sie die Installationseinstellungen in die Befehlszeile eingeben. Sie können Kaspersky Embedded Systems Security 2.2 zentral als Remote-Installation installieren: über Gruppenrichtlinien von Active Directory oder mithilfe der Aufgabe zur Remote-Installation von Kaspersky Security Center.

Sie können Kaspersky Embedded Systems Security 2.2 auf einem Computer installieren, ihn konfigurieren und die Einstellungen in einer Konfigurationsdatei speichern, um später die angelegte Datei für die Installation von Kaspersky Embedded Systems Security 2.2 auf anderen Computern zu benutzen (Option gilt nicht bei der Installation über Gruppenrichtlinien des Active Directory).

Installationsassistent starten

Mit dem Installationsassistenten können Sie installieren:

- Die Komponenten von Kaspersky Embedded Systems Security 2.2 (siehe Abschnitt "Programmkomponenten von Kaspersky Embedded Systems Security 2.2" auf Seite 23) auf einem geschützten Computer aus der Datei \product\setup.exe, die im Lieferumfang enthalten ist.
- Konsole für Kaspersky Embedded Systems Security 2.2 (siehe Abschnitt "Konsole für Kaspersky Embedded Systems Security 2.2 installieren" auf Seite 43) aus der Datei \client\setup.exe aus dem Lieferumfang auf dem geschützten Computer oder einem anderen LAN-Computer.

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 2.2 mit den Standardinstallationseinstellungen. Mit den Optionen von Kaspersky Embedded Systems Security 2.2 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 2.2 und der Programm-Konsole auch Beispiele für Befehle verwenden (siehe Abschnitt "Installation und Deinstallation des Programms aus der Befehlszeile" auf Seite 53).

Zentrale Installation über Kaspersky Security Center

Wenn Sie Kaspersky Security Center zur Verwaltung des Antiviren-Schutzes der Netzwerk-Computer einsetzen, können Sie Kaspersky Embedded Systems Security 2.2 mit der Aufgabe zur Remote-Installation von Kaspersky Security Center auf mehreren Computern installieren.

Die Computer, auf denen Sie Kaspersky Embedded Systems Security 2.2 installieren mittels Kaspersky Security Center installieren möchten (siehe Abschnitt "Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center" auf Seite 59), können sich entweder in derselben Domäne wie das Kaspersky Security Center oder in einer anderen Domäne befinden oder überhaupt zu keiner Domäne gehören.

Zentrale Installation über Gruppenrichtlinien des Active Directory

Mit den Gruppenrichtlinien von Active Directory können Sie Kaspersky Embedded Systems Security 2.2 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 2.2 nur mit den empfohlenen Installationseinstellungen zu installieren.

Die Computer, auf denen Kaspersky Embedded Systems Security 2.2 mithilfe von Active Directory-Gruppenrichtlinien installiert wird (siehe Abschnitt "Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory" auf Seite 64) muss 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 enthält eine Beschreibung des Installations- bzw. Deinstallationsprozesses für Kaspersky Embedded Systems Security 2.2 und die Programmkonsole mithilfe eines Installationsassistenten, sowie Informationen über die erweiterten Einstellungen von Kaspersky Embedded Systems Security 2.2 und die Aktionen nach der Installation des Programms.

In diesem Abschnitt

Installation mit dem Installationsassistenten

Die folgenden Abschnitte enthalten Informationen über die Installation von Kaspersky Embedded Systems Security 2.2 und der Programmkonsole.

► *Gehen Sie folgendermaßen vor, um Kaspersky Embedded Systems Security 2.2 zu installieren und das Programm zu verwenden:*

1. Installieren Sie Kaspersky Embedded Systems Security 2.2 auf einem geschützten Computer
2. Installieren Sie die Programmkonsole auf den Computern, von denen Sie Kaspersky Embedded Systems Security 2.2 verwalten möchten.
3. Wenn Sie die Programmkonsole im Netzwerk auf keinem anderen Computer als dem geschützten Computer installiert haben, sind zusätzliche Einstellungen erforderlich, damit Kaspersky Embedded Systems Security 2.2 von den Programmkonsolenbenutzern ferngesteuert verwaltet werden kann.
4. Führen Sie nach der Installation von Kaspersky Embedded Systems Security 2.2 Aktionen durch

In diesem Abschnitt

Installation von Kaspersky Embedded Systems Security 2.2

Bevor Sie Kaspersky Embedded Systems Security 2.2 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, in der Administratorengruppe auf dem geschützten Computer angemeldet ist.

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 2.2 an. Sie können die Installation von Kaspersky Embedded Systems Security 2.2 bei 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 30.

► *So installieren Sie Kaspersky Embedded Systems Security 2.2 mithilfe eines Installationsassistenten:*

1. Starten Sie auf dem Computer die Datei des Begrüßungsprogramms setup.exe.
2. Klicken Sie im folgenden Fenster im Block **Installation** auf den Link **Kaspersky Embedded Systems Security 2.2 installieren**.
3. Klicken Sie im folgenden Begrüßungsfenster des Installationsassistenten von Kaspersky Embedded Systems Security 2.2 auf die Schaltfläche **Weiter**.

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

   Wenn Sie die EULA und/oder die Datenschutzrichtlinie nicht akzeptieren, wird die Installation abgebrochen.
6. Klicken Sie auf **Weiter**.

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

   Standardmäßig umfasst die empfohlene Installation alle Komponenten von Kaspersky Embedded Systems Security 2.2, mit Ausnahme der Komponente "Firewall-Verwaltung".

   Die Komponente Unterstützung des SNMP-Protokolls von Kaspersky Embedded Systems Security 2.2 wird nur auf dem geschützten Computer installiert, wenn auf dem Computer der Dienst SNMP Microsoft Windows installiert ist.
8. Um alle Änderungen im Fenster **Benutzerdefinierte Installation** zu verwerfen, klicken Sie auf die Schaltfläche **Zurücksetzen**. Klicken Sie auf **Weiter**.

9. Gehen Sie im folgenden Fenster **Zielordner auswählen** wie folgt vor:
   - Geben Sie bei Bedarf einen Ordner an, in dem die Dateien von Kaspersky Embedded Systems Security 2.2 gespeichert werden sollen.
   - Sehen Sie sich erforderlichenfalls die Informationen über den verfügbaren Speicherplatz auf den lokalen Festplatten an, indem Sie auf die Schaltfläche **Laufwerk** klicken.

   Klicken Sie auf **Weiter**.
10. Passen Sie im folgenden 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**.
11. Gehen Sie im folgenden Fenster **Einstellungen aus einer Konfigurationsdatei importieren** wie folgt vor:
    a. Um die Einstellungen für Kaspersky Embedded Systems Security 2.2 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**.
12. Führen Sie im folgenden Fenster **Programm aktivieren** eine der folgenden Aktionen aus:
    - Wenn Sie das Programm aktivieren möchten, geben Sie die Schlüsseldatei für Kaspersky Embedded Systems Security 2.2 zur Aktivierung des Programms an.
    - Wenn Sie das Programm später aktivieren möchten, klicken Sie auf die Schaltfläche **Weiter**.
    - Wenn Sie zuvor eine Schlüsseldatei im Ordner \server (der zum Lieferumfang gehört) gespeichert haben, wird der Name dieser Datei im Feld **Schlüssel** angezeigt.

      Wenn Sie einen Schlüssel aus der Datei, die in einem anderen Ordner gespeichert ist, hinzufügen möchten, geben Sie die Schlüsseldatei an.

      Nach dem Hinzufügen der Schlüsseldatei werden im Fenster die Lizenzinformationen angezeigt. Kaspersky Embedded Systems Security 2.2 zeigt das berechnete Datum an, an dem die Lizenz abläuft. Die Gültigkeitsdauer der Lizenz wird ab dem Hinzufügen des Schlüssels gezählt, läuft jedoch spätestens nach dem Ablauf der Gültigkeitsfrist der Schlüsseldatei ab.

      Klicken Sie auf die Schaltfläche **Weiter**, um den Schlüssel im Programm anzuwenden.
13. Klicken Sie im Fenster **Bereit zur Installation** auf die Schaltfläche **Installieren**. Der Assistent installiert nun die Komponenten von Kaspersky Embedded Systems Security 2.2.
14. Sobald die Installation abgeschlossen wurde, öffnet sich das Fenster **Die Installation wurde erfolgreich abgeschlossen.**
15. Aktivieren Sie das Kontrollkästchen **Versionshinweise lesen**, um die Ausgabedaten nach Fertigstellung des Installationsassistenten anzusehen.
16. Klicken Sie auf **OK**.

Das Fenster des Installationsassistenten wird geschlossen. Sobald die Installation abgeschlossen wurde, ist Kaspersky Embedded Systems Security 2.2 einsatzbereit, vorausgesetzt, dass Sie einen Schlüssel für die Aktivierung des Programms hinzugefügt haben.

Installation der Konsole für Kaspersky Embedded Systems Security 2.2

Folgen Sie den Anweisungen des Installationsassistenten und geben 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, mit dessen Berechtigungen Sie den Installationsassistenten starten, zur Administratorengruppe auf dem Computer gehört.
2. Starten Sie auf dem Computer die Begrüßungsdatei setup.exe.

   Das Fenster des Willkommen-Programms wird geöffnet.
3. Klicken Sie auf den Link **Konsole für Kaspersky Embedded Systems Security 2.2 installieren**.

   Es öffnet sich das Begrüßungsfenster des Installationsassistenten. Klicken Sie auf **Weiter**.
4. Überprüfen Sie die Bedingungen der EULA und der Datenschutzrichtlinie im geöffneten Fenster, und wählen Sie die **Bedingungen dieser EULA** und die **Datenschutzrichtlinie, die den Umgang mit Daten beschreibt** aus, um mit der Installation fortzufahren. Klicken Sie auf **Weiter**.

   Das Fenster **Erweiterte Einstellungen für die Installation** wird geöffnet.
5. Gehen Sie im folgenden Fenster **Erweiterte Einstellungen für die Installation** wie folgt vor:
   - Wenn Sie planen, Kaspersky Embedded Systems Security 2.2 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 Komponenten der 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 2.2 finden Sie im Abschnitt "Programmkomponenten von Kaspersky Embedded Systems Security 2.2 und ihre Codes für den Dienst Windows Installer" auf Seite 22.
6. Gehen Sie im folgenden Fenster **Zielordner auswählen** wie folgt vor:
   a. Geben Sie bei Bedarf einen anderen Ordner an, in dem die Dateien des Anti-Virus gespeichert werden sollen.
   b. Klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster **Bereit zur Installation** auf die Schaltfläche **Installieren**.

   Der Assistent installiert nun die ausgewählten Komponenten.
8. Klicken Sie auf **OK**.

Das Fenster des Installationsassistenten wird geschlossen. Die Programmkonsole wird auf einem geschützten Computer installiert.

Wenn Sie das Paket "Administrations-Tools" nicht auf dem geschützten Computer, sondern auf einem anderen Netzwerkcomputer installiert haben, nehmen Sie Erweiterte Einstellungen vor (siehe Abschnitt "Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Computer" auf Seite 44).

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 2.2 von den Benutzern ferngesteuert verwaltet werden kann:

- Fügen Sie auf dem geschützten Computer die Benutzer von Kaspersky Embedded Systems Security 2.2 zur Gruppe ESS Administrators hinzu.
- Erlauben Sie die Netzwerkverbindungen für den Dienst Kaspersky Security Management Service (kavfsgt.exe) (Siehe Abschnitt "Über Zugriffsrechte für den Verwaltungsdienst Kaspersky Security Management Service" auf Seite 86), wenn auf dem geschützten Computer die Windows-Firewall oder die Firewall eines Drittherstellers verwendet wird.
- Wenn Sie während der Installation der Programmkonsole auf einem Computer unter Microsoft Windows das Kontrollkästchen **Remote-Zugriff erlauben** nicht aktiviert haben, erlauben Sie Netzwerkverbindungen für die Konsole für die Programmkonsole manuell über die Firewall auf diesem Computer.

Netzwerkverbindungen für die Programmkonsole erlauben

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

Die Programmkonsole auf dem Remote-Computer verwendet das Protokoll DCOM, um Informationen über die Ereignisse für Kaspersky Embedded Systems Security 2.2, 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.

Auf dem Remote-Computer, auf dem die Programmkonsole installiert ist, gehen Sie 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 die ausführbare Datei des Fernverwaltungsprozesses für Kaspersky Embedded Systems Security 2.2 kavfsrcn.exe.

  Über TCP-Port 135 greift der Client-Computer, auf dem die Programmkonsole installiert ist, auf den geschützten Computer zu und der Computer beantwortet seine Anfragen.
- Konfigurieren Sie die Regeln für ausgehende Verbindungen der Windows-Firewall, um eine Verbindung zuzulassen.

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

Führen Sie zur Konfiguration jeder anderen Software- oder Hardware-Firewall die gleichen Schritte aus.

Wenn die Programmkonsole geöffnet war, während Sie die Verbindung zwischen dem geschützten Computer und dem Computer, auf dem die Programmkonsole installiert ist, angepasst haben, müssen Sie die Programmkonsole schließen, auf die Beendigung des Prozesses zur Remote-Verwaltung von Kaspersky Embedded Systems Security 2.2 kavfsrcn.exe warten und die Programmkonsole anschließend neu starten. Die neuen Verbindungseinstellungen werden angewendet.

► *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 2.2 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** des 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**.

► *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 2.2 zu erlauben, gehen Sie wie folgt vor:*

1. Schließen Sie die Konsole für Kaspersky Embedded Systems Security 2.2 auf dem Remote-Computer.
2. Führen Sie eine der Aktionen durch:
   - In Microsoft Windows XP oder Microsoft Windows Vista™:
     a. Klicken Sie in Microsoft Windows XP SP2 oder höher auf **Start** > **Windows-Firewall**.

        Klicken Sie in Microsoft Windows Vista auf **Start** > **Systemsteuerung** > **Windows-Firewall** und wählen Sie im Fenster **Windows-Firewall** den Punkt **Einstellungen ändern** aus.

b. Klicken Sie im Fenster Windows-Firewall (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 2.2. 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 Ordner, den Sie bei der Installation der Konsole für Kaspersky Embedded Systems Security 2.2 mithilfe von Microsoft Management Console als Zielordner angegeben haben.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf die Schaltfläche **OK** im Fenster **Windows-Firewall (Einstellungen für Windows-Firewall**).

► *Ausgehende Regel für Windows-Firewall hinzufügen:*

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 sich öffnenden 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 2.2 ausgeführt werden müssen

Wenn Sie das Programm aktiviert haben, startet Kaspersky Embedded Systems Security 2.2 die Aufgaben zum Schutz und zur Untersuchung sofort nach der Installation. Wenn während der Installation von Kaspersky Embedded Systems Security 2.2 die Option **Echtzeitschutz nach der Installation des Programms aktivieren** (Standardoption) ausgewählt wurde, untersucht das Programm die Objekte des Dateisystems des Computers, wenn darauf zugegriffen wird. Jeden Freitag um 20:00 Uhr führt Kaspersky Embedded Systems Security 2.2 die Aufgabe Untersuchung wichtiger Bereiche aus.

Es wird empfohlen, nach der Installation von Kaspersky Embedded Systems Security 2.2 folgende Aktionen auszuführen:

- Die Aufgabe zum Update der Programm-Datenbanken starten. Nach der Installation untersucht Kaspersky Embedded Systems Security 2.2 Objekte anhand von Datenbanken, die im Lieferumfang des Programms enthalten sind.

  Es wird empfohlen, sofort ein Update der Datenbanken von Kaspersky Embedded Systems Security 2.2 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 2.2 auf dem geschützten Computer kein Virenschutzprogramm mit aktivierter Funktion zum Echtzeitschutz für Dateien installiert war.
- Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security 2.2 anpassen.

In diesem Abschnitt

Aufgabe Update der Programm-Datenbanken von Kaspersky Embedded Systems Security 2.2 starten und anpassen

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

1. Konfiguration einer Verbindung zur 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.

► *Um die Verbindung zu den Kaspersky-Lab-Update-Servern in der Aufgabe 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 2.2** > **Administrations-Tools** > **Konsole für Kaspersky Embedded Systems Security 2.2**.
   - Wenn Sie die Programmkonsole nicht auf einem geschützten Computer gestartet haben, stellen Sie eine Verbindung mit dem geschützten Computer her:
     a. Öffnen Sie das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens 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. 86), 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 folgenden Fenster **Aufgabeneinstellungen** die Registerkarte **Verbindungseinstellungen**.
6. Führen Sie folgende Aktionen aus:
   a. Wenn in Ihrem Netzwerk das Web Proxy Auto-Discovery Protocol (WPAD-Protokoll) zur automatischen Erkennung von Proxyservern in einem lokalen Netzwerk eingerichtet ist, tragen Sie die Einstellungen des Proxyservers ein: Aktivieren Sie im Einstellungsblock **Proxyserver-Einstellungen** das Kontrollkästchen **Einstellungen des angegebenen Proxyservers verwenden**, tragen Sie im Feld **Adresse** die Adresse und im Feld **Port** die Portnummer des Proxyservers ein.
   b. Wenn in Ihrem Netzwerk eine Authentifizierung für den Zugriff auf den Proxyserver erforderlich ist, wählen Sie die gewünschte Methode zur Authentifizierung in der Dropdown-Liste des Blocks **Einstellungen für die Authentifizierung auf dem Proxyserver** aus:
      - **NTLM-Authentifizierung verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung (NTLM-authentication) unterstützt. Kaspersky Embedded Systems Security 2.2 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 2.2 verwendet das von Ihnen vorgegebene Benutzerkonto für die Authentifizierung am 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 **Aufgabeneinstellungen** auf **OK**.

Die Verbindungseinstellungen mit der Update-Quelle werden in der Aufgabe 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 Ergebnisbereich des Knotens **Kaspersky Embedded Systems Security** anzeigen.

Untersuchung wichtiger Bereiche

Nachdem Sie die Datenbanken von Kaspersky Embedded Systems Security 2.2 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. Öffnen 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 Arbeitsbereich wird der Aufgabenstatus als **Läuft** angegeben.

► *Um das Protokoll über Ausgabenausführung anzuzeigen, machen Sie Folgendes,*

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

Ändern der Programmkomponenten und Wiederherstellen von Kaspersky Embedded Systems Security 2.2

Komponenten von Kaspersky Embedded Systems Security 2.2 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 der Zugriff auf die Programmverwaltung kennwortgeschützt ist, verlangt Kaspersky Embedded Systems Security 2.2 beim Versuch, im erweiterten Schritt des Assistenten Programmkomponenten zu löschen oder ihre Zusammensetzung zu verändern, die Eingabe des Kennworts.

► *Um die Programmkomponenten von Kaspersky Embedded Systems Security 2.2 zu ändern, gehen Sie wie folgt vor:*

1. Klicken Sie auf **Start** und wählen Sie den Punkt **Alle Programme > Kaspersky Embedded Systems Security 2.2 > 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 für die Installation verfügbaren Komponenten die Komponenten, die Sie zu Kaspersky Embedded Systems Security 2.2 hinzufügen bzw. 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 und wählen Sie im Kontextmenü:
     - den Punkt **Die Komponente wird auf der lokalen Festplatte installiert**, wenn Sie eine einzelne Komponente installieren möchten,
     - den Punkt **Die Komponente und ihre Teilkomponenten werden auf der lokalen Festplatte installiert**, wenn Sie eine Gruppe von Komponenten installieren möchten.
   - Um früher installierte Komponenten zu entfernen, klicken Sie auf die Schaltfläche neben dem Namen der ausgewählten Komponente und wählen Sie im Kontextmenü den Punkt **Die Komponente wird nicht verfügbar sein**.

   Klicken Sie auf **Installieren**.

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 2.2 wird gemäß den angegebenen Einstellungen geändert.

Wenn bei der Ausführung von Kaspersky Embedded Systems Security 2.2 Probleme aufgetreten sind (Kaspersky Embedded Systems Security 2.2 stürzt ab, Aufgaben stürzen ab oder werden nicht gestartet), können Sie versuchen, Kaspersky Embedded Systems Security 2.2 zu reparieren. Wenn die Reparatur ausgeführt wird, können entweder die aktuellen Werte der Einstellungen von Kaspersky Embedded Systems Security 2.2 beibehalten werden, oder alle Einstellungen von Kaspersky Embedded Systems Security 2.2 können auf die Standardwerte zurückgesetzt werden.

► *Um Kaspersky Embedded Systems Security 2.2 nach der fehlerhaften Beendigung des Programms oder der Aufgaben wieder herzustellen, gehen Sie wie folgt vor:*

1. Klicken Sie auf **Start** und wählen Sie den Punkt **Alle Programme > Kaspersky Embedded Systems Security 2.2 > Ändern oder Löschen** aus.

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

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

   Das Fenster **Installierte Komponenten reparieren** wird geöffnet.

3. Aktivieren Sie im Fenster **Installierte Komponenten reparieren** das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**, wenn Sie die konfigurierten Einstellungen des Programms zurücksetzen und Kaspersky Embedded Systems Security 2.2 mit den vorinstallierten Standardeinstellungen wiederherstellen möchten. Klicken Sie auf **Installieren**.
4. Bestätigen Sie im Fenster **Bereit zur Wiederherstellung** den Vorgang zur Wiederherstellung der Zusammensetzung des Programms, indem Sie auf die Schaltfläche **Installieren** klicken.
5. Klicken Sie im Fenster, das nach Abschluss der Wiederherstellung geöffnet wird, auf **OK**.

Kaspersky Embedded Systems Security 2.2 wird gemäß den angegebenen Einstellungen wiederhergestellt.

Deinstallation mit dem Installationsassistenten

Dieser Abschnitt enthält Anleitungen zur Deinstallation von Kaspersky Embedded Systems Security 2.2 und der Programmkonsole von einem geschützten Computer mithilfe des Installationsassistenten.

In diesem Abschnitt

Deinstallation von Kaspersky Embedded Systems Security 2.2

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

Sie können Kaspersky Embedded Systems Security 2.2 mit dem Installations-/Deinstallationsassistenten vom geschützten Computer deinstallieren.

Nach der Deinstallation von Kaspersky Embedded Systems Security 2.2 von einem geschützten Computer ist möglicherweise ein Neustart erforderlich. Sie können den Neustart verschieben.

Das Löschen, die Wiederherstellung und das Hinzufügen des Programms über die Windows-Systemsteuerung sind nicht möglich, wenn das Betriebssystem die Funktion Benutzerkontensteuerung (User Account Control) verwendet oder wenn der Zugriff auf die Programmverwaltung kennwortgeschützt ist.

Wenn der Zugriff auf die Programmverwaltung kennwortgeschützt ist, verlangt Kaspersky Embedded Systems Security 2.2 beim Versuch, im erweiterten Schritt des Assistenten Programmkomponenten zu löschen oder ihre Zusammensetzung zu verändern, die Eingabe des Kennworts.

► *So deinstallieren Sie Kaspersky Embedded Systems Security 2.2:*

1. Klicken Sie auf **Start** und wählen Sie den Punkt **Alle Programme > Kaspersky Embedded Systems Security 2.2 > Ändern oder Löschen** aus.

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

2. Wählen Sie den Punkt **Entfernen von Programmkomponenten** aus. Klicken Sie auf **Weiter**.

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

3. 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 2.2 die Quarantäneobjekte exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Aktivieren Sie das Kontrollkästchen **Backup-Objekte exportieren**, damit Kaspersky Embedded Systems Security 2.2 die 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 wiederhergestellten Objekte exportieren möchten. Standardmäßig erfolgt der Export von Objekten in den Ordner: %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\Uninstall.

   Klicken Sie auf **Weiter**.

4. Bestätigen Sie im Fenster **Bereit zur Deinstallation** den Löschvorgang, indem Sie auf die Schaltfläche **Entfernen** klicken.

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

Kaspersky Embedded Systems Security 2.2 wird von einem geschützten Computer deinstalliert.

Deinstallation der Konsole für Kaspersky Embedded Systems Security 2.2

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

Sie können die Programmkonsole mit Hilfe 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 **Startmenü** den Punkt **Alle Programme > Kaspersky Embedded Systems Security 2.2 > Administrations-Tools > Ändern oder Löschen** aus.

2. Das Fenster **Installation ändern, reparieren oder entfernen** des Assistenten wird geöffnet.

   Wählen Sie die Variante **Entfernen von Programmkomponenten** und klicken Sie auf **Weiter**.

3. Es öffnet sich das Fenster **Bereit zur Deinstallation**. Klicken Sie auf die Schaltfläche **Löschen**.

   Es öffnet sich das Fenster **Die Deinstallation wurde abgeschlossen**.

4. Klicken Sie auf **OK**.

Der Deinstallationsvorgang wird abgeschlossen, und das Fenster des Assistenten 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 2.2 aus der Befehlszeile gelten. Außerdem finden Sie hier Beispiele für Befehle, mit denen Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile installiert und deinstalliert werden kann, sowie Beispiele für Befehle, mit denen Komponenten von Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile hinzugefügt oder entfernt werden können.

In diesem Abschnitt

Über die Installation und Deinstallation von Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile

Sie können Kaspersky Embedded Systems Security 2.2 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 \client\esstools.msi verwenden.

Installieren Sie mit Berechtigungen des Benutzerkontos, das zur Administratorengruppe auf dem Computer gehört, auf dem Sie installieren.

Wenn Sie auf dem geschützten Computer eine der Dateien aus \product\ess_x86(x64).msi ohne Reserveschlüssel starten, wird Kaspersky Embedded Systems Security 2.2 mit der empfohlenen Installation 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 2.2

Dieser Abschnitt bietet Beispiele für Befehle zur Installation von Kaspersky Embedded Systems Security 2.2.

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 2.2 aus der Datei setup.exe

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security 2.2 installieren mit den empfohlenen Installationseinstellungen zu installieren, ohne dass eine Interaktion mit dem Benutzer erfolgt:*

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

► *Um Kaspersky Embedded Systems Security 2.2 mit den folgenden Einstellungen zu installieren, gehen Sie wie folgt vor:*

- nur Komponente Echtzeitschutz für Dateien und Untersuchung auf Befehl installieren;
- den Echtzeitschutz beim Start von Kaspersky Embedded Systems Security 2.2 nicht starten
- und Dateien nicht von der Untersuchung auszuschließen, deren Ausnahme von Microsoft empfohlen wird,

führen Sie folgenden Befehl aus:

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

Beispiele für Befehle zur Installation: msi-Datei des Installationspakets starten

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security 2.2 installieren mit den empfohlenen Installationseinstellungen zu installieren, ohne dass eine Interaktion mit dem Benutzer erfolgt:*

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

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security 2.2 mit den empfohlenen Installationseinstellungen zu installieren und die Installationsoberfläche anzuzeigen:*

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

- *Um Kaspersky Embedded Systems Security 2.2 mit der Aktivierung aus der Schlüsseldatei C:\0000000A.key zu installieren:*

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

- *Um Kaspersky Embedded Systems Security 2.2 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
```

- *Um Kaspersky Embedded Systems Security 2.2 zu installieren und seine Dateien im Zielordner C:\ESS zu speichern, geben Sie den folgenden Befehl ein:*

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

- *Um Kaspersky Embedded Systems Security 2.2 zu installieren, speichern Sie die Log-Datei des Installationsprotokolls mit dem Namen ess.log im Ordner, in dem die msi-Datei des Installationspakets für Kaspersky Embedded Systems Security 2.2 gespeichert ist, und geben Sie den folgenden Befehl ein:*

```
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 2.2 mit den folgenden Einstellungen zu installieren:*

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

- *Um Kaspersky Embedded Systems Security 2.2 mit der Aktivierung aus der Schlüsseldatei C:\0000000A.key zu installieren und Kaspersky Embedded Systems Security 2.2 gemäß den in der Konfigurationsdatei C:\settings.xml beschriebenen Einstellungen anzupassen, geben Sie den folgenden Befehl ein:*

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

- *Um den Anwendungspatch bei der Ausführung von Kaspersky Embedded Systems Security 2.2 zu installieren, 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 2.2 ausgeführt werden müssen

Wenn Sie das Programm aktiviert haben, startet Kaspersky Embedded Systems Security 2.2 die Aufgaben zum Schutz und zur Untersuchung sofort nach der Installation. Wenn Sie während der Installation von Kaspersky Embedded Systems Security 2.2 die Option **Echtzeitschutz nach der Installation des Programms aktivieren** ausgewählt haben, untersucht das Programm die Objekte des Dateisystems des Computers, wenn darauf zugegriffen wird. Jeden Freitag um 20:00 Uhr führt Kaspersky Embedded Systems Security 2.2 die Aufgabe Untersuchung wichtiger Bereiche aus.

Es wird empfohlen, nach der Installation von Kaspersky Embedded Systems Security 2.2 folgende Aktionen auszuführen:

- Aufgabe Update der Programm-Datenbanken von Kaspersky Embedded Systems Security 2.2 starten. Nach der Installation untersucht Kaspersky Embedded Systems Security 2.2 Objekte anhand von Datenbanken, die im Lieferumfang enthalten sind. Es wird empfohlen, die sofort ein Datenbanken-Update für Kaspersky Embedded Systems Security 2.2 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 2.2 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 auf dem Computer durch, wenn vor der Installation von Kaspersky Embedded Systems Security 2.2 auf dem geschützten Computer 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 über Ausgabenausführung in der Datei scancritical.log im aktuellen Ordner.

- Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security 2.2 anpassen.

Komponenten hinzufügen und entfernen. Beispiele für Befehle

Die Komponente "Kontrolle des Programmstarts" 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 2.2 hinzuzufügen oder zu entfernen.

► *Um die Komponente Untersuchung auf Befehl zu den bereits installierten Komponenten hinzufügen, führen Sie folgenden Befehl aus:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn EULA=1 PRIVACYPOLICY=1
```

oder

```
\computer\setup.exe /s /p "ADDLOCAL=Oas,Ods" /p EULA=1 /p PRIVACYPOLICY=1
```

Wenn Sie nicht nur Komponenten, die Sie installieren möchten, sondern auch bereits installierte Komponenten angeben, installiert Kaspersky Embedded Systems Security 2.2 die angegebenen Komponenten neu.

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

```
msiexec /i ess.msi "ADDLOCAL=Oas,AppCtrl,Ksn,AntiExploit,DevCtrl,Firewall,
LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,TrayApp,AVPro
tection,RamDisk REMOVE=Ods,Fim" /qn
```

Deinstallation von Kaspersky Embedded Systems Security 2.2. Beispiele für Befehle

► *Um Kaspersky Embedded Systems Security 2.2 vom geschützten Computer zu deinstallieren, führen Sie folgenden Befehl aus:*

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

oder

- Für 32-Bit-Betriebssysteme:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn
```

► *Um die Konsole für Kaspersky Embedded Systems Security 2.2 zu deinstallieren, führen Sie folgenden Befehl aus:*

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

oder

- Für 32-Bit-Betriebssysteme:

```
msiexec /x {A727008F-F8CC-4B35-848A-1AECEEF22178} /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn
```

► *Um Kaspersky Embedded Systems Security 2.2 von einem geschützten Computer zu deinstallieren, auf dem der Kennwortschutz aktiviert ist, führen Sie folgenden Befehl aus:*

- Für 32-Bit-Betriebssysteme:

```
msiexec.exe /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec.exe /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn
```

Rückgabecodes

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

Tabelle 13. Rückgabecodes

Code	Beschreibung
1324	Der Name des Zielordners enthält unzulässige Zeichen.
25001	Unzureichende Rechte für die Installation von Kaspersky Embedded Systems Security 2.2. Um das Programm zu installieren, starten Sie den Installationsassistenten mit den Rechten des lokalen Administrators.
25003	Kaspersky Embedded Systems Security 2.2 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 2.2 über Kaspersky Security Center. Er beschreibt ferner, wie man Kaspersky Embedded Systems Security 2.2 über Kaspersky Security Center installiert und deinstalliert, sowie die Aktionen, die nach der Installation von Kaspersky Embedded Systems Security 2.2 ausgeführt werden müssen.

In diesem Abschnitt

Allgemeine Informationen zur Installation über Kaspersky Security Center

Sie können Kaspersky Embedded Systems Security 2.2 mithilfe einer Remote-Installationsaufgabe über Kaspersky Security Center installieren.

Nach Abschluss der Remote-Installationsaufgabe ist Kaspersky Embedded Systems Security 2.2 auf mehreren Computern mit einheitlichen Einstellungen installiert.

Alle Computer können in eine Administrationsgruppe zusammengeführt werden und Sie können eine Gruppenaufgabe zur Installation von Kaspersky Embedded Systems Security 2.2 auf den Computern dieser Gruppe erstellen.

Sie können eine Remote-Installationsaufgabe für Kaspersky Embedded Systems Security 2.2 erstellen, die sich auf eine Auswahl von Computern bezieht, die nicht zur gleichen Administrationsgruppe gehören. Legen Sie dazu eine Liste mit Computern an, auf denen Kaspersky Embedded Systems Security 2.2 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 2.2

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 2.2 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 2.2 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 2.2 installieren möchten, gehören zur gleichen Domäne wie der Administrationsserver und der Administrationsserver ist unter dem 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, ausführen.

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$**-Ressource
- Recht **Als Dienst starten**

Ablauf der Installation von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2).
- Auf den geschützten Computern ist der Administrationsagent von Kaspersky Security Center installiert. Wenn der Administrationsagent von Kaspersky Security Center nicht auf den geschützten Computern installiert ist, können Sie ihn im Rahmen der Remote-Installationsaufgabe zusammen mit Kaspersky Embedded Systems Security 2.2 installieren.

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

► *Um Kaspersky Embedded Systems Security 2.2 mithilfe einer Aufgabe zur Remote-Installation zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Erweitern Sie im Kaspersky Security Center den Knoten **Remote-Installation**, und wählen Sie im untergeordneten Knoten **Installationspakete** die Option **Installationspaket für ein Kaspersky Lab-Programm** erstellen.
3. Geben Sie den Namen des Installationspakets ein.
4. Geben Sie die Datei "ess.kud" aus dem Lieferumfang von Kaspersky Embedded Systems Security 2.2 als Installationspaketdatei an.

   Das Fenster **EULA und Datenschutzrichtlinie** wird geöffnet.
5. Wenn Sie mit den Bedingungen der EULA und der Datenschutzrichtlinie einverstanden sind, aktivieren Sie die Kontrollkästchen **Bedingungen dieser EULA** und **Datenschutzrichtlinie, die den Umgang mit Daten beschreibt**, um mit der Installation fortzufahren.

   Sie müssen den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie akzeptieren, um fortzufahren.
6. So ändern Sie den Umfang der zu installierenden Komponenten von Kaspersky Embedded Systems Security 2.2 (siehe Abschnitt "Ändern der Programmkomponenten und Wiederherstellen von Kaspersky Embedded Systems Security 2.2" auf Seite 49) und die standardmäßigen Installationseinstellungen (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 30) im Installationspaket:
   a. Öffnen Sie im Kaspersky Security Center den Knoten **Remote-Installation**.
   b. Öffnen Sie im untergeordneten Knoten **Installationspakete** im Arbeitsbereich das Kontextmenü für das neu erstellte Installationspaket von Kaspersky Embedded Systems Security 2.2. 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 der Komponenten von Kaspersky Embedded Systems Security 2.2, 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**.

7. Erstellen Sie im Knoten **Installationspakete** eine Aufgabe zur Remote-Installation von Kaspersky Embedded Systems Security 2.2 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*.

8. Starten Sie die Remote-Installationsaufgabe für Kaspersky Embedded Systems Security 2.2.

Kaspersky Embedded Systems Security 2.2 wird auf den in der Aufgabe angegebenen Computern installiert.

Aktionen, die nach der Installation von Kaspersky Embedded Systems Security 2.2 ausgeführt werden müssen

Nach der Installation von Kaspersky Embedded Systems Security 2.2 wird empfohlen, die Datenbanken von Kaspersky Embedded Systems Security 2.2 auf den Computern zu aktualisieren. Sollte vor der Installation von Kaspersky Embedded Systems Security 2.2 auf den Computern kein Virenschutzprogramm mit aktiviertem Echtzeitschutz installiert gewesen sein, wird außerdem empfohlen, eine Untersuchung wichtiger Bereiche der Computer durchzuführen.

Wenn Computer, auf denen Sie Kaspersky Embedded Systems Security 2.2 installiert haben, von Kaspersky Security Center zu einer Administrationsgruppe zusammengefasst sind, können Sie diese Aufgaben auf folgende Arten ausführen:

1. Für die Gruppe der Computer, auf denen Sie Kaspersky Embedded Systems Security 2.2 installiert haben, eine Aufgabe zum Update der Programm-Datenbanken erstellen. Den Administrationsserver für Kaspersky Security Center als Update-Quelle festlegen.
2. Eine Gruppenaufgabe zur Untersuchung auf Befehl mit dem Aufgabenstatus Untersuchung wichtiger Bereiche erstellen. Das Programm Kaspersky Security Center bewertet den Sicherheitszustand jedes Computers der Gruppe dann aufgrund der Ausführungsergebnisse dieser Gruppe, nicht nach den Ergebnissen der Systemaufgabe Untersuchung wichtiger Bereiche.
3. Erstellen Sie eine neue Richtlinie für die Computergruppe. In den Eigenschaften der erstellten Richtlinie auf der Registerkarte **Systemaufgaben** den nach Zeitplan gesteuerten Start von Systemaufgaben zur Untersuchung auf Befehl und Update der Programm-Datenbanken auf den Computern der Administrationsgruppe deaktivieren.

Sie können auch die Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security 2.2 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. Erweitern Sie in der Verwaltungskonsole für Kaspersky Security Center den Knoten **Remote-Installation** und erstellen Sie im untergeordneten Knoten **Installationspakete** auf Basis der Datei client\setup.exe ein neues Installationspaket. Um das neue Installationspaket zu erstellen:
   - Geben Sie im Fenster **Auswahl des Installationspakets** die Datei client\setup.exe aus dem Ordner des Lieferumfangs von Kaspersky Embedded Systems Security 2.2 an und aktivieren Sie das Kontrollkästchen **Updates von Repository in das Installationspaket kopieren**.
   - 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, geben Sie folgenden Befehl ein:

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1
     PRIVACYPOLICY=1"
     ```
2. Erstellen Sie im 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*.
3. Starten Sie die angelegte Aufgabe zur Remote-Installation.

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

Deinstallation von Kaspersky Embedded Systems Security 2.2 über Kaspersky Security Center

Wenn der Zugriff auf die Verwaltung von Kaspersky Embedded Systems Security 2.2 auf den Computern im Netzwerk kennwortgeschützt ist, geben Sie beim Erstellen der Aufgabe zum Löschen von Programmgruppen das Kennwort ein. Wenn der Kennwortschutz nicht zentralisiert mit einer Richtlinie von Kaspersky Security Center verwaltet wird, wird Kaspersky Embedded Systems Security 2.2 erfolgreich von den Computern deinstalliert, auf denen der Zugriff auf die Programmverwaltung mit einem Kennwort geschützt ist, das mit dem eingegebenen Kennwort übereinstimmt. Kaspersky Embedded Systems Security 2.2 wird nicht von den restlichen Computern deinstalliert.

► *Um Kaspersky Embedded Systems Security 2.2 zu deinstallieren, führen Sie in der Verwaltungskonsole von Kaspersky Security Center folgende Aktionen aus:*

1. Erstellen 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 2.2 nur mit den Standardinstallationseinstellungen deinstallieren (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 30).

Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory

In diesem Abschnitt wird die Installation und Deinstallation von Kaspersky Embedded Systems Security 2.2 über Gruppenrichtlinien von Active Directory beschrieben. Er enthält ferner Informationen über die Aktionen, die nach der Installation von Kaspersky Embedded Systems Security 2.2 über Gruppenrichtlinien ausgeführt werden müssen.

In diesem Abschnitt

Installation von Kaspersky Embedded Systems Security 2.2 über Gruppenrichtlinien von Active Directory

Sie können Kaspersky Embedded Systems Security 2.2 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 2.2 oder die Programmkonsole installieren möchten, müssen zu einer Domäne und einer Organisationseinheit gehören.

Die Betriebssysteme auf den Computern, auf denen Sie Kaspersky Embedded Systems Security 2.2 mithilfe der Richtlinie installieren wollen, müssen die gleiche Bit-Version (32-Bit oder 64-Bit) besitzen.

Sie müssen über Administratorrechte auf der Domain verfügen.

Um Kaspersky Embedded Systems Security 2.2 zu installieren, verwenden Sie die Installationspakete ess_x86(x64).msi. Um die Programmkonsole zu installieren, verwenden Sie das Installationspaket esstools.msi.

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

► *Um Kaspersky Embedded Systems Security 2.2 (oder die Programmkonsole) zu installieren, gehen Sie wie folgt vor:*

1. Speichern Sie die msi-Datei des Installationspakets, die der Bit-Version (32-Bit oder 64-Bit) des installierten Microsoft Windows-Betriebssystems entspricht, in einem freigegebenen Ordner auf dem Domain-Controller.
2. Erstellen Sie auf dem Domain-Controller eine neue Richtlinie für die Gruppe, zu der die Computer gehören.
3. Legen Sie mit dem **Group Policy Object Editor** ein neues Installationspaket im Knoten **Computer-Konfiguration** an. Geben Sie den Pfad zur msi-Datei des Installationspakets für Kaspersky Embedded Systems Security 2.2 (oder die Programmkonsole) im UNC-Format (Universal Naming Convention) ein.
4. 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** für eine ausgewählte Gruppe.
5. Übernehmen Sie die Änderungen mit dem Befehl `gpupdate /force`.

Kaspersky Embedded Systems Security 2.2 wird auf den Computern der Gruppe nach deren Neustart und vor der Anmeldung bei Microsoft Windows installiert.

Aktionen, die nach der Installation von Kaspersky Embedded Systems Security 2.2 ausgeführt werden müssen

Nach der Installation von Kaspersky Embedded Systems Security 2.2 auf den geschützten Computern wird empfohlen, sofort die Programm-Datenbanken zu aktualisieren und eine Untersuchung wichtiger Bereiche des Computers durchzuführen. Sie können diese Aktionen (siehe Abschnitt "Aktionen, die nach der Installation von Kaspersky Embedded Systems Security 2.2 ausgeführt werden müssen" auf Seite 47) in der Programmkonsole ausführen.

Sie können auch die Benachrichtigungen des Administrators über Ereignisse in Kaspersky Embedded Systems Security 2.2 anpassen.

Deinstallation von Kaspersky Embedded Systems Security 2.2 über Gruppenrichtlinien von Active Directory

Wenn Sie Kaspersky Embedded Systems Security 2.2 (oder die Programmkonsole) auf den Gruppencomputern mithilfe der Gruppenrichtlinie von Active Directory installiert haben, können Sie diese Richtlinie zur Deinstallation von Kaspersky Embedded Systems Security 2.2 (oder der Programmkonsole) verwenden.

Sie können das Programm nur mit den Standarddeinstallationseinstellungen entfernen.

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 der Zugriff auf die Programmverwaltung kennwortgeschützt ist, ist die Deinstallation von Kaspersky Embedded Systems Security 2.2 über die Gruppenrichtlinien von Active Directory nicht möglich.

► *Um Kaspersky Embedded Systems Security 2.2 (oder die Programmkonsole) zu deinstallieren, gehen Sie wie folgt vor:*

1. Wählen Sie auf dem Domain-Controller eine Organisationseinheit aus, von deren Computern Sie Kaspersky Embedded Systems Security 2.2 oder die Programmkonsole deinstallieren möchten.
2. Wählen Sie eine Richtlinie aus, die für die Installation von Kaspersky Embedded Systems Security 2.2 erstellt wurde, öffnen Sie im **Editor für Gruppenrichtlinien** im Knoten **Software-Installation** (**Computerkonfiguration** > **Software-Konfiguration** > **Software-Installation**) das Kontextmenü des Installationspakets für Kaspersky Embedded Systems Security 2.2 (die Programmkonsole) und wählen Sie den Befehl **Alle Aufgaben > Löschen**.
3. Wählen Sie die Entfernungsmethode **Sofortige Deinstallation der Software von Benutzern und Computern**.
4. Übernehmen Sie die Änderungen mit dem Befehl `gpupdate /force`.

Kaspersky Embedded Systems Security 2.2 wird von den Computern nach deren Neustart und vor der Anmeldung bei Microsoft Windows deinstalliert.

Funktionsüberprüfung für Kaspersky Embedded Systems Security 2.2. Verwendung des EICAR-Testvirus

Dieser Abschnitt beschreibt den EICAR-Testvirus und das Vorgehen, mit dem die Funktionen "Echtzeitschutz" und "Untersuchung auf Befehl" von Kaspersky Embedded Systems Security 2.2 mithilfe des EICAR-Testvirus überprüft werden.

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 Schädling und enthält keinen Programmcode, 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 2.2 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 über Ausgabenausführung angezeigt.

Sie können die Datei eicar.com verwenden, um zu prüfen, wie Kaspersky Embedded Systems Security 2.2 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 2.2 die Datei eicar.com mit einem Präfix verarbeiten kann, aktivieren Sie im Block der Sicherheitseinstellungen **Schutz von Objekten** die Option **Alle Objekte** für die Aufgaben zum Echtzeitschutz für Dateien und die Aufgaben zur Untersuchung auf Befehl in Kaspersky Embedded Systems Security 2.2.

Tabelle 14. Präfixe in EICAR-Dateien

Präfix	Dateistatus nach Untersuchung und Aktion von Kaspersky Embedded Systems Security 2.2
Ohne Präfix	Kaspersky Embedded Systems Security 2.2 weist dem Objekt den Status **Infiziert oder gefunden** zu und löscht es.
SUSP–	Kaspersky Embedded Systems Security 2.2 weist dem Objekt den Status **Möglicherweise infiziert** (mit heuristischer Analysemethode erkannt) zu und löscht es (möglicherweise infizierte Objekte werden nicht desinfiziert).
WARN–	Kaspersky Embedded Systems Security 2.2 weist dem Objekt den Status **Möglicherweise infiziert** (Code des Objektes stimmt partiell mit einem bekannten schädlichen Code überein) zu und löscht es (möglicherweise infizierte Objekte werden nicht desinfiziert).
CURE–	Kaspersky Embedded Systems Security 2.2 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.

Test von Echtzeitschutz und Untersuchung auf Befehl

Nach der Installation von Kaspersky Embedded Systems Security 2.2 können Sie bestätigen, dass Kaspersky Embedded Systems Security 2.2 Objekte erkennt, die bösartigen Code enthalten. Zur Überprüfung können Sie den EICAR-Testvirus verwenden (siehe Abschnitt "EICAR-Testvirus" auf Seite 66).

► *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 in diesem Ordner deaktiviert ist.

2. Wenn Sie außerdem noch die Benachrichtigungen für die Benutzer des Netzwerks prüfen möchten, vergewissern Sie sich, dass auf dem geschützten Computer und 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 Funktion Benachrichtigung über Terminaldienste zu überprüfen, kopieren Sie die Datei eicar.com auf einen Computer, der mithilfe des Programms "Remote Desktop Connection" an den Computer angeschlossen ist.
   - Um die Funktion Benachrichtigung über den Windows Messenger Dienst zu überprüfen, kopieren Sie die Datei eicar.com von dem Computer, auf dem Sie sie gespeichert haben, über die Netzwerkumgebung dieses Computers.

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

- Die Datei eicar.com wurde vom geschützten Computer gelöscht.
- In der Programmkonsole wurde dem Protokoll über Ausgabenausführung der Status **Kritisch** zugewiesen. Im Protokoll ist eine Zeile mit Informationen über eine Bedrohung in der Datei eicar.com erschienen. (Um einen Protokoll über Ausgabenausführung anzuzeigen, erweitern Sie in der Struktur der Programmkonsole den Knoten **Echtzeitschutz des Computers**, wählen Sie die Aufgabe Echtzeitschutz für Dateien aus, und klicken Sie im Ergebnisbereich des Knotens auf den Link **Protokoll öffnen**).
  - Auf dem Computer, von dem aus Sie die Datei kopiert haben, wird eine Meldung des Windows Messenger Dienstes mit folgendem Inhalt angezeigt: "Kaspersky Embedded Systems Security 2.2 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>".

    Sehen Sie nach, ob 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 in diesem Ordner deaktiviert ist.

2. Öffnen Sie die Programmkonsole.

3. Führen Sie folgende Aktionen aus:
   a. Öffnen 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 wurde von der Festplatte des Computers gelöscht.
- In der Programmkonsole weist der Protokoll über Ausgabenausführung den Status **Kritisch** auf. Im Ausführungsprotokoll für die Aufgabe zur Untersuchung wichtiger Bereiche ist eine Zeile mit Informationen über eine Bedrohung in der Datei eicar.com enthalten. (Um einen Protokoll über Ausgabenausführung aufzurufen, erweitern Sie in der Struktur der Programmkonsole den Knoten **Untersuchung auf Befehl**, wählen Sie die Aufgabe Untersuchung wichtiger Bereiche aus, und klicken Sie im Ergebnisbereich auf den Link **Protokoll öffnen**.)

Programmoberfläche

Sie können Kaspersky Embedded Systems Security 2.2 über die lokale Programmkonsole und dem Verwaltungs-Plug-In verwalten. Aktionen, die über die lokale Programmkonsole ausgeführt werden können, finden Sie im *Benutzerhandbuch für Kaspersky Embedded Systems Security 2.2*. Die Benutzung des Verwaltungs-Plug-ins erfolgt in der Benutzeroberfläche der Verwaltungskonsole von Kaspersky Security Center. 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 2.2
- 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
- Technischer Support

Der Leistungsumfang und die Nutzungsdauer des Programms hängen vom Lizenztyp ab, unter dem das Programm aktiviert wurde.

Das Programm wird mit einem Schlüssel für eine erworbene kommerzielle Lizenz aktiviert.

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

Kaspersky Embedded Systems Security 2.2 bietet zwei Typen von kommerziellen Lizenzen:

- Standardlizenz für Kaspersky Embedded Systems Security
- Die erweiterte Lizenz für Kaspersky Embedded Systems Security Compliance Edition, die zwei zusätzliche Komponenten für die System-Diagnose beinhaltet: "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 Kaspersky Embedded Systems Security 2.2-Datenbanken nicht aktualisiert werden). Zur weiteren Nutzung von Kaspersky Embedded Systems Security 2.2 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 Aktivierungscode

Ein *Aktivierungscode* ist eine eindeutige Zeichenfolge, die aus 20 Buchstaben und Ziffern besteht. Sie müssen einen Aktivierungscode eingeben, um einen Schlüssel zum Aktivieren von Kaspersky Embedded Systems Security 2.2 hinzuzufügen. Der Aktivierungscode wird an die E-Mail-Adresse übermittelt, die Sie beim Kauf von Kaspersky Embedded Systems Security 2.2 angegeben haben.

Um das Programm mit einem Aktivierungscode zu aktivieren, ist ein Internetzugang für die Verbindung mit den Kaspersky-Lab-Aktivierungsservern erforderlich.

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

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 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 Sie von Kaspersky Lab erhalten. Mit der Schlüsseldatei wird ein Schlüssel hinzugefügt. Mit diesem Schlüssel wird das Programm aktiviert.

Eine Schlüsseldatei wird an die E-Mail-Adresse übermittelt, die Sie beim Kauf von Kaspersky Embedded Systems Security 2.2 angegeben haben.

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

Eine versehentlich gelöschte Schlüsseldatei kann wiederhergestellt werden. Die Schlüsseldatei kann unter anderem auch für die Registrierung bei Kaspersky CompanyAccount erforderlich sein.

Zur Wiederherstellung der Schlüsseldatei stehen Ihnen die folgenden Optionen zur Verfügung:

- Kontaktaufnahme mit dem Technischen Support https://support.kaspersky.com/de.
- Eine Schlüsseldatei auf der Website von Kaspersky Lab auf Basis des vorhandenen Aktivierungscodes anfordern.

Über die Bereitstellung von Daten

Im Endbenutzer-Lizenzvertrag für Kaspersky Embedded Systems Security 2.2, 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 das Lizenzzertifikat: Identifikator des zu installierenden Programms und dessen Vollversion, einschließlich Versionsnummer, Typ und Lizenz-ID, Installations-Identifikator, eindeutige 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 des Endbenutzer-Lizenzvertrags 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 2.2 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), die den vollständigen Text des Endbenutzer-Lizenzvertrags enthält. Diese Datei ist neben den Programminstallationsdateien Teil des Lieferumfangs von Kaspersky Embedded Systems Security 2.2.

Lokale Datenverarbeitung

Während der Ausführung der in diesem Handbuch beschriebenen Hauptfunktionen des Programms verarbeitet und speichert Kaspersky Embedded Systems Security 2.2 lokal eine Folge von Daten auf dem geschützten Computer:

- 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, 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, Instanzen von ausführbaren Dateien, die gestartet werden, und die Typen, Namen, Prüfsummen und Attribute dieser Dateien.

Kaspersky Embedded Systems Security 2.2 verarbeitet und speichert Daten als Teil der Grundfunktionalität des Programms, insbesondere für die Protokollierung von Programmereignissen und den Empfang von Diagnosedaten. Lokal verarbeitete Daten werden entsprechend den konfigurierten und angewandten Programmeinstellungen verarbeitet und geschützt.

Mit Kaspersky Embedded Systems Security 2.2 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 auf dem Laufwerk, auf dem die Daten protokolliert werden, ändern.

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

Standardmäßig werden alle auf einem lokalen Computer gespeicherten Daten nach der Deinstallation von Kaspersky Embedded Systems Security 2.2 entfernt. Ausgenommen davon sind Dateien mit Diagnoseinformationen (Trace- und Dump-Dateien) sowie die Einträge zur Programmaktivität im Windows-Ereignisprotokoll. Sie müssen diese Dateien manuell entfernen. Detaillierte Informationen zum Konfigurieren von Diagnoseprozessen finden Sie in den entsprechenden Abschnitten dieses Handbuchs.

Bei der Deinstallation des Programms können Sie die Inhalte der Quarantäne und des Backups speichern.

Aktivierung des Programms mithilfe eines Schlüssels

Sie können Kaspersky Embedded Systems Security 2.2 aktivieren, indem Sie einen Schlüssel anwenden.

Wenn Sie einen Schlüssel als aktiven Schlüssel hinzufügen und in Kaspersky Embedded Systems Security 2.2 bereits ein anderer aktiver Schlüssel hinzugefügt worden ist, wird der zuvor hinzugefügte Schlüssel durch den neuen ersetzt. Der früher hinzugefügte aktive Schlüssel wird gelöscht.

Wenn Sie einen Schlüssel als Reserveschlüssel hinzufügen und in Kaspersky Embedded Systems Security 2.2 bereits ein anderer Reserveschlüssel hinzugefügt worden ist, wird der zuvor hinzugefügte Schlüssel durch den neuen ersetzt. Der früher hinzugefügte Reserveschlüssel wird gelöscht.

Wenn Sie einen neuen Schlüssel als aktiven Schlüssel hinzufügen und in Kaspersky Embedded Systems Security 2.2 bereits ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt worden sind, wird der zuvor hinzugefügte aktive Schlüssel durch den neuen ersetzt und der Reserveschlüssel wird nicht gelöscht.

► *So aktivieren Sie Kaspersky Embedded Systems Security 2.2:*

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 den Schlüssel auch als Reserve hinzufügen. Aktivieren Sie dazu das Kontrollkästchen **Als Reserveschlüssel verwenden**.

4. Klicken Sie auf **OK**.

Der ausgewählte Schlüssel wird angewendet. Die Informationen über den hinzugefügten Schlüssel werden im Ergebnisbereich des Knotens **Lizenzverwaltung** angezeigt.

Aufrufen von Informationen über die aktive Lizenz

Lizenzinformationen anzeigen

Die Informationen zur aktuellen Lizenz werden im Ergebnisbereich des **Kaspersky Embedded Systems Security** Hauptknotens der Programmkonsole angezeigt. Der Schlüsselstatus kann folgende Werte annehmen:

- **Schlüsselstatus wird überprüft** – Kaspersky Embedded Systems Security 2.2 überprüft eine hinzugefügte Schlüsseldatei oder einen verwendeten Aktivierungscode und wartet auf die Antwort zum aktuellen Lizenzstatus.
- **Gültigkeitsdauer der Lizenz** – Kaspersky Embedded Systems Security 2.2 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 Reserveschlüssel oder Aktivierungscode hinzugefügt
  - Der hinzugefügte Schlüssel befindet sich in der schwarzen Liste und seine Blockierung steht unmittelbar bevor
- **Das Programm wurde nicht aktiviert** – Kaspersky Embedded Systems Security 2.2 ist nicht aktiviert, da kein Schlüssel oder Aktivierungscode hinzugefügt wurde. Der Status ist rot hervorgehoben.

- **Die Lizenz ist abgelaufen!** – Kaspersky Embedded Systems Security 2.2 ist nicht aktiviert, da die Lizenz abgelaufen ist. Der Status ist rot hervorgehoben.
- **Verstoß gegen den Endbenutzer-Lizenzvertrag** – Kaspersky Embedded Systems Security 2.2 ist nicht aktiviert, da die Bedingungen des Endbenutzer-Lizenzvertrags verletzt wurden (siehe Abschnitt "Über den Endbenutzer-Lizenzvertrag" auf S. 70). Der Status ist rot hervorgehoben.
- **Der Schlüssel wurde auf die schwarze Liste gesetzt** – die hinzugefügte Schlüsseldatei 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 die Informationen über die aktuelle Lizenz einzusehen,*

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 15. Allgemeine Lizenzinformationen im Knoten Lizenzverwaltung

Feld	Beschreibung
Aktivierungscode	Nummer des Aktivierungscodes. Dieses Feld wird ausgefüllt, wenn Sie das Programm mithilfe eines Aktivierungscodes aktivieren.
Aktivierungsstatus	Informationen über den Aktivierungsstatus des Programms. Die Informationen in der Spalte Aktivierungsstatus in der Steuerleiste des Knotens Lizenzverwaltung können die folgenden Werte aufweisen: • **Übernommen** – wenn Sie das Programm mithilfe eines Aktivierungscodes oder eines Schlüssels aktiviert haben. • **Aktivierung** – wenn Sie einen Aktivierungscode für die Aktivierung des Programms verwendet haben und der Aktivierungsprozess noch nicht abgeschlossen ist. Der Status nimmt den Wert Übernommen nach Abschluss der Programmaktivierung und nach dem Update des Inhalts im Ergebnisbereich des Knotens an. • **Fehler beim Aktivieren** – wenn das Programm nicht aktiviert werden konnte. Die Ursache für das Fehlschlagen der Aktivierung finden Sie im Protokoll über Ausgabenausführung.
Schlüssel	Nummer des Schlüssels, mit dessen Hilfe Sie das Programm aktiviert haben.
Lizenztyp	Lizenztyp: kommerziell.
Gültig bis	Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Status des Aktivierungscodes oder Schlüssels	Status des Aktivierungscodes oder des Schlüssels: aktiver oder Reserveschlüssel.

► *Um Details über die Lizenz einzusehen.*

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 2.2 gekauft haben (siehe Tabelle unten).

Tabelle 16. Ausführliche Lizenzinformationen im Fenster Eigenschaften: <Status des Aktivierungscodes bzw. Schlüssels>

Feld	Beschreibung
Registerkarte Allgemein	
Schlüssel	Nummer des Schlüssels, mit dessen Hilfe Sie das Programm aktiviert haben.
Schlüssel hinzugefügt am	Datum, an dem der Schlüssel zum Programm hinzugefügt wurde.
Lizenztyp	Lizenztyp: kommerziell.
Läuft ab in (Tagen)	Anzahl der Tage bis zum Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Gültig bis	Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz. Wenn Sie das Programm auf Basis eines unbefristeten Abonnements aktivieren, wird der Feldwert *Unbefristet* angezeigt. Wenn Kaspersky Embedded Systems Security 2.2 das Ablaufdatum der Lizenz nicht ermitteln kann, wird der Wert *Unbekannt* angezeigt.
Programm	Programmname, für den der Schlüssel oder der Aktivierungscode hinzugefügt wurde.
Nutzungsbeschränkung für Schlüssel	Vorgesehene Beschränkungen für die Verwendung des Schlüssels (sofern vorhanden).
Verfügbarkeit des Technischen Supports	Informationen darüber, ob Kaspersky Lab oder ein Partner dem Kunden nach den Lizenzbedingungen technischen Support leisten.
Registerkarte Erweitert	
Lizenzinformationen	Nummer und Typ der aktiven Lizenz.
Support-Informationen	Kontaktinformationen von Kaspersky Lab oder von dem Partner, der für den technischen Support verantwortlich ist. Dieses Feld kann leer sein, wenn kein technischer Support geleistet wird.
Informationen zum Benutzer	Informationen zum Käufer der Lizenz: Name des Auftraggebers und Name des Unternehmens, für das die Lizenz erworben wurde.

Funktionsbeschränkungen nach Ablauf der Lizenz

Wenn die aktive Lizenz abläuft, werden die Funktionskomponenten wie folgt in ihrer Ausführung eingeschränkt:

- Alle Aufgaben mit Ausnahme von Echtzeitschutz für Dateien, Untersuchung auf Befehl und Integritätsprüfung für Programme werden gestoppt
- Der Start aller Aufgaben mit Ausnahme von Echtzeitschutz, Untersuchung auf Befehl und Integritätsprüfung für Programme wird verboten 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 (Speicher, Berichte, Diagnoseinformationen) stehen weiterhin zur Verfügung.

Verlängerung der Lizenz

Standardmäßig werden Sie 14 Tage vor dem Ablaufdatum der Lizenzgültigkeit von Kaspersky Embedded Systems Security 2.2 über den baldigen Ablauf der Lizenz benachrichtigt. Dabei wird der Status **Gültigkeitsdauer der Lizenz** im Ergebnisbereich des **Kaspersky Embedded Systems Security** Hauptknotens gelb hervorgehoben.

Sie können die Gültigkeitsdauer der Lizenz schon vor deren Ablauf verlängern, indem Sie einen zusätzlichen Aktivierungscode oder einen Reserveschlüssel hinzufügen. So vermeiden Sie, dass der Server 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 bzw. der Aktivierungscode wird hinzugefügt, und nach Ablauf des aktiven Schlüssels bzw. Aktivierungscodes für Kaspersky Embedded Systems Security 2.2 automatisch aktiviert.

Schlüssel löschen

Sie können den hinzugefügten Schlüssel entfernen.

Wenn in Kaspersky Embedded Systems Security 2.2 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.

Starten und Beenden des Plug-in für Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt enthält Informationen zum Start und Stoppen des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security 2.2 sowie von Kaspersky Security Service.

In diesem Kapitel

Plug-in für Kaspersky Embedded Systems Security 2.2 starten

In Kaspersky Security Center sind für den Start des Plug-in für Kaspersky Embedded Systems Security 2.2 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*.

Kaspersky Security Service starten und anhalten

Standardmäßig wird der Dienst von Kaspersky Security Service beim Hochfahren des Betriebssystems automatisch gestartet. Kaspersky Security Service verwaltet die Programmprozesse, bei denen die Aufgaben zum Echtzeitschutz des Computers, zur Überwachung der Computer-Aktivitäten, zur Untersuchung auf Befehl und zum Update ausgeführt werden.

Beim Start von Kaspersky Embedded Systems Security 2.2 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 2.2 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 **Kaspersky Embedded Systems Security** Hauptknotens.
2. Wählen Sie einen der folgenden Befehle:
   - **Dienst beenden**
   - **Dienst starten**

Der Dienst von Kaspersky Security Service wird gestartet oder beendet.

Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt enthält Informationen über die Rechte zur Verwaltung von Kaspersky Embedded Systems Security 2.2 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 2.2

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 2.2 erstellt wird, sowie die Gruppe "SYSTEM" Zugriff auf alle Funktionen von Kaspersky Embedded Systems Security 2.2.

Benutzer, die Zugriff auf die Funktionen Rechte **ändern** von Kaspersky Embedded Systems Security 2.2 haben, können auch anderen Benutzern, die am geschützten Computer registriert sind oder zur Domäne gehören, den Zugriff auf Funktionen von Kaspersky Embedded Systems Security 2.2 gewähren.

Wenn ein Benutzer nicht in die Liste der Benutzer von Kaspersky Embedded Systems Security 2.2 registriert ist, kann er die Programmkonsole nicht öffnen.

Sie können für einen Benutzer oder eine Benutzergruppe eine der folgenden vordefinierten Stufen für den Zugriff auf die Funktionen von Kaspersky Embedded Systems Security 2.2 auswählen:

- **Vollständige Kontrolle** – Zugriff auf alle Programmfunktionen: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Embedded Systems Security 2.2, der Komponenteneinstellungen, der Rechte von Benutzern von Kaspersky Embedded Systems Security 2.2, sowie Anzeigen der Statistik für Kaspersky Embedded Systems Security 2.2.
- **Ändern** – Zugang zu allen Programmfunktionen mit Ausnahme der Veränderung der Benutzerrechte: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Embedded Systems Security 2.2 und der Einstellungen der Komponenten von Kaspersky Embedded Systems Security 2.2.
- **Lesen** – Anzeigen der allgemeinen Einstellungen von Kaspersky Embedded Systems Security 2.2, der Einstellungen der Komponenten von Kaspersky Embedded Systems Security 2.2, der Statistik für Kaspersky Embedded Systems Security 2.2 und der Benutzerrechte für Kaspersky Embedded Systems Security 2.2.

Sie können auch die erweiterten Zugriffsrechte konfigurieren (siehe Abschnitt "Konfiguration der Zugriffsrechte für Kaspersky Embedded Systems Security 2.2 und Kaspersky Security Service" auf Seite 87): Zugriff auf bestimmte Funktionen von Kaspersky Embedded Systems Security 2.2 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 17. Über Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2

Zugriffsrechte	Beschreibung
Aufgabenverwaltung	Berechtigung zum Starten, Beenden, Anhalten bzw. Fortsetzen der Aufgaben von Kaspersky Embedded Systems Security 2.2.
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 2.2 aus einer Konfigurationsdatei importieren • Programmeinstellungen bearbeiten
Lesen von Parametern	Berechtigungen: • Allgemeine Einstellungen und Aufgabeneinstellungen für Kaspersky Embedded Systems Security 2.2 anzeigen. • Exportieren der Einstellungen von Kaspersky Embedded Systems Security 2.2 in eine Konfigurationsdatei. • Einstellungen für Protokollen über Aufgabenausführung, für das Systemaudit-Protokoll und für Benachrichtigungen anzeigen.
Verwalten von Speichern	Berechtigungen: • Objekte in Quarantäne verschieben • Objekte aus der Quarantäne und dem Backup löschen • Objekte aus der Quarantäne und dem Backup wiederherstellen
Verwaltung von Protokollen	Berechtigung zum Löschen von Protokollen über Aufgabenausführung und zum Leeren des Systemaudit-Protokolls
Lesen von Protokollen	Berechtigung zur Anzeige der Ereignisse von Anti-Virus in Protokollen über Aufgabenausführung und im Systemaudit-Protokoll.
Lesen der Statistik	Berechtigung zum Anzeigen der Statistik für die einzelnen Aufgaben von Kaspersky Embedded Systems Security 2.2.
Lizenzverwaltung für das Programm	Kaspersky Embedded Systems Security 2.2 kann aktiviert oder deaktiviert werden.
Programm entfernen	Berechtigung zum Deinstallieren von Kaspersky Embedded Systems Security 2.2.
Lesen von Benutzerrechten	Berechtigung zum Anzeigen der Benutzerlisten von Kaspersky Embedded Systems Security 2.2 und der Zugriffsrechte der einzelnen Benutzer
Ändern von Rechten	Berechtigungen: • Liste der Benutzer ändern, die Zugriff auf die Programmverwaltung haben • Benutzerzugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2 bearbeiten

Über die Rechte zur Verwaltung des Dienstes Kaspersky Security Service

Bei der Installation registriert Kaspersky Embedded Systems Security 2.2 in Windows den Dienst von Kaspersky Security Service (KAVFS), da dieser die Komponenten beinhaltet, die beim Hochfahren des Betriebssystems gestartet werden. Um die Gefahr des Zugriffs Unbefugter auf die Programmfunktionen und Sicherheitseinstellungen auf dem 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 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.

Sie können das Benutzerkonto "SYSTEM" weder löschen noch dessen Rechte ändern. Wenn die Rechte des Benutzerkontos "SYSTEM" geändert wurden, werden beim Speichern der Änderungen die maximalen Berechtigungen für dieses Benutzerkonto wiederhergestellt.

Benutzer, die Zugriff auf Funktionen (siehe Abschnitt "Über Rechte zur Verwaltung von Kaspersky Embedded Systems Security 2.2" auf S. 82) der Stufe "Rechte ändern" haben, 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 2.2 eine der folgenden vordefinierten Stufen des Zugriffs 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 2.2 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 18. Differenzierung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2

Funktion	Beschreibung
Einstellungen des Dienstes lesen	Berechtigung zum Aufrufen 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

Funktion	Beschreibung
Status beim Dienst abfragen	Berechtigung zur Abfrage des Ausführungsstatus des Dienstes bei Kaspersky Security Service.
Abhängige Dienste auflisten	Berechtigung zum Aufruf einer Liste der Dienste, von denen Kaspersky Security Service abhängt, sowie der Dienste, die von Kaspersky Security Service abhängen.
Diensteinstellungen konfigurieren	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 zu 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.

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 2.2 installiert und wird für die Registrierung von Kaspersky Security Service als PPL beim Start des Betriebssystems verwendet. Wenn Kaspersky Security Service (kavfs.exe) 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 Benutzerberichten 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 2.2 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 startet alle untergeordneten Prozesse als PPL.

► *Führen Sie folgenden Befehl aus, um Kaspersky Embedded Systems Security 2.2 als PPL zu installieren:*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Mithilfe der Befehlszeile können Sie die PPL-Verwendung konfigurieren.

Über Zugriffsrechte für Kaspersky Security Management Service

Sie können die Liste der Dienste von Kaspersky Embedded Systems Security 2.2 überprüfen.

Während der Installation registriert Kaspersky Embedded Systems Security 2.2 den Dienst Kaspersky Security Management Service (KAVFSGT). 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 2.2 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 2.2 auf dem geschützten Computer 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 2.2 erlauben oder verweigern.

Sie können unter dem lokalen Benutzerkonto eine Verbindung mit Kaspersky Embedded Systems Security 2.2 herstellen, wenn auf dem geschützten Computer das Benutzerkonto mit dem gleichen Namen und dem gleichen Kennwort registriert ist.

Konfiguration der Zugriffsrechte für Kaspersky Embedded Systems Security 2.2 und Kaspersky Security Service

Sie können die Liste der Benutzer und Benutzergruppen ändern, denen der Zugriff auf die Funktionen von Kaspersky Embedded Systems Security 2.2 und die Verwaltung von Kaspersky Security Service erlaubt ist, sowie 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 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen aus:
   - Wählen Sie **Benutzerrechte für die Programmverwaltung** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security 2.2 haben.
   - Wählen Sie den Punkt **Benutzerrechte für die Verwaltung von Security Service** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung von Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security 2.2** wird geöffnet.
4. Im sich öffnenden Fenster gehen Sie wie folgt vor:
   - Um einen Benutzer oder eine Gruppe zur Benutzerliste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie den Benutzer oder die Gruppe aus, dem bzw. der Sie die Rechte zuweisen möchten.
   - Wählen Sie den Benutzer oder die Gruppe aus, für die Sie den Zugriff beschränken möchten, und klicken Sie auf **Löschen**, um einen Benutzer oder eine Gruppe aus der Liste zu löschen.
5. 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 2.2 oder von Kaspersky Security Service zu ändern:*

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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen aus:
   - Wählen Sie **Benutzerrechte für die Programmverwaltung ändern** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security 2.2 haben.
   - Wählen Sie den Punkt **Benutzerrechte für die Verwaltung von Kaspersky Security Service ändern** aus, 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.
4. Wählen Sie im folgenden Fenster in der Liste **Gruppen** oder Benutzer den Benutzer oder die Benutzergruppe aus, dessen bzw. deren Rechte Sie ändern möchten.
5. Aktivieren Sie im Block **Berechtigungen für die Gruppe "<Benutzer (Gruppe)>"** die Kontrollkästchen **Erlauben** oder **Blockieren** für die folgenden Zugriffsstufen:
   - **Vollständige Kontrolle**: Uneingeschränkte Rechte zur Verwaltung von Kaspersky Embedded Systems Security 2.2 oder Kaspersky Security Service.
   - **Lesen**:
     - Folgende Rechte für die Verwaltung von Kaspersky Embedded Systems Security 2.2: **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 2.2 mit Ausnahme von **Rechte ändern**.
  - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Diensteinstellungen konfigurieren**, **Rechte lesen**.
- **Ausführung**: Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Dienst starten**, **Dienst beenden**, **Dienst anhalten/fortsetzen**, **Rechte lesen**, **Benutzeranfragen an den Dienst**.

6. Wenn Sie erweiterte Einstellungen der Rechte für einen Benutzer oder eine Gruppe vornehmen möchten (**Sonderrechte**), klicken Sie auf **Erweitert**.
   a. Wählen Sie im folgenden Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Embedded Systems Security 2.2** den jeweiligen Benutzer oder die jeweilige Gruppe aus.
   b. Klicken Sie auf **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 2.2** auf **OK**.
7. Klicken Sie im Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** auf die Schaltfläche **Übernehmen**.

Die konfigurierten Rechte für die Verwaltung von Kaspersky Embedded Systems Security 2.2 oder Kaspersky Security Service werden gespeichert.

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security 2.2

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste mithilfe der Einstellungen der Rechte der Benutzer (siehe Abschnitt "Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2" auf Seite 82) beschränken. Außerdem können Sie den Zugriff auf die Ausführung kritischer Vorgänge zusätzlich schützen, indem Sie in den Einstellungen von Kaspersky Embedded Systems Security 2.2 einen Kennwortschutz einrichten.

Kaspersky Embedded Systems Security 2.2 verlangt die Eingabe eines Kennworts beim Zugriff auf die folgenden Programmfunktionen:

- Verbindung mit der Programmkonsole;
- Deinstallation von Kaspersky Embedded Systems Security 2.2
- Änderung der Einstellungen von Kaspersky Embedded Systems Security 2.2;
- Ausführung der Befehle der Befehlszeile.

In der Benutzeroberfläche von Kaspersky Embedded Systems Security 2.2 wird das angegebene Kennwort auf dem Bildschirm verborgen. Kaspersky Embedded Systems Security 2.2 speichert das eingegebene Kennwort in Form einer Prüfsumme, die bei der Erstellung des Kennworts berechnet wird.

Sie können die Einstellungen des kennwortgeschützten Programms exportieren und importieren. Die Konfigurationsdatei, die beim Export der Einstellungen des geschützten Programms erstellt wird, enthält den Wert der Prüfsumme des Kennworts und den Wert des Modifikators, der zur Verlängerung der Kennwortzeile verwendet wird.

Ändern Sie den Wert der Prüfsumme oder des Modifikators in der Konfigurationsdatei nicht. Der Import von manuell geänderten kennwortgeschützten Einstellungen kann zur vollständigen Sperrung des Zugriffs auf die Programmverwaltung führen.

► *Um den Zugriff auf die Funktionen von Kaspersky Embedded Systems Security 2.2 zu schützen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen konfigurieren möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Richtlinieneinstellungen für eine Gruppe von Computern anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie **<Name der Richtlinie> > Eigenschaften**.
   - Um die Programmeinstellungen für einen einzelnen Computer anzupassen, öffnen Sie die gewünschten Einstellungen in den **Programmeinstellungen** (siehe Abschnitt "**Konfiguration von lokalen Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center**" auf S. 107) im Kaspersky Security Center-Fenster.
3. Klicken Sie im Block **Sicherheit** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Sicherheitseinstellungen** wird geöffnet.
4. Aktivieren Sie im Block **Einstellungen für den Kennwortschutz** das Kontrollkästchen **Kennwortschutz verwenden**.

   Die Felder **Kennwort** und **Kennwort bestätigen** werden aktiv.
5. Geben Sie im Feld **Kennwort** den Wert ein, den Sie für den Schutz des Zugriffes auf die Funktionen von Kaspersky Embedded Systems Security 2.2 verwenden möchten.
6. Geben Sie im Feld **Kennwort bestätigen** das Kennwort erneut ein.
7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert. Kaspersky Embedded Systems Security 2.2 fragt das festgelegte Kennwort beim Zugriff auf die geschützten Funktionen ab.

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 festgelegte Kennwort jederzeit in den Einstellungen des Programms ändern oder verwerfen.

► *Um das festgelegte Kennwort zurückzusetzen,*

deaktivieren Sie das Kontrollkästchen **Kennwortschutz verwenden** in den Richtlinien- oder Programmeinstellungen.

Der Kennwortschutz wird deaktiviert. Kaspersky Embedded Systems Security 2.2 löscht die Prüfsumme des alten Kennworts aus den Programmeinstellungen.

Netzwerkverbindungen für den Dienst Kaspersky Security Management Service erlauben

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

► *Um Netzwerkverbindungen für den Dienst von Kaspersky Security Management Service auf dem geschützten Computer zu erlauben, gehen Sie wie folgt vor:*

1. Wählen Sie auf einem geschützten Computer unter Microsoft Windows den Punkt **Start > Systemsteuerung > Sicherheit > Windows-Firewall**.
2. Wählen Sie im Fenster **Einstellungen für Windows-Firewall** den Punkt **Einstellungen ändern** aus.
3. Aktivieren Sie auf der Registerkarte **Ausnahmen** in der Liste mit vordefinierten Ausnahmen die Kontrollkästchen **COM + Netzwerkzugriff, Windows Management Instrumentation (WMI)** und **Remote Administration**.
4. Klicken Sie auf die Schaltfläche **Programm hinzufügen**.
5. Wählen Sie im Fenster **Programm hinzufügen** die Datei kavfsgt.exe aus. Diese Datei befindet sich im Ordner, den Sie bei der Installation der Programmkonsole als Zielordner angegeben haben.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Einstellungen für Windows-Firewall** auf die Schaltfläche **OK**.

Netzwerkverbindungen für Kaspersky Security Management Service auf dem geschützten Computer erlauben.

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 2.2 auf mehreren Computern.

In diesem Kapitel

Über Richtlinien

Sie können in Kaspersky Security Center einheitliche Richtlinien erstellen, um den Schutz auf mehreren Computern zu verwalten, auf denen Kaspersky Embedded Systems Security 2.2 installiert ist.

Eine Richtlinie übernimmt die in ihr eingetragenen Einstellungen, Funktionen und Aufgaben für Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 Echtzeitschutz 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.

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 Einstellungen für Aufgaben zum Echtzeitschutz des Computers anpassen.
2. Anpassung der Richtlinieneinstellungen. Im Fenster **Eigenschaften: <Name der Richtlinie>** der erstellten Richtlinie können Sie die Aufgabeneinstellungen zum Echtzeitschutz des Computers, die allgemeinen Einstellungen für Kaspersky Embedded Systems Security 2.2, die Quarantäne- und Backup-Einstellungen, die Genauigkeitsstufe für Berichte über Aufgabenausführung sowie Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Embedded Systems Security 2.2 definieren.

► *Gehen Sie folgendermaßen vor, um eine Richtlinie für eine Gruppe von Computern zu erstellen, auf denen Kaspersky Embedded Systems Security 2.2 installiert ist:*

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

   Daraufhin wird das Fenster **Assistent für neue Richtlinien**geöffnet.
3. Wählen Sie im Fenster **Wählen Sie die Gruppe aus, für die Sie eine Richtlinie erstellen möchten** Kaspersky Embedded Systems Security 2.2 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. Um eine für die vorherige Programmversion verwendete Richtlinienkonfiguration zu übernehmen, gehen Sie wie folgt vor:
   a. Aktivieren Sie das Kontrollkästchen **Einstellungen aus Richtlinie für vorherige Programmversion verwenden**.
   b. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie die Richtlinie, die Sie übernehmen möchten.
   c. Klicken Sie auf **Weiter**.
6. Wählen Sie im Fenster **Vorgangsart auswählen** eine der folgenden Optionen aus:
   - **Neu**, um eine neue Richtlinie mit den Standardeinstellungen zu erstellen.
   - **Richtlinie importieren, die mit früheren Versionen 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 **Echtzeitschutz des Computers** bei Bedarf die Einstellungen der Aufgaben Echtzeitschutz für Dateien und die Verwendung von KSN und Exploit-Prävention Ihren Bedürfnissen entsprechend 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 die Standardeinstellungen von Aufgaben für den Echtzeitschutz des Computers.

   - Wenn Sie die standardmäßig festgelegten Einstellungen der Aufgabe Echtzeitschutz für Dateien ändern möchten, klicken Sie im Abschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**. Passen Sie im nächsten 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 Abschnitt **Verwendung von KSN**. Passen Sie im nächsten 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 "Konfiguration der Datenverarbeitung" auf Seite 181).

   - Wenn Sie die Standardeinstellungen der Komponente "Exploit-Prävention" ändern möchten, klicken Sie auf die Schaltfläche **Einstellungen** im Block **Exploit-Prävention**. Passen Sie im nächsten Fenster die Funktionen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.

8. Wählen Sie im Fenster **Gruppenrichtlinie für das Programm 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, wird sie deaktiviert und eine neue Richtlinie wird 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. Im Fenster **Beenden** klicken Sie auf die Schaltfläche **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 2.2 anpassen.

Richtlinie anpassen

Im Fenster **Eigenschaften: <Name der Richtlinie>** einer vorhandenen Richtlinie können Sie folgende Einstellungen anpassen: allgemeine Einstellungen von Kaspersky Embedded Systems Security 2.2, Einstellungen für Quarantäne und Backup-Einstellungen, Einstellungen für die vertrauenswürdige Zone, Einstellungen für den Echtzeitschutz, Überwachung der Server-Aktivitäten, Genauigkeitsstufe für Protokollen über Aufgabenausführung, Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Embedded Systems Security 2.2, 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 den untergeordneten Knoten **Richtlinien** im Ergebnisfenster.
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 Block **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 nicht möchten, dass die Richtlinie auf allen Computern übernommen wird, die zur ausgewählten Gruppe gehören.

   Die Einstellung **Out-Of-Office Richtlinie** ist bei der Verwendung von Kaspersky Embedded Systems Security 2.2 nicht verfügbar.
5. Konfigurieren Sie in den Abschnitten **Benachrichtigung über Ereignisse**, **Programmeinstellungen**, **Protokolle und Benachrichtigungen**, **Zusätzlich** und **Revisionsverlauf** die allgemeinen Einstellungen der Programmausführung (s. Tabelle unten).
6. Konfigurieren Sie in den Abschnitten **Echtzeit-Computerschutz**, **Überwachung der Server-Aktivitäten**, **Netzwerküberwachung** und **System-Diagnose** die Einstellungen für die Ausführung der Aufgaben des Programms sowie die Einstellungen für deren Start (s. 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.

Eine Anleitung für die Konfiguration der Aufgaben und Programmfunktionen in der Programmkonsole finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

Abschnitte mit Richtlinieneinstellungen für Kaspersky Embedded Systems Security 2.2

Allgemein

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

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

Ereignisbenachrichtigungen

Im Abschnitt **Ereignisbenachrichtigungen** können Sie die Einstellungen für die folgenden Ereigniskategorien konfigurieren:

- *Kritische Ereignisse*
- *Funktionsfehler*
- *Warnung*
- *Infomeldung*

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 19. Einstellungen des Abschnitts "Programmeinstellungen"

Abschnitt	Einstellungen
Skalierbarkeit und Oberfläche	Im Abschnitt **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 Abschnitt **Sicherheit und Zuverlässigkeit** 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 Abschnitt **Verbindungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Proxyserver-Einstellungen für die Verbindung mit den Update-Computern, den Aktivierungsservern und KSN konfigurieren: • Festlegung der Proxyserver-Einstellungen • Geben Sie die Einstellungen für die Authentifizierung auf dem Proxyserver an.

Abschnitt	Einstellungen
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 20. Einstellungen des Abschnitts "Zusätzlich"

Abschnitt	Einstellungen
Vertrauenswürdige Zone	Im Abschnitt **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	Klicken Sie auf die Schaltfläche **Einstellungen**, um die Untersuchungseinstellungen für USB-Wechseldatenträger anzupassen.
Benutzerrechte für die Programmverwaltung	In diesem Abschnitt können Sie Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Embedded Systems Security 2.2 anpassen.
Benutzerrechte für die Verwaltung von Security Service	In diesem Abschnitt können Sie 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 und Backup 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 Übermittlung von Informationen über im Backup und in der Quarantäne gespeicherte Objekte an den Administrationsserver

Echtzeitschutz des Computers

Tabelle 21. Einstellungen des Abschnitts "Echtzeitschutz des Computers"

Abschnitt	Einstellungen
Echtzeitschutz für Dateien	Im Abschnitt **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 des Aufgabenstarts anpassen
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 • Datenübertragung und Verwendung von Kaspersky Security Center als KSN-Proxyserver anpassen Klicken Sie auf die Schaltfläche **Datenverarbeitung**, um die KSN-Erklärung zu akzeptieren oder abzulehnen und die Einstellungen für den zuverlässigen Datenaustausch anzupassen.
Exploit-Prävention	Im Abschnitt **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 Server-Aktivitäten

Tabelle 22. Einstellungen des Blocks "Überwachung der Server-Aktivitäten"

Abschnitt	Einstellungen
Kontrolle des Programmstarts	Im Abschnitt **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 des Aufgabenstarts anpassen
Gerätekontrolle	Im Abschnitt **Gerätekontrolle** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Funktionsmodus der Aufgabe auswählen • Einstellungen für den Aufgabenstart festlegen

Netzwerküberwachung

Tabelle 23. Einstellungen des Blocks "Netzwerküberwachung"

Abschnitt	Einstellungen
Firewall-Verwaltung	Im Abschnitt **Firewall-Verwaltung** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Firewall-Regeln anpassen • Einstellungen des Aufgabenstarts anpassen

System-Diagnose

Tabelle 24. Einstellungen des Abschnitts "System-Diagnose"

Abschnitt	Einstellungen
Überwachung der Datei-Integrität	Im Abschnitt **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 25. Einstellungen des Abschnitts "Protokolle und Benachrichtigungen"

Abschnitt	Einstellungen
Protokolle über Aufgabenausführung	Im Abschnitt **Protokollen über Aufgabenausführung** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Ereigniskategorie protokollierter Ereignisse für die ausgewählten Programmkomponenten angeben • Speicherdauer für Protokollen über Aufgabenausführung festlegen • Konfiguration der SIEM-Integration in Kaspersky Security Center.
Ereignisbenachrichtigungen	Im Abschnitt **Ereignisbenachrichtigungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Benachrichtigung der Benutzer über das Ereignis *Objekt gefunden* • Benachrichtigung des Administrators über ein beliebiges ausgewähltes Ereignis aus der Liste der Ereignisse im Block **Benachrichtigungen anpassen**
Interaktion mit dem Administrationsserver	Im Block **Interaktion mit dem Administrationsserver** können Sie über die Schaltfläche **Einstellungen** die Typen der Objekte auswählen, über die Kaspersky Embedded Systems Security 2.2 Informationen an den Administrationsserver übergeben soll.

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.

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 einem lokal auf jedem Computer der Administrationsgruppe festgelegten 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 2.2 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:

- Aufgabe zur Untersuchung auf Befehl: Untersuchung wichtiger Bereiche, Untersuchung von Quarantäne-Objekten, Untersuchung beim Hochfahren des Betriebssystems, Integritätsprüfung für Programm-Module
- 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 2.2 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 2.2 auf der Computergruppe konfigurieren möchten, den Befehl **Eigenschaften**.
3. Öffnen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Programmeinstellungen**. Klicken Sie im Block **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 (siehe Abschnitt "Über Richtlinien" auf Seite 92), die Sie anpassen, aktiv ist und für die ausgewählte Computergruppe übernommen wurde.
5. Klicken Sie auf **OK**.

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

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Embedded Systems Security 2.2, 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 Erlaubnisregeln
- 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 Block **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 100) 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

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *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 Ergebnisbereich auf der Registerkarte **Geräte** das Kontextmenü des geschützten Computers und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im erscheinenden Fenster im Abschnitt **Aufgaben** auf **Hinzufügen**.
   - Für das Erstellen einer Gruppenaufgabe:
     a. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, für die Sie eine Aufgabe erstellen möchten.
     b. Öffnen Sie im Ergebnisbereich die Registerkarte **Aufgaben** und wählen Sie **Aufgabe erstellen**.
   - Um eine Aufgabe für eine beliebige Auswahl an Computern zu erstellen, öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center den Knoten **Geräteauswahl** und wählen Sie den Punkt **Aufgabe erstellen** aus.

   Darauf öffnet sich der Assistent für neue Aufgaben.

2. Wählen Sie im Fenster **Aufgabentyp** unter der Überschrift **Kaspersky Embedded Systems Security 2.2** den Typ der zu erstellenden Aufgabe aus.
3. Wenn Sie einen anderen Aufgabentyp als Rollback des Datenbanken-Updates oder Programmaktivierung ausgewählt haben, wird das Fenster **Einstellungen** geöffnet. Je nach Typ der zu erstellenden Aufgabe führen Sie eine der folgenden Aktionen aus:

   - *Wenn Sie eine Aufgabe zur Untersuchung auf Befehl erstellen*:

     a. Erstellen Sie im Fenster **Untersuchungsbereich** einen Untersuchungsbereich:

     Standardmäßig gehören zum Untersuchungsbereich wichtige Bereiche des Computers. Untersuchungsbereiche sind in der Tabelle mit dem Symbol ☑ gekennzeichnet.

     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 vordefinierte Bereiche, Festplatten, Ordner, Netzwerkobjekte oder Dateien zum Untersuchungsbereich hinzuzufügen, klicken Sie mit der rechten Maustaste auf die Tabelle **Untersuchungsbereich** und wählen Sie Bereich hinzufügen. 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 untergeordnete Ordner oder Dateien von der Untersuchung auszuschließen, wählen Sie den hinzugefügten Ordner (die hinzugefügte Festplatte) im Fenster **Untersuchungsbereich** des Assistenten aus, öffnen Sie das Kontextmenü und wählen Sie die Option **Anpassen**. Klicken Sie dann im Fenster Sicherheitsstufe auf **Einstellungen** und deaktivieren Sie im Fenster **Untersuchung auf Befehl anpassen** auf der Registerkarte **Allgemein** die Kontrollkästchen **Untergeordnete Ordner** und **Untergeordnete Dateien**.
     - Um die Sicherheitseinstellungen für den Untersuchungsbereich zu ändern, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Bereich, dessen Parameter Sie ändern wollen, und wählen Sie **Anpassen**. Wählen Sie im Fenster **Untersuchung auf Befehl anpassen** eine der vordefinierten Sicherheitsstufen aus oder klicken Sie auf die Schaltfläche **Einstellungen**, um die Sicherheitseinstellungen manuell anzupassen. Das Anpassen der Sicherheitseinstellungen wird genauso wie in der Konsole für Kaspersky Embedded Systems Security 2.2 durchgeführt.
     - Um eingebettete Objekte aus einem hinzugefügten Untersuchungsbereich auszuschließen, öffnen Sie das Kontextmenü in der Tabelle **Untersuchungsbereich**, klicken Sie auf **Ausnahme hinzufügen** und geben Sie die auszuschließenden Objekte an: Wählen Sie in der Liste Vordefinierter Bereich einen vordefinierten Bereich aus, geben Sie einen Datenträger des Computers, einen Ordner oder eine Datei auf einem geschützten Computer oder auf einem anderen Computer im Netzwerk an. Klicken Sie dann auf **OK**.
     - Bereiche, die vom Untersuchungsbereich ausgenommen sind, werden in der Tabelle mit dem Symbol ☐ markiert.

     b. Gehen Sie im Fenster **Einstellungen** wie folgt vor.

     Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie Objekte, die in der vertrauenswürdigen Zone von Kaspersky Embedded Systems Security 2.2 beschrieben werden, vom Untersuchungsbereich der Aufgabe ausschließen wollen.

Wenn Sie planen, die zu erstellende Aufgabe als Untersuchung wichtiger Bereiche zu verwenden, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**. Das Programm Kaspersky Security Center berücksichtigt bei der Bewertung des Sicherheitsstatus des Computers (bzw. der Computer) die Ergebnisse der Ausführung von Aufgaben mit dem Status *Aufgabe zur Untersuchung wichtiger Bereiche*, und nicht nur die Ergebnisse der Systemaufgabe **Untersuchung wichtiger Bereiche**. Bei der Erstellung einer lokalen Aufgabe zur Untersuchung auf Befehl ist das Kontrollkästchen nicht verfügbar.

Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Basispriorität **Niedrig** zuzuweisen, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**. Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security 2.2 ausgeführt werden, haben standardmäßig die Priorität **Mittel** (Normal). Wenn die Priorität eines Prozesses gesenkt wird, erhöht sich dadurch die Ausführungsdauer der Aufgabe und die Ausführungsgeschwindigkeit der Prozesse anderer aktiver Anwendungen wird gesteigert.

- *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-Computers 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 2.2 den Computer nach Abschluss der Aufgabe automatisch neu startet, aktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**. Um den Neustart des Computers nach Abschluss der Aufgabe zu verhindern, deaktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**.

  c. Wenn Sie Informationen über Upgrades der Module von Kaspersky Embedded Systems Security 2.2 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.

- *Wenn Sie die Aufgabe Update-Verteilung erstellen*, geben Sie im Fenster **Einstellungen für die Update-Verteilung** die Zusammensetzung der Updates und den Ordner der lokalen Update-Quelle an, in der das Update gespeichert wird.
- *Wenn Sie die Aufgabe Programmaktivierung erstellen*, verwenden Sie im Fenster **Aktivierungsparameter** die Schlüsseldatei, mit deren Hilfe Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie eine Aufgabe zur Verlängerung der Lizenz erstellen möchten.
- *Wenn Sie die Aufgabe "Automatisches Erstellen von Erlaubnisregeln" oder die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen*, geben Sie im Fenster **Einstellungen** die Parameter an, auf deren Grundlage die Liste der Erlaubnisregeln erstellt wird:
  a. Geben Sie das Präfix für die Namen der Regeln an (nur für die Aufgabe "Automatisches Erstellen von Erlaubnisregeln").
  b. Passen Sie die Einstellungen des Gültigkeitsbereichs der Erlaubnisregeln mit dem Status "erlaubt" (nur für die Aufgabe "Automatisches Erstellen von Erlaubnisregeln") an. Klicken Sie auf **Weiter**.
  c. Legen Sie die Aktionen fest, die die Aufgabe während der Erstellung von Erlaubnisregeln (nur für die Aufgabe "Automatisches Erstellen von Erlaubnisregeln") und nach ihrem Abschluss ausführen soll.

4. Passen Sie die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen). Gehen Sie im Fenster **Zeitplan** wie folgt vor:
   a. Um den Zeitplan zu aktivieren, aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.
   b. Legen Sie eine Frequenz für den Aufgabenstart fest: Wählen Sie in der Liste **Startintervall** einen der folgenden Werte aus: **Alle n Stunden**, **Alle n Tage**, **Wöchentlich**, **Bei Programmstart**, **Nach dem Update der Programm-Datenbanken** (in den Gruppenaufgaben "Update der Programm-Datenbanken", "Update der Programm-Module" können Sie zusätzlich die Frequenz **Nach Update-Download durch den Administrationsserver** angeben):
      - Wenn Sie **Alle n Stunden** gewählt haben, geben Sie in der Optionsgruppe **Einstellungen für den Aufgabenstart** im Feld Alle **<Anzahl> Stunde(n)** die Anzahl der Stunden an.
      - Wenn Sie **Alle n Tage** gewählt haben, geben Sie in der Optionsgruppe **Einstellungen für den Aufgabenstart** im Feld Alle **<Anzahl> Tag(e)** die Anzahl der Tage an.
      - Wenn Sie **Wöchentlich** gewählt haben, geben Sie in der Optionsgruppe **Einstellungen für den Aufgabenstart** im Feld **Alle <Anzahl> Woche(n)** die Anzahl der Wochen an. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet wird (standardmäßig wird eine Aufgabe montags gestartet).
   c. Geben Sie im Feld **Startzeit** die Startzeit der Aufgabe ein, und geben Sie im Feld **Beginnen am** das Datum, an dem der Zeitplan in Kraft tritt.

d. Geben Sie, falls erforderlich, weitere Zeitplaneinstellungen an: Klicken Sie auf **Erweitert** und gehen Sie im Fenster **Erweiterte Zeitplan-Einstellungen** wie folgt vor:

- Legen Sie eine maximale Dauer für die Aufgabenausführung fest: Geben Sie in der Optionsgruppe **Einstellungen für das Anhalten der Aufgabe** im Feld **Dauer** die Anzahl der Stunden und Minuten an.
- Legen Sie fest, für welchen Zeitraum die Aufgabe im Verlauf von 24 Stunden angehalten werden soll: Geben Sie in der Optionsgruppe **Einstellungen für das Anhalten der Aufgabe** in den Feldern **Anhalten von** und **bis** den Start- und Endpunkt des Zeitraums an.
- Legen Sie ein Datum fest, ab dem der Zeitplan ungültig wird: Aktivieren Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und wählen Sie im Dialogfenster **Kalender** ein Datum aus, ab dem der Zeitplan nicht mehr gelten soll.
- Aktivieren Sie den Start von übersprungenen Aufgaben: Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.
- Aktivieren Sie die Verwendung der Option, mit der der Startzeitpunkt auf ein Intervall verteilt wird: Aktivieren Sie das Kontrollkästchen **Aufgabenstart zufällig wählen innerhalb von** und geben Sie einen Wert in Minuten an.

e. Klicken Sie auf **OK**.

5. Wenn die zu erstellende Aufgabe eine Aufgabe für eine zufällige Zusammenstellung von Computern ist, wählen Sie die Netzwerkcomputer (Gruppen) aus, an denen die Aufgabe ausgeführt werden soll.
6. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, mit dem Sie die Aufgabe ausführen möchten.
7. 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").
8. 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 im Fenster Programmeinstellungen für einen einzelnen Computer im Netzwerk anzupassen, 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 **Einstellungen: <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**.
      - Anschließend wählen Sie den Punkt **Eigenschaften** im Kontextmenü der ausgewählten Aufgabe.
5. Um die Programmeinstellungen anzupassen, gehen Sie wie folgt vor:
   a. Wechseln Sie zum Block **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**.

      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 **Programmeinstellungen** geändert werden.

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

Gruppenaufgaben in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Node **Verwaltete Geräte** 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 **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und 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 Block **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 Reserve-Aktivierungscode oder Reserveschlüssel verwenden**, wenn Sie einen Aktivierungscode oder einen Schlüssel 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 <Name der Aufgabe>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

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

Tabelle 26. Einstellungen für Gruppenaufgaben in Kaspersky Embedded Systems Security 2.2

Aufgabentyp in Kaspersky Embedded Systems Security 2.2	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
Automatisches Erstellen von Regeln (Siehe Aufgabe "Automatisches Erstellen von Erlaubnisregeln" und Aufgabe "Erstellen von Regeln für die Gerätekontrolle" auf Seite 114)	**Einstellungen**	Beim Anpassen der Einstellungen der Aufgabe "Automatisches Erstellen von Erlaubnisregeln" können Sie: • den Schutzbereich ändern, indem Sie Ordnerpfade und Dateitypen hinzufügen oder löschen und Dateitypen angeben, für die der Start durch automatisch erstellte Regeln erlaubt ist. • gestartete Programme berücksichtigen oder nicht berücksichtigen.
	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 2.2 nach Abschluss der Aufgaben erstellt werden.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Aufgabentyp in Kaspersky Embedded Systems Security 2.2	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
Programm aktivieren (siehe Abschnitt "Aufgabe Programm aktivieren" auf Seite 117)	**Aktivierungsparameter**	Sie können für die Programmaktivierung oder für die Verlängerung der Lizenzlaufzeit einen Schlüssel hinzufügen.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Update-Verteilung (siehe Abschnitt "Update-Aufgaben" auf Seite 118)	**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 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 2.2 die kopierten Updates speichern soll.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Aufgabentyp in Kaspersky Embedded Systems Security 2.2	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
Update der Programm-Datenbanken (siehe Abschnitt "Update-Aufgaben" auf Seite 118)	**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 Block 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 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.
	Zeitplan	Sie können die Einstellungen für den Start einer geplanten Aufgabe anpassen.
Update der Programm-Module (siehe Abschnitt "Update-Aufgaben" auf Seite 118)	**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.

Aufgabentyp in Kaspersky Embedded Systems Security 2.2	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
	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 2.2 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 2.2 nach Abschluss der Installation kritischer Updates anpassen.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Untersuchung auf Befehl (siehe Abschnitt "Erstellen einer Aufgabe zur Untersuchung auf Befehl" auf Seite 120)	**Untersuchungsbereich**	Sie können einen Untersuchungsbereich für die Aufgabe zur Untersuchung auf Befehl festlegen sowie zur Einstellung der Sicherheitsstufe wechseln.
	Fenster **Untersuchung auf Befehl anpassen**	Sie können eine der vordefinierten 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.

Aufgabentyp in Kaspersky Embedded Systems Security 2.2	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
Integritätsprüfung von Programm-Modulen (auf S. 119)	**Zeitplan**	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Für Aufgaben des Typs 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

Aufgaben "Automatisches Erstellen von Erlaubnisregeln" und "Erstellen von Regeln für die Gerätekontrolle"

► *Um die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" oder die Aufgabe "Automatisches Erstellen von Erlaubnisregeln" anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Node **Verwaltete Geräte** 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 **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und 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.
5. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

6. Im Abschnitt **Einstellungen** können Sie die folgenden Einstellungen konfigurieren:
   - den Schutzbereich ändern, indem Sie Ordnerpfade und Dateitypen hinzufügen oder löschen und Dateitypen angeben, für die der Start durch automatisch erstellte Regeln erlaubt ist.
   - gestartete Programme berücksichtigen oder nicht berücksichtigen.
7. 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 empfiehlt sich, 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 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 Kriterium für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts festgelegt. Kaspersky Embedded Systems Security 2.2 erlaubt Programme, die mithilfe von Dateien mit einem angegebenen Fingerabdruck: und Header gestartet werden.

     Die Verwendung dieses Kontrollkästchens stellt die strengste 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 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**

  Dropdown-Liste, welche die Auswahl der Kriterien für das Auslösen der Erlaubnisregeln 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 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 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 den Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle "Erlaubnisregeln für Programme aus folgenden Ordnern erstellen" angegeben wurden.

- **SHA256-Hash verwenden**

  Wenn diese Option ausgewählt ist, wird in den Parametern 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 den angegebenen Werten der Prüfsumme.

  Diese Option wird empfohlen, wenn maximal sichere Regeln erstellt werden müssen: Die Prüfsumme, die nach dem Algorithmus SHA256 berechnet wird, ist eine eindeutige ID der Datei. Die Verwendung der erhaltenen SHA256-Prüfsumme als Auslösekriterium für die Regel engt den Gültigkeitsbereich der Regel bis auf eine Datei ein.

- **Regeln für Benutzer oder Benutzergruppe erstellen**.

  Feld, in dem der Benutzer und/oder die Benutzergruppe angegeben sind. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer und/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 2.2 nach Abschluss der Aufgaben erstellt werden.

8. 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).
9. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
10. 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*

11. Klicken Sie im Fenster **Eigenschaften <Name der Aufgabe>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Aufgabe Programm aktivieren

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Node **Verwaltete Geräte** 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 **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und 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.
5. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
6. Wenden 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.
7. 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).
8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
9. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

10. Klicken Sie im Fenster **Eigenschaften <Name der Aufgabe>** 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 in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Node **Verwaltete Geräte** 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 **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und 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 Block **Update-Quelle** die Einstellungen für die Update-Quelle an und optimieren Sie die Nutzung des Laufwerk-Subsystems.
     a. Im Block **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 Block **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 2.2 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 2.2 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 <Name der Aufgabe>** 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 von Programm-Modulen

► *Um eine Gruppenaufgabe zum Update der Programm-Module zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Node **Verwaltete Geräte** 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 **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und 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 der Programm-Module ausführen 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 <Name der Aufgabe>** auf **OK**.

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Erstellen einer Aufgabe zur Untersuchung auf Befehl

► *Um eine neue Aufgabe zu erstellen, führen Sie in der Verwaltungskonsole von Kaspersky Security Center folgende Aktionen aus:*

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 des Administrationsservers von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, zu der der geschützte Computer gehört.
     b. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Geräte** das Kontextmenü für die Zeile mit Informationen über den geschützten Computer und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im erscheinenden Fenster im Abschnitt **Aufgaben** auf **Hinzufügen**.

- Für das Erstellen einer Gruppenaufgabe:

  a. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, für die Sie eine Richtlinie erstellen möchten.

  b. Öffnen Sie im Ergebnisfenster das Kontextmenü auf der Registerkarte **Aufgaben** und wählen Sie den Punkt **Neu > Aufgabe**.

- Um eine Aufgabe für eine beliebige Auswahl an Computern zu erstellen, öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center den Knoten **Geräteauswahl** und wählen Sie den Punkt **Aufgabe erstellen** aus.

Darauf öffnet sich der Assistent für neue Aufgaben.

2. Geben Sie im Fenster **Aufgabenname festlegen** einen Aufgabennamen an (maximal 100 Zeichen, wobei folgende Zeichen unzulässig sind: **I * < > ? \ / | :)**. Es wird empfohlen, den Aufgabentyp im Namen anzugeben (z. B. "Untersuchung auf Befehl der freigegebenen Ordner").
3. Wählen Sie im Fenster **Aufgabentyp** unter der Überschrift **Kaspersky Embedded Systems Security 2.2** die Aufgabe **Untersuchung auf Befehl** aus und 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 anpassen** 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 168).

- 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 **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:

   - Verwendung der heuristischen Analyse an (siehe Abschnitt "Verwendung der heuristischen Analyse" auf Seite 162) passen.
   - Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie Objekte, die in der vertrauenswürdigen Zone von Kaspersky Embedded Systems Security 2.2 beschrieben werden, 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 2.2 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 2.2 die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs in der Aufgabe Echtzeitschutz für Dateien.

     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 2.2 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 2.2 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 2.2 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 2.2 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 das Ereignis "Untersuchung wichtiger Bereiche wurde ausgeführt" 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 die Aufgabe "Untersuchung wichtiger Bereiche" standardmäßig aktiviert.

6. Klicken Sie auf **Weiter**.

7. Richten Sie im Fenster **Zeitplan** einen Zeitplan für die Aufgabe ein (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite 130).
8. Geben Sie ein Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll, und legen Sie einen Aufgabennamen fest.
9. Klicken Sie auf **Fertig**.

Die neue Aufgabe zur Untersuchung auf Befehl wird für einen ausgewählten Computer oder eine Computergruppe erstellt.

Aufgabe zur Untersuchung auf Befehl konfigurieren

► *Um eine bestehende Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Node **Verwaltete Geräte** 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 **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und 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. Im Abschnitt **Einstellungen** können Sie die folgenden Aktionen vornehmen:
   a. Aktivieren Sie im Block **Untersuchungsbereich** die Kontrollkästchen der Dateiressourcen, die Sie in den Untersuchungsbereich aufnehmen möchten.
   b. Klicken Sie auf die Schaltfläche **Anpassen** und wählen Sie eine Sicherheitsstufe aus.

      Sie können eine der vordefinierten Sicherheitsstufen auswählen oder die Sicherheitsstufe manuell anpassen.
   c. Um die Sicherheitsstufe manuell anzupassen, klicken Sie im Fenster **Untersuchung auf Befehl anpassen** auf die Schaltfläche **Einstellungen**.

6. Im Abschnitt **Einstellungen** können Sie die folgenden Aktionen vornehmen:
   a. Im Block **Heuristische Analyse** können Sie die Verwendung der heuristischen Analyse aktivieren oder deaktivieren und die Analysetiefe mithilfe eines Schiebereglers im Block **Heuristische Analyse** anpassen.
   b. Erweiterte Einstellungen anpassen (siehe Abschnitt "Erstellen einer Aufgabe zur Untersuchung auf Befehl" auf Seite 120).
7. 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).
8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
9. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

10. Klicken Sie im Fenster **Eigenschaften <Name der Aufgabe>** auf **OK**.

    Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Zuweisen des Status "Aufgabe zur Untersuchung wichtiger Bereiche" an eine Aufgabe zur Untersuchung auf Befehl

In der Grundeinstellung 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 2.2 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.
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** im Fenster **Eigenschaften: <Aufgabenname>** entweder bei der Erstellung einer Aufgabe zur Untersuchung auf Befehl für eine Gruppe von Computern oder für eine Auswahl von Computern oder zu einem späteren Zeitpunkt aktivieren.

3. Unter Verwendung einer neuen oder vorhanden Richtlinie deaktivieren Sie den Start von Systemaufgaben zur Untersuchung nach Zeitplan (siehe Abschnitt "Zeitplan für den Start von lokalen Systemaufgaben anpassen" auf S. 100) 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 Aufgabenstatus "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.

Untersuchung von in der Cloud gespeicherten Dateien

Über Cloud-Dateien

Kaspersky Embedded Systems Security 2.2 kann mit Cloud-Dateien von Microsoft OneDrive interagieren. Das Programm unterstützt die neue Funktion "OneDrive Files On-Demand".

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 über Ausgabenausführung 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 "Automatisches Erstellen von Erlaubnisregeln" 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.

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

Wenn bei der Arbeit von Kaspersky Embedded Systems Security 2.2 ein Problem auftreten sollte (z. B. Kaspersky Embedded Systems Security 2.2 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 2.2 aktivieren und diese Dateien zur Analyse an den Technischen Support von Kaspersky Lab übermitteln.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 verwaltet. Sie können Zugriffsrechte konfigurieren (s. Abschnitt "Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2" auf S. 82) und den Zugriff auf Protokolle, Trace- und Dump-Dateien nur für bestimmte Benutzer erlauben.

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

1. Öffnen Sie in der Verwaltungskonsole für Kaspersky Security Center das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf S. 107).
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 2.2 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 2.2 in der Protokolldatei speichert.

       Sie können eine der folgenden Genauigkeitsstufen auswählen:

       - **Kritische Ereignisse** – Kaspersky Embedded Systems Security 2.2 speichert nur Informationen über kritische Ereignisse in der Protokolldatei.
       - **Fehler** – Kaspersky Embedded Systems Security 2.2 speichert Informationen über kritische Ereignisse und Fehler in der Protokolldatei.
       - **Wichtige Ereignisse** – Kaspersky Embedded Systems Security 2.2 speichert Informationen über kritische Ereignisse, Fehler und wichtige Ereignisse in der Protokolldatei.
       - **Informative Ereignisse** – Kaspersky Embedded Systems Security 2.2 speichert Informationen über kritische Ereignisse, Fehler, wichtige Ereignisse und informative Ereignisse in der Protokolldatei.
       - **Alle Debug-Informationen** – Kaspersky Embedded Systems Security 2.2 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 27. Subsystemcodes in Kaspersky Embedded Systems Security 2.2

Code des Subsystems	Name des Subsystems
*	Alle Komponenten.
gui	Subsystem der Benutzeroberfläche, Snap-In von Kaspersky Embedded Systems Security 2.2 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 2.2
wp	Arbeitsprozess, der die Aufgaben zum Antiviren-Schutz realisiert
blgate	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security 2.2
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-Berichts
perfcount	Subsystem für Leistungsindikatoren

Die Einstellungen für die Protokollierung von Snap-ins für Kaspersky Embedded Systems Security 2.2 (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 2.2 werden sofort nach dem Speichern der Einstellungen für die Fehlerdiagnose wirksam.

Standardmäßig werden in Kaspersky Embedded Systems Security 2.2 sämtliche Debug-Informationen für alle Komponenten von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 nach Zeitplan einrichten sowie die diesbezüglichen Einstellungen anpassen.

In diesem Abschnitt

Zeitplan-Einstellungen für den Aufgabenstart anpassen

In der Programmkonsole können Sie einen Startzeitplan für lokale Systemaufgaben und benutzerdefinierten Aufgaben erstellen. Für den Start von Gruppenaufgaben kann kein Zeitplan erstellt werden.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und gehen Sie wie folgt vor:
   - Um die Einstellungen einer Richtlinie anzupassen, wählen Sie in der Gruppe der Computer **Richtlinie > <Name der Richtlinie> > <Abschnitt> > Einstellungen > Aufgabenverwaltung** aus.
   - Wenn Sie Programmeinstellungen für einen einzelnen Computer konfigurieren möchten, öffnen Sie die erforderlichen Einstellungen im Fenster **Aufgabeneinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf S. 107) in Kaspersky Security Center.

     Das Fenster **Einstellungen** wird geöffnet.
2. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Zeitplan** 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.

3. Passen Sie die Zeitplaneinstellungen entsprechend an. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie in der Liste **Startintervall** einen der folgenden Werte aus:
      - **Alle n Stunden**, 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.
      - **Alle n Tage**, 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 2.2 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 **Beginnen am** 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 **TASK** 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. 100).

4. Passen Sie auf der Registerkarte **Erweitert** die folgenden Zeitplaneinstellungen gemäß Ihren Anforderungen an.
   - Im Block **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 Block **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 **Zeitabstände für den Start** und geben Sie einen Wert in Minuten ein.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen für den Aufgabenstart zu speichern.

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 die Schaltfläche **Übernehmen**.

Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden gespeichert.

Programmeinstellungen verwalten

Dieser Abschnitt enthält Informationen über die Konfiguration der allgemeinen Einstellungen von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center.

In diesem Kapitel

Verwaltung von Kaspersky Embedded Systems Security 2.2 über Kaspersky Security Center

Sie können mehrere Computer, auf denen Kaspersky Embedded Systems Security 2.2 installiert ist und die Teil einer Administrationsgruppe sind, mithilfe des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security 2.2 zentral verwalten. Ferner erlaubt Kaspersky Security Center ein separates Anpassen der Betriebseinstellungen für jeden in der Administrationsgruppe enthaltenen Computer.

Die *Administrationsgruppe* wird auf Seiten von Kaspersky Security Center manuell erstellt und beinhaltet mehrere Computer, auf denen Kaspersky Embedded Systems Security 2.2 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 2.2 auf diesem Computer durch die aktive Richtlinie von Kaspersky Security Center kontrolliert wird.

Sie können Kaspersky Embedded Systems Security 2.2 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 Computer-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 einheitlicher 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 zur automatischen Erstellung von Erlaubnisregeln konfigurieren.
- **Mithilfe von Aufgaben für eine Auswahl von Geräten**. Aufgaben für eine Auswahl von Geräten ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit begrenzter Ausführungsdauer und für Computer, die nicht einer der erstellten Administrationsgruppen zugeordnet sind, per Fernzugriff.
- **Mithilfe des Eigenschaftenfensters 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 2.2 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 der Ausführung der Protokolle und Benachrichtigungen. Sie können diese Einstellungen sowohl für Computergruppen als auch für einen einzelnen Computer anpassen.

Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center

Sie können die allgemeinen Einstellungen von Kaspersky Embedded Systems Security 2.2 für Computergruppen und für einen einzelnen Computer über Kaspersky Security Center konfigurieren.

In diesem Abschnitt

Skalierbarkeit und Schnittstelle in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *Um die Einstellungen der Skalierbarkeit und der Programmoberfläche zu konfigurieren, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

   > Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Skalierbarkeit und Oberfläche** auf die Schaltfläche **Einstellungen**.
4. Konfigurieren Sie im Fenster **Skalierbarkeit und Oberfläche** auf der Registerkarte **Allgemein** die folgenden Einstellungen:
   - Passen Sie im Block **Skalierbarkeitseinstellungen** die Einstellungen an, durch die die Anzahl der von Kaspersky Embedded Systems Security 2.2 verwendeten Arbeitsprozesse festgelegt wird:
     - **Skalierbarkeitseinstellungen automatisch ermitteln**.

       Die Zahl der verwendeten Prozesse wird von Kaspersky Embedded Systems Security 2.2 automatisch geregelt.
     - **Anzahl der Arbeitsprozesse manuell angeben**.

       Die Zahl der aktiven Arbeitsprozesse wird von Kaspersky Embedded Systems Security 2.2 gemäß den angegebenen Werten geregelt.

       Dieser Wert gilt als Standard.
       - **Maximale Anzahl aktiver Prozesse.**

         Die maximale Anzahl der von Kaspersky Embedded Systems Security 2.2 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**.

5. Klicken Sie auf **OK**.

Die vorgenommenen Programmeinstellungen werden gespeichert.

Sicherheitseinstellungen in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *Um die Sicherheitsparameter manuell anzupassen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Sicherheit und Zuverlässigkeit** auf die Schaltfläche **Einstellungen**.
4. Konfigurieren Sie im Fenster **Sicherheitseinstellungen** die folgenden Einstellungen:
   - Passen Sie im Block **Einstellungen für Zuverlässigkeit** die Wiederherstellungseinstellungen für die Aufgaben von Kaspersky Embedded Systems Security 2.2 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 2.2 nach einer Störung bzw. einer fehlerhaften Beendigung des Programms.

       Ist das Kontrollkästchen aktiviert, stellt Kaspersky Embedded Systems Security 2.2 die Aufgaben von Kaspersky Embedded Systems Security 2.2 nach einer Störung oder einer fehlerhaften Beendigung automatisch wieder her.

Ist das Kontrollkästchen deaktiviert, stellt Kaspersky Embedded Systems Security 2.2 die Aufgaben von Kaspersky Embedded Systems Security 2.2 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 2.2. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Wiederherstellen von Aufgaben ausführen** aktiviert ist.

- Legen Sie im Block **Aktionen beim Wechsel in den USV-Akkubetrieb** die von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 beim Wechsel des Computers auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben an.

    Ist dieses Kontrollkästchen deaktiviert, setzt Kaspersky Embedded Systems Security 2.2 beim Wechsel des Computers auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben fort.

    Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  Der Computer wechselt nur dann auf eine USV-Quelle, wenn der Akkuladezustand unter 90 % fällt.

- Legen Sie im Block **Einstellungen für den Kennwortschutz** das Kennwort für den Schutz des Zugriffs auf die Funktionen von Kaspersky Embedded Systems Security 2.2 fest.

5. Klicken Sie auf **OK**.

Die konfigurierten Sicherheitseinstellungen werden gespeichert.

Verbindungseinstellungen über Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

Die angepassten Verbindungseinstellungen werden für die Verbindungsaufnahme von Kaspersky Embedded Systems Security 2.2 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 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Proxyserver** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Verbindungseinstellungen** wird geöffnet.
4. Konfigurieren Sie im Fenster **Verbindungseinstellungen** die folgenden Parameter:
   - Nehmen Sie im Block **Proxyserver-Einstellungen** die Einstellungen für die Verwendung eines Proxyservers vor:
     - **Keinen Proxyserver verwenden**.

       Ist diese Einstellung ausgewählt, verwendet Kaspersky Embedded Systems Security 2.2 keinen Proxyserver zur Verbindungsaufnahme mit den KSN-Diensten, sondern stellt die Verbindung direkt her.
     - **Proxyserver-Einstellungen automatisch ermitteln**.

       Ist diese Einstellung ausgewählt, ermittelt Kaspersky Embedded Systems Security 2.2 die Einstellungen für die Verbindungsaufnahme mit den KSN-Diensten mithilfe des Protokolls Web Proxy Auto-Discovery Protocol (WPAD) automatisch.

       Diese Variante gilt als Standard.

- **Einstellungen des angegebenen Proxyservers verwenden**.

  Ist diese Einstellung ausgewählt, verwendet Kaspersky Embedded Systems Security 2.2 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 2.2 installiert ist.

  Ist das Kontrollkästchen aktiviert, wird aus dem Netzwerk, zu dem der Computer mit installiertem Kaspersky Embedded Systems Security 2.2 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 Block **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**.

5. Klicken Sie auf **OK**.

Die vorgenommenen Verbindungseinstellungen werden gespeichert.

Über die Konfiguration erweiterter Programmoptionen

Sie können über Kaspersky Security Center erweiterte Optionen für Kaspersky Embedded Systems Security 2.2 für Computergruppen und für einzelne Computer anpassen.

In diesem Abschnitt

Einstellungen für die vertrauenswürdige Zone in Kaspersky Security Center anpassen

Die vertrauenswürdige Zone wird standardmäßig in neu erstellten Richtlinien und Aufgaben übernommen.

► *Zur Konfiguration der vertrauenswürdigen Zone 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Zusätzlich** in der Optionsgruppe **Vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
4. Geben Sie auf der Registerkarte **Ausnahmen** die Objekte an, die Kaspersky Embedded Systems Security 2.2 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 2.2 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**. Geben Sie im erscheinenden Fenster folgende Einstellungen an:
  - **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 2.2 die festgelegten vordefinierten Bereiche, Dateien, Ordner, Laufwerke oder Skriptdateien während der Ausführung der Untersuchung unter Anwendung der Komponente von Kaspersky Embedded Systems Security 2.2, die im Block **Gültigkeitsbereich der Ausnahme** ausgewählt ist.

    Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
  - **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 2.2 die angegebenen gefundenen Objekte bei der Untersuchung.

    Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security 2.2 alle Objekte, die im Programm standardmäßig angegeben sind.

    Das Kontrollkästchen ist standardmäßig deaktiviert.
  - **Gültigkeitsbereich der Ausnahme**

    Name der Aufgabe von Kaspersky Embedded Systems Security 2.2, in der die Regel angewendet wird.
  - Geben Sie im Feld **Kommentar** bei Bedarf zusätzlich erläuternde Informationen zur Ausnahme an.

5. Geben Sie im Fenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** die Prozesse an, die Kaspersky Embedded Systems Security 2.2 bei der Untersuchung überspringen soll:
   - **Datei-Prozesse beim Erstellen einer Backup-Kopie nicht untersuchen**

     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 2.2 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 2.2 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.

- **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**

  Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung der Datei-Aktivität vertrauenswürdiger Prozesse.

  Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security 2.2 bei der Untersuchung die Dateivorgänge vertrauenswürdiger Prozesse.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security 2.2 die Dateivorgänge vertrauenswürdiger Prozesse.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

6. Fügen Sie bei Bedarf Prozesse hinzu, deren Datei-Aktivität Sie nicht untersuchen möchten (siehe Abschnitt "vertrauenswürdige Prozesse hinzufügen" auf Seite 142), indem Sie auf die Schaltfläche **Hinzufügen** klicken.
7. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**, um die Änderungen zu speichern.

Vertrauenswürdige Prozesse hinzufügen

► *Um einen oder mehrere Prozesse zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

   > Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. Klicken Sie im Abschnitt **Zusätzlich** in der Optionsgruppe **Vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
4. Wählen Sie auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**.
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 2.2 den vollständigen Ordnerpfad, um den Status der Vertrauenswürdigkeit des Prozesses zu bestimmen.

        Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad der Datei nicht als Kriterium für die Bestimmung des Status der Vertrauenswürdigkeit des Prozesses berücksichtigt.

        Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     b. **Datei-Hash zur Bestimmung der Vertrauenswürdigkeit des Prozesses verwenden**.

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security 2.2 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 als Kriterium für die Bestimmung des Status der Vertrauenswürdigkeit des Prozesses berücksichtigt.

        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 2.2 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, 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 Computer-Einstellungen über Kaspersky Security Center verwenden.

- **Ein Prozess auf der Grundlage von Namen und Pfad.**

  Nehmen Sie im nächsten Fenster **Vertrauenswürdigen Prozess manuell hinzufügen** folgende Einstellungen vor:

  a. Geben Sie einen Pfad zur ausführbare Datei (inklusive Dateiname) an.

  b. Klicken Sie auf **OK**.

- **Ein Prozess auf der Grundlage der Eigenschaften des Objekts.**

  Nehmen Sie im nächsten Fenster **Vertrauenswürdigen Prozess hinzufügen** 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 2.2 den vollständigen Ordnerpfad, um den Status der Vertrauenswürdigkeit des Prozesses zu bestimmen.

     Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der Ordnerpfad der Datei nicht als Kriterium für die Bestimmung des Status der Vertrauenswürdigkeit des Prozesses berücksichtigt.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  c. **Datei-Hash zur Bestimmung der Vertrauenswürdigkeit des Prozesses verwenden**.

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security 2.2 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 als Kriterium für die Bestimmung des Status der Vertrauenswürdigkeit des Prozesses berücksichtigt.

     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 **Vertrauenswürdigen Prozess 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, dann wird Kaspersky Embedded Systems Security 2.2 die Aktion anwenden, die in den Aufgabeneinstellungen der Software oder der Webressource, die zu dieser Kategorie gehört, festgelegt sind.

► *Um die Not-a-virus-Maske zu verwenden, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Zusätzlich** in der Optionsgruppe **Vertrauenswürdige Zone** auf **Einstellungen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
4. Scrollen Sie auf der Registerkarte **Ausnahmen** 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.

Untersuchung von Wechseldatenträgern

Sie können die Untersuchung von Wechseldatenträgern anpassen, die über USB an den geschützten Computer angeschlossen werden.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 erlaubt den Zugriff auf Wechseldatenträger während der Untersuchung.

Die Ergebnisse der Untersuchung jedes Wechseldatenträgers werden im Protokoll über die Ausführung der Aufgabe zur 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 28. 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 2.2 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.

Um die Einstellungen der Untersuchung von Wechseldatenträgern beim Anschließen anzupassen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Zusätzlich** im Block **Untersuchung von Wechseldatenträgern** auf **Einstellungen**.

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.
4. Im Block **Direkte Untersuchung nach dem Anschließen** gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen **Wechseldatenträger beim Anschließen über USB untersuchen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security 2.2 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.
5. Klicken Sie auf **OK**.

   Die vorgenommenen Einstellungen werden gespeichert und übernommen.

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.

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *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 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Öffnen Sie den Abschnitt **Zusätzlich** und gehen Sie wie folgt vor:
   - Wenn Sie die Zugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security 2.2 für Benutzer oder eine Benutzergruppe konfigurieren möchten, klicken Sie im Block **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 Block **Benutzerrechte für die Verwaltung von Security Service** auf die Schaltfläche **Einstellungen**.
4. Passen Sie im folgenden Fenster die Zugriffsrechte (siehe Abschnitt "Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security 2.2" auf Seite 82) Ihren Bedürfnissen entsprechend an.

Die vorgenommenen Einstellungen werden gespeichert.

Quarantäne- und Backup-Einstellungen in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *Um die Backup-Einstellungen in Kaspersky Security Center anzupassen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Zusätzlich** auf die Schaltfläche **Einstellungen** im Block **Speicher**.
4. 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 in den 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.

5. Passen Sie im Fenster **Speicher** auf der Registerkarte **In Quarantäne verschieben** die folgenden Einstellungen für **In Quarantäne verschieben** an:

   - Wenn Sie den Ordner **In Quarantäne verschieben** ändern möchten, geben Sie im Eingabefeld für den Ordner **In Quarantäne verschieben** den vollständigen Ordnerpfad auf einem lokalen Laufwerk des geschützten Computers an.
   - Wenn Sie die maximale Größe für **In Quarantäne verschieben** 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 des freien Speicherplatzes für **In Quarantäne verschieben** 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.

6. 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 2.2 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 Benutzer des Terminalcomputers können Informationen über Ereignisse des Typs *Objekt gefunden* erhalten.

Sie können die Ereignisbenachrichtigungen für Kaspersky Embedded Systems Security 2.2 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 **Ereignisse** oder im Fenster **Benachrichtigungen anpassen** können Sie die folgenden Benachrichtigungstypen anpassen:

- Auf der Registerkarte **Ereignisse** (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 Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

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 **Ereignisse** als auch im Fenster **Benachrichtigungen anpassen** einstellen, erhält der Systemadministrator Benachrichtigungen über diese Ereignisse durch die angegebene Methode zweimal.

In diesem Abschnitt

Protokolleinstellungen anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *Um die Berichte für Kaspersky Embedded Systems Security 2.2 anzupassen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Block **Protokollen über Aufgabenausführung** auf die Schaltfläche **Einstellungen**.
4. Passen Sie im Fenster **Einstellungen für Protokolle** die folgenden Eigenschaften für Kaspersky Embedded Systems Security 2.2 gemäß Ihren Anforderungen an:
   - Passen Sie die Genauigkeitsstufe der Ereignisse im Protokoll an. Gehen Sie hierzu wie folgt vor:
     a. Wählen Sie in der Liste **Komponente** die Komponente von Kaspersky Embedded Systems Security 2.2, deren Genauigkeitsstufe für Ereignisse Sie festlegen möchten.
     b. Um eine Genauigkeitsstufe in den Protokollen über Aufgabenausführung und im Systemaudit-Protokoll einer bestimmten Komponente anzugeben, wählen Sie die entsprechende Stufe in der Liste **Ereigniskategorie** 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 über Aufgabenausführung gespeichert bleiben sollen.
   - Geben Sie an, wie viele Tage die im Knoten **Systemaudit-Protokoll** angezeigten Informationen gespeichert werden sollen.
5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für Protokolle werden gespeichert.

Sicherheits-Ereignisbericht

Kaspersky Embedded Systems Security 2.2 führt ein Sicherheitsprotokoll über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Computer verbunden sind. In diesem Bericht 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 Echtzeitschutz des Computers, Untersuchung auf Befehl, Überwachung der Datei-Integrität, Kontrolle des Programmstarts und Gerätekontrolle).

Sie können das Sicherheitsprotokoll wie auch das Systemaudit-Protokoll leeren. Dabei registriert Kaspersky Embedded Systems Security 2.2 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 Programmberichte 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 Berichtsverwaltung 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 Berichtseinstellungen 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 Berichts für Sicherheitsverletzungen.

Kaspersky Embedded Systems Security 2.2 kann die Ereignisse in den Programmberichten 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 29. 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 Berichte 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 primären 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 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Block **Protokolle über Aufgabenausführung** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen für Protokolle und Benachrichtigungen** wird geöffnet.
4. Wählen Sie die Registerkarte **SIEM-Integration** aus.
5. Aktivieren Sie im Block **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.
6. Aktivieren Sie bei Bedarf im Block **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 Berichte 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 Berichte 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 Sicherheitsberichts: Das Programm löscht niemals automatisch die Ereignisse des Sicherheitsberichts.

7. Geben Sie im Block **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.

8. Gehen Sie im Block **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 bei Bedarf 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.

9. Klicken Sie auf **OK**.

Die angepassten Einstellungen der SIEM-Integration werden übernommen.

Benachrichtigungseinstellungen anpassen

► *Um die Benachrichtigungen für Kaspersky Embedded Systems Security 2.2 anzupassen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Block **Ereignisbenachrichtigungen** auf die Schaltfläche **Einstellungen**.
4. Passen Sie im Fenster **Benachrichtigungen anpassen** die folgenden Eigenschaften für Kaspersky Embedded Systems Security 2.2 gemäß Ihren Anforderungen an:
   - Wählen Sie in der Liste **Benachrichtigungen anpassen** den Benachrichtigungstyp aus, dessen Einstellungen Sie anpassen möchten.
   - Passen Sie im Block **Benachrichtigung für die Benutzer** die Methode für die Benachrichtigung der Benutzer an. Geben Sie bei Bedarf einen Benachrichtigungstext ein.
   - Passen Sie im Block **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 Block **Grenzwerte für Ereigniserstellung** die Zeitintervalle an, nach deren Ablauf Kaspersky Embedded Systems Security 2.2 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 Tage seit der letzten erfolgreichen Aufgabe zur Untersuchung wichtiger Bereiche.

       Der Standardwert beträgt 30 Tage.
5. Klicken Sie auf **OK**.

Die festgelegten Benachrichtigungseinstellungen werden gespeichert.

Interaktion mit dem Administrationsserver anpassen

► *Um die Typen der Objekte auszuwählen, über die Kaspersky Embedded Systems Security 2.2 Informationen an den Kaspersky Security Center-Administrationsserver übergeben soll, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Berichte und Benachrichtigungen** im Block **Interaktion mit dem Administrationsserver** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Netzwerklisten des Administrationsservers** wird geöffnet.
4. Wählen Sie im Fenster **Netzwerklisten des Administrationsservers** die Objekttypen aus, über die Kaspersky Embedded Systems Security 2.2 Informationen an den Kaspersky Security Center-Administrationsserver übergeben soll:
   - Objekte in der Quarantäne
   - Objekte im Backup
5. Klicken Sie auf **OK**.

   Kaspersky Embedded Systems Security 2.2 wird Informationen über die ausgewählten Objekttypen an den Administrationsserver übertragen.

Echtzeitschutz des Computers

Dieser Abschnitt informiert über die Komponenten für den Echtzeitschutz des Computers: Echtzeitschutz für Dateien, Verwendung von KSN und Exploit-Prävention. Darüber hinaus enthält dieser Abschnitt Anweisungen zum Anpassen der Einstellungen für Aufgaben zum Echtzeitschutz sowie zum Anpassen der Sicherheitseinstellungen des geschützten Computers.

In diesem Kapitel

Echtzeitschutz für Dateien

Dieser Abschnitt informiert über die Aufgabe Echtzeitschutz für Dateien und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

Über die Aufgabe zum Echtzeitschutz für Dateien

Bei Ausführung der Aufgabe zum Echtzeitschutz für Dateien untersucht Kaspersky Embedded Systems Security 2.2 folgende Objekte des geschützten Computers, wenn auf diese zugegriffen wird:

- Dateien
- Alternative Datenströme der Dateisysteme (NTFS-Streams).
- MBR und Bootsektoren von lokalen Festplatten und externer Geräte
- Container-Dateien von Windows Server 2016 und Windows Server 2019

Wenn ein Programm eine Datei auf dem Computer speichert oder eine Datei vom Computer abruft, fängt Kaspersky Embedded Systems Security 2.2 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. Kaspersky Embedded Systems Security 2.2 gibt die Datei dem Programm zurück, wenn sie nicht infiziert ist oder erfolgreich desinfiziert wurde.

Kaspersky Embedded Systems Security 2.2 fängt Dateioperationen ab, die in Containern von Windows Server 2016 und Windows Server 2019 ausgeführt werden.

Ein Container ist eine isolierte Umgebung, in der Programme ohne direkte Interaktion mit dem Betriebssystem ausgeführt werden können. Wenn der Container sich innerhalb des Schutzbereichs der Aufgabe befindet, untersucht Kaspersky Embedded Systems Security 2.2 die Container-Dateien, auf die von Benutzern zugegriffen wird, auf Bedrohungen der Computer-Sicherheit. Wenn eine Bedrohung gefunden wird, versucht das Programm, den Container zu desinfizieren. Ist der Versuch erfolgreich, setzt der Container seine Ausführung fort; misslingt die Desinfektion, so wird der Container deaktiviert.

Kaspersky Embedded Systems Security 2.2 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.

Aufgabe zum Echtzeitschutz für Dateien anpassen

Die Systemaufgabe Echtzeitschutz für Dateien weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 30. Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien

Einstellung	Standardwert	Beschreibung
Schutzbereich	Gesamter Computer ohne virtuelle Festplatten	Sie können den Schutzbereich beschränken.
Sicherheitsstufe	Einheitlich für den gesamten Schutzbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Sie können für bestimmte Knoten in der Dateistruktur des Computers: • Eine andere vordefinierte Sicherheitsstufe übernehmen. • Sicherheitsstufe manuell ändern. • Sicherheitseinstellungen des ausgewählten Knotens zur späteren Verwendung in einer Vorlage speichern.
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 2.2 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.

Einstellung	Standardwert	Beschreibung
KSN zum Schutz verwenden	Wird verwendet	Sie können Ihren Computer 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 Computer blockieren, von denen schädliche Aktivitäten ausgehen	Wird nicht verwendet.	Sie können Computer, bei denen schädliche Aktivitäten festgestellt wurden, zur Liste der nicht vertrauenswürdigen Computer hinzufügen.

► *Um die Aufgabe Echtzeitschutz für Dateien zu konfigurieren, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz für Dateien** auf die Schaltfläche **Einstellungen** im Block **Echtzeitschutz für Dateien**.

   Das Fenster **Echtzeitschutz für Dateien** wird geöffnet.
4. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Auf der Registerkarte **Allgemein**:
     - Schutzmodus (siehe Abschnitt "Schutzmodus auswählen" auf S. 163) für Objekte
     - Heuristische Analyse verwenden (auf S. 162)
     - Einstellungen für die Integration mit anderen Komponenten von Kaspersky Embedded Systems Security 2.2.
   - Auf der Registerkarte **Aufgabenverwaltung**:
     - Einstellungen für den Aufgabenstart nach Zeitplan (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite. 130).

5. 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 für die Aufgabe Echtzeitschutz für Dateien" auf Seite 164).
     - 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 (siehe Abschnitt "Vordefinierte Sicherheitsstufen wählen" auf S. 166) oder passen Sie die Schutzeinstellungen manuell an (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf S. 168).
6. Klicken Sie im Fenster **Echtzeitschutz für Dateien** auf **OK**.

Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung gespeichert.

Heuristische Analyse verwenden

Sie können die heuristische Analyse verwenden und die Analysestufe für Aufgaben von Kaspersky Embedded Systems Security 2.2 anpassen.

► *Um die heuristische Analyse anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie die Programmeinstellungen (siehe Abschnitt "Methoden zur Verwaltung von Kaspersky Embedded Systems Security 2.2 durch Kaspersky Security Center" auf Seite 133) oder die Richtlinieneinstellungen (siehe Abschnitt "Richtlinie anpassen" auf Seite 95), für die Sie die Heuristische Analyse konfigurieren möchten.
2. Deaktivieren oder aktivieren Sie 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. 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.

Schutzmodus auswählen

Sie können den Schutzmodus in der Aufgabe Echtzeitschutz für Dateien auswählen. Im Block **Schutzmodus für Objekte** können Sie festlegen, bei welcher Art des Zugriffs auf die Objekte Kaspersky Embedded Systems Security 2.2 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. 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Einstellungen** im Block **Echtzeitschutz für Dateien**.

   Das Fenster **Echtzeitschutz für Dateien** wird geöffnet.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** den Schutzmodus aus, den Sie festlegen möchten:

   - **Intelligenter Modus**

     Kaspersky Embedded Systems Security 2.2 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 2.2 das Objekt erst dann erneut, wenn es von diesem Prozess zum letzten Mal gespeichert wird.

   - **Beim Öffnen und Ändern**

     Kaspersky Embedded Systems Security 2.2 untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern.

     Diese Variante gilt als Standard.

   - **Beim Öffnen**

     Kaspersky Embedded Systems Security 2.2 untersucht alle Objekte, wenn diese zum Lesen, zur Ausführung oder zum Ändern geöffnet werden.

   - **Beim Ausführen**

     Kaspersky Embedded Systems Security 2.2 untersucht die Datei nur beim Öffnen zum Ausführen.

5. Klicken Sie auf **OK**.

Der ausgewählte Schutzmodus für die Objekte wird eingestellt.

Schutzbereich für die Aufgabe Echtzeitschutz für Dateien

Dieser Abschnitt enthält Informationen über die Einrichtung und Nutzung eines Schutzbereichs in der Aufgabe Echtzeitschutz für Dateien und dessen weitere Verwendung.

In diesem Abschnitt

Vordefinierte Schutzbereiche

Die Dateiressourcen des geschützten Computers werden in den Einstellungen der Aufgabe **Echtzeitschutz für Dateien** auf der Registerkarte **Schutzbereich** 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 2.2 deckt die folgenden vordefinierten Schutzbereiche ab:

- **Lokale Festplatten**. Kaspersky Embedded Systems Security 2.2 schützt Dateien auf den Festplatten des Computers.
- **Wechseldatenträger**. Kaspersky Embedded Systems Security 2.2 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 2.2 schützt die Dateien, die in Netzwerkordnern gespeichert sind oder aus diesen von auf dem Computer laufenden Programmen abgefragt werden. Kaspersky Embedded Systems Security 2.2 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 Laufwerke, die mit dem Befehl SUBST erzeugt wurden, werden in der Dateistruktur des Computers in der Programmkonsole nicht 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 nicht in der Liste 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 wählen

Für Knoten, die in der Liste der Dateiressourcen des Computers ausgewählt sind, 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 2.2 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 31. 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 untersuchen, wenn größer als (MB)	8 MB	8 MB	Nicht konfiguriert.
Alternative NTFS-Ströme	Ja	Ja	Ja
Bootsektoren und MBR	Ja	Ja	Ja

Einstellungen	Sicherheitsstufe		
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.

► *Um eine vordefinierte Sicherheitsstufe auszuwählen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Einstellungen** im Block **Echtzeitschutz für Dateien**.

   Das Fenster **Echtzeitschutz für Dateien** wird geöffnet.
4. 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.

5. Wählen Sie die gewünschte Sicherheitsstufe in der Dropdown-Liste aus:
   - **Maximale Sicherheit**
   - **Empfohlen**
   - **Maximale Leistung**
6. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung gespeichert.

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 wählen" auf S. 166).

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für bestimmte Knoten der Struktur oder Liste der Dateiressourcen des Computers festlegen.

Bei der Arbeit mit der Struktur der Dateiressourcen auf dem Computer werden die Sicherheitseinstellungen, die für den ausgewählten übergeordneten Knoten konfiguriert wurden, automatisch für alle untergeordneten Knoten übernommen. Die Sicherheitseinstellungen des übergeordneten Knotens werden für untergeordnete Knoten, die gesondert konfiguriert werden, nicht übernommen.

► *So passen Sie die Sicherheitsparameter eines bestimmten Knotens manuell an:*

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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Einstellungen** im Block **Echtzeitschutz für Dateien**.

   Das Fenster **Echtzeitschutz für Dateien** wird geöffnet.

4. 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.

5. Auf der Registerkarte **Sicherheitsstufe** können Sie eine bereits vorhandene Stufe auswählen, oder Sie klicken auf die Schaltfläche **Einstellungen**, um die Einstellungen anzupassen.

6. Sie können die benutzerdefinierten Sicherheitseinstellungen des ausgewählten Knotens gemäß Ihren Bedürfnissen anpassen:

   - Allgemeine Einstellungen (siehe Abschnitt "Allgemeine Aufgabeneinstellungen anpassen" auf Seite 169)
   - Aktionen (siehe Abschnitt "Aktionen anpassen" auf Seite 172)
   - Optimierung (siehe Abschnitt "Leistung optimieren" auf Seite 174)

7. Klicken Sie im Fenster **Schutzbereichseinstellungen** auf **Speichern**.

Die neuen Einstellungen des Schutzbereichs werden gespeichert.

Allgemeine Aufgabeneinstellungen anpassen

► *So passen Sie die allgemeinen Sicherheitseinstellungen der Aufgabe zum Echtzeitschutz für Dateien an:*

1. Öffnen Sie das Fenster **Einstellungen für den Echtzeitschutz für Dateien** (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 168) anpassen.
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 2.2 untersucht alle Objekte.

   - **Objekte, die nach Format untersucht werden**

     Kaspersky Embedded Systems Security 2.2 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 2.2 enthalten.

   - **Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden**

     Kaspersky Embedded Systems Security 2.2 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 2.2 enthalten.

- **Objekte, die nach der angegebenen Erweiterungsliste untersucht werden**

  Kaspersky Embedded Systems Security 2.2 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 2.2 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 Objekt 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 2.2 als neu oder seit der letzten Untersuchung geändert erkennt, aktiviert oder deaktiviert.

   Wenn dieses Kontrollkästchen aktiviert ist, untersucht und schützt Kaspersky Embedded Systems Security 2.2 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 Sicherheitsstufen **Maximale Leistung** und **Empfohlen** standardmäßig aktiviert. Wurde die Sicherheitsstufe **Maximale Sicherheit** ausgewählt, ist das Kontrollkästchen deaktiviert.

> Um zwischen den verfügbaren Optionen hin- und herzuwechseln, 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 2.2 Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Embedded Systems Security 2.2 bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

   - **Alle / Nur neue SFX-Archive**

     Selbstentpackende Archive untersuchen.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Embedded Systems Security 2.2 SFX-Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Embedded Systems Security 2.2 bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe 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 2.2 Mail-Datenbankdateien.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Mail-Datenbankdateien von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe 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 2.2 Dateien in Mail-Formaten.

Wenn dieses Kontrollkästchen deaktiviert ist, werden Dateien in Mail-Formaten von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe 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 für den Echtzeitschutz für Dateien** (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 168) anpassen.
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 2.2 den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Bericht über 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 Schutzbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security 2.2 die Sicherheitsstufe automatisch auf **Benutzerdefiniert**.

   - **Zugriff verweigern**.

     Ist diese Einstellung ausgewählt, verweigert Kaspersky Embedded Systems Security 2.2 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 2.2 den Zugriff auf gefundene oder andere gefundene Objekte nicht und führt keine Aktionen an ihnen durch. Das folgende Ereignis wird im Bericht über 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 Schutzbereich separat konfiguriert werden. Dieser Modus wird standardmäßig bei keiner Sicherheitsstufe anwendet. Wenn Sie diesen Modus auswählen, ändert Kaspersky Embedded Systems Security 2.2 die Sicherheitsstufe automatisch auf **Benutzerdefiniert**.

   - **Zugriff verweigern**.

     Ist diese Einstellung ausgewählt, verweigert Kaspersky Embedded Systems Security 2.2 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:

     - **Quarantäne**.
     - **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 eine primäre und eine sekundäre Aktion festlegen, indem Sie auf die Schaltfläche **Einstellungen** neben dem Kontrollkästchen klicken.

      Wenn das Kontrollkästchen deaktiviert ist, führt Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 die festgelegte Aktion nicht aus, wenn das übergeordnete Objekt nicht bearbeitet werden kann.

   Das Kontrollkästchen ist für die Sicherheitsstufe **Maximale Sicherheit** standardmäßig aktiviert und für die Sicherheitsstufen **Empfohlen** und **Maximale Leistung** standardmäßig deaktiviert.

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 für den Echtzeitschutz für Dateien** (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf Seite 168) anpassen.
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 2.2 die angegebenen Objekte bei der Untersuchung.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security 2.2 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 Website der Viren-Enzyklopädie http://www.securelist.com.

  Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Embedded Systems Security 2.2 die angegebenen gefundenen Objekte bei der Untersuchung.

  Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Embedded Systems Security 2.2 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 Block **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 in der Grundeinstellung aktiviert.

   - **Zusammengesetzte Objekte nicht untersuchen, 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 2.2 bei der Untersuchung auf Viren übersprungen.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security 2.2 zusammengesetzte Objekte unabhängig von der Größe.

     Das Kontrollkästchen ist für die Sicherheitsstufen **Empfohlen** und **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 2.2 nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems.

     Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security 2.2 Dateien des NTFS-Systems unabhängig vom Erstellungs- oder Änderungsdatum.

     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 2.2 nur neue oder veränderte Dateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Embedded Systems Security 2.2 Dateien unabhängig vom Erstellungs- oder Änderungsdatum.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

5. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Verwendung von KSN

Dieser Abschnitt informiert über die Aufgabe Verwendung von KSN und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

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 2.2 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 2.2 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 zur 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 2.2 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 2.2 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 "Konfiguration der Datenverarbeitung" auf Seite 181) der Aufgabe "Verwendung von KSN" die KSN-Erklärung lesen und die Aufgabe mithilfe des Kontrollkästchens **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Private Security Network** aktivieren. Indem Sie die Bedingungen akzeptieren, erklären Sie sich damit einverstanden, dass alle Datentypen, die in der KPSN-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 2.2: Jegliche Verarbeitung KSN-bezogener Daten wird gestoppt.

Konfiguration der Aufgabe Verwendung von KSN

Sie können die Standard-Einstellungen der Aufgabe "Verwendung von KSN" anpassen (siehe Tabelle unten).

Tabelle 32. Standardeinstellungen für die Aufgabe "Verwendung von KSN"

Einstellung	Standardwert	Beschreibung
Aktionen für Objekte, die in KSN nicht vertrauenswürdig sind	Löschen	Sie können die Aktionen festlegen, die Kaspersky Embedded Systems Security 2.2 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 2.2 den MD5-Hash für Dateien beliebiger Größe.
KSN-Erklärung	Das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network**wird deaktiviert.	Entscheiden Sie nach der Installation, ob Sie an KSN teilnehmen möchten. 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.
Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Managed Protection	Deaktiviert	Sie können den KMP-Dienst aktivieren oder deaktivieren. Dieser Dienst ist nur verfügbar, wenn beim Kauf des Programms der zusätzliche Lizenzvertrag unterzeichnet wurde.

Einstellung	Standardwert	Beschreibung
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	Ausgewählt	Die Daten werden standardmäßig über das Kaspersky Security Center an KSN gesendet.

► *Um die Einstellungen der Aufgabe Verwendung von KSN zu konfigurieren, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Einstellungen** im Block **Verwendung von KSN**.

   Das Fenster **Verwendung von KSN** wird geöffnet.
4. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:
   - Geben Sie im Block **Aktion für Objekte, die in KSN nicht vertrauenswürdig sind** die Aktion an, die Kaspersky Embedded Systems Security 2.2 ausführen soll, wenn ein Objekt gefunden wird, das laut KSN als nicht vertrauenswürdig eingestuft ist:
     - **Löschen**

       Kaspersky Embedded Systems Security 2.2 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 2.2 nimmt Informationen über das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, in das Protokoll über Ausgabenausführung auf. Das nicht vertrauenswürdige Objekt wird von Kaspersky Embedded Systems Security 2.2 nicht gelöscht.

- Begrenzen Sie im Block **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 2.2 nicht ermittelt.

    Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security 2.2 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 2.2 die Prüfsumme berechnen soll.
- Aktivieren oder deaktivieren Sie 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*.

5. 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 Computers automatisch gestartet wird.

   Das Programm startet die Aufgabe Verwendung von KSN zukünftig nach Zeitplan.
6. Passen Sie die Datenverarbeitung (s. Abschnitt "Datenverarbeitung konfigurieren" auf S. 181) vor dem Start der Aufgabe an.
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 Protokoll über Ausgabenausführung gespeichert.

Konfiguration der Datenverarbeitung

► *Um festzulegen, welche Daten von den KSN-Diensten verarbeitet werden, und die KSN-Erklärung zu akzeptieren, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Datenverarbeitung** im Block **Verwendung von KSN**.

   Das Fenster **Datenverarbeitung** wird geöffnet.
4. Lesen Sie auf der Registerkarte **Statistiken und 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 2.2 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 2.2 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 2.2 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 2.2 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 2.2 neu starten.

Um den KMP-Dienst nutzen zu können, müssen Sie den entsprechenden Lizenzvertrag signieren und Konfigurationsdateien auf einem geschützten Computer ausführen.

Um den KMP-Dienst nutzen zu können, müssen die Bedingungen zur Datenverarbeitung in der KSN-Erklärung auf der Registerkarte **Statistiken und 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 2.2 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**).

Siehe den Abschnitt "Lokale Datenverarbeitung" dieses Handbuchs für genauere Informationen zu Daten, die an Kaspersky Lab gesendet werden.

Die entsprechenden Kontrollkästchen können nur dann aktiviert bzw. deaktiviert werden, wenn das Kontrollkästchen **Ich akzeptiere die Bedingungen der Erklärung zu Kaspersky Security Network** aktiviert ist.

Kaspersky Embedded Systems Security 2.2 sendet standardmäßig Prüfsummen von Dateien sowie zusätzliche Statistiken, nachdem Sie die KSN-Erklärung akzeptiert haben.

Tabelle 33. 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
☑	• Anfragen bezüglich der Reputation werden gesendet • Kontrollkästchen ist editierbar	• Zusätzliche Statistiken werden gesendet • Kontrollkästchen ist editierbar
☑	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist nicht editierbar
☐	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist editierbar
☐	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist nicht editierbar

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 2.2 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 Einstellungen zum Schutz der Prozesse vor der Ausnutzung von Schwachstellen anpassen.

Die Komponente schützt den Prozess-Speicher vor Exploits mithilfe der Einschleusung eines externen Agenten zum Schutz von Prozessen (im Weiteren "Agent") in den geschützten Prozess.

Der externe Schutz-Agent ist ein dynamisch ladendes Modul von Kaspersky Embedded Systems Security 2.2, 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 das Entladen des Agenten aus dem Prozess nach seiner Entfernung aus der Liste der geschützten Prozesse ist nur nach einem Neustart des Prozesses möglich.

Das Entladen des Agenten aus den geschützten Prozessen setzt voraus, dass die Prozesse beendet werden: Beim Entfernen der Komponente "Exploit-Prävention" friert das Programm die Umgebung ein und erzwingt das Entladen des Agenten aus den geschützten Prozessen. Wenn der Agent während der Deinstallation der Komponente in einen der geschützten Prozesse eingeschleust wird, müssen Sie den betroffenen Prozess beenden. Möglicherweise muss 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 2.2 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-Präventionsdienst

Um eine möglichst effektive Nutzung der Funktionen der Komponente "Exploit-Prävention" zu gewährleisten, muss auf dem geschützten Computer der Kaspersky Security Exploit-Präventionsdienst 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 des Kaspersky Security Exploit-Präventionsdienstes schützt Kaspersky Embedded Systems Security 2.2 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.

Sollte der Kaspersky Security Exploit-Präventionsdienst 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 2.2 den Prozess nicht – unabhängig vom Modus, der in den Einstellungen der Komponente "Exploit-Prävention" angegeben ist.

- **Nur über missbräuchlich verwendete Prozesse benachrichtigen**: Wenden Sie diesen Modus an, um mithilfe von Ereignissen im Bericht für Sicherheitsverletzungen Daten über Exploits in geschützten Prozessen zu erhalten.

  In diesem Modus protokolliert Kaspersky Embedded Systems Security 2.2 alle Exploit-Versuche in Form von Ereignissen.

Einstellungen zum Schutz des Prozess-Speichers anpassen

► *Um die Einstellungen der Exploit-Prävention für die Prozesse anpassen, die zur Liste mit geschützten Prozessen hinzugefügt wurden, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Einstellungen** im Block **Exploit-Prävention**.

   Das Fenster **Exploit-Prävention** wird geöffnet.

4. 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 2.2 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 2.2 nicht vor Exploits geschützt.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - **Bei Exploit beenden**.

     In diesem Modus beendet Kaspersky Embedded Systems Security 2.2 einen geschützten Prozess beim Fund eines Exploit-Versuchs, wenn ein aktives Verfahren zur Risikominderung angewendet wird.

   - **Nur über missbräuchlich verwendete Prozesse benachrichtigen**.

     In diesem Modus benachrichtigt Kaspersky Embedded Systems Security 2.2 anhand eines Terminalfensters über Exploits. Der missbräuchlich verwendete Prozess wird auch weiterhin ausgeführt.

     Wenn Kaspersky Embedded Systems Security 2.2 während der Ausführung des Programms im Modus **Bei Exploit beenden** einen Exploit in einem kritischen Prozess findet, wechselt die Komponente zwangsläufig in den Modus **Über missbräuchlich verwendete Prozesse nur informieren**.

5. 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 2.2 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 2.2 kein Terminalfenster an, wenn ein Exploit-Versuch gefunden oder ein missbräuchlich verwendeter Prozess beendet wurde. Das Terminalfenster wird unabhängig vom Status des Kaspersky Security Exploit-Präventionsdienstes 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 2.2 die Risiken der Ausnutzung von Schwachstellen von bereits gestarteten Prozessen unabhängig davon, ob der Dienst Kaspersky Security Service läuft. Kaspersky Embedded Systems Security 2.2 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 2.2 keine Prozesse vor Exploits, wenn Kaspersky Security Service beendet wurde.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security 2.2 speichert und übernimmt die angepassten Einstellungen zum Schutz des Prozess-Speichers.

Geschützte Prozesse hinzufügen

Die Komponente "Exploit-Prävention" schützt einige Prozesse standardmäßig. Sie können diese Prozesse 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. 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Echtzeitschutz des Computers** auf die Schaltfläche **Einstellungen** im Block **Exploit-Prävention**.

   Das Fenster **Exploit-Prävention** wird geöffnet.
4. Klicken Sie auf der Registerkarte **Geschützte Prozesse** auf die Schaltfläche **Durchsuchen**.

   Das Microsoft-Windows-Explorer-Fenster wird geöffnet.
5. Wählen Sie den Prozess aus, den Sie zur Liste hinzufügen möchten.
6. Klicken Sie auf **Öffnen**.

   Der Prozessname wird in der Zeile angezeigt.
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der angegebene Prozess wird zur Liste der geschützten Prozesse hinzugefügt.
8. Wählen Sie den hinzugefügten Prozess aus und klicken Sie auf **Methoden zur Exploit-Prävention angeben**.

   Das Fenster **Methoden zur Exploit-Prävention angeben** wird geöffnet.
9. 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 Methoden 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.

     b. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Attack Surface Reduction anwenden**.

10. Passen Sie die Einstellungen die 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
        - Intranet
        - Vertrauenswürdige Websites
        - Websites mit eingeschränktem Zugriff
        - Computer

    Diese Einstellungen gelten nur für den Internet Explorer®.
11. Klicken Sie auf **OK**.

Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Exploit-Präventionstechniken

Tabelle 34. Exploit-Präventionstechniken

Exploit-Präventionstechnik	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
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).

Exploit-Präventionstechnik	Beschreibung
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.

Überwachung der Server-Aktivitäten

Dieser Abschnitt enthält Informationen über die Funktionen von Kaspersky Embedded Systems Security 2.2 zur Kontrolle der Starts und Verbindungen von Apps durch externe Geräte über USB und die Windows Firewall.

In diesem Kapitel

Verwaltung des Programmstarts aus Kaspersky Security Center

Sie können den Programmstart auf allen Computern im Unternehmensnetzwerk erlauben oder verbieten, indem Sie einheitliche Listen mit Regeln für die Kontrolle des Programmstarts aufseiten von Kaspersky Security Center für Computergruppen erstellen.

In diesem Abschnitt

Über die Verwendung von Profilen bei der Konfiguration der Aufgabe zur Kontrolle des Programmstarts in der Richtlinie von Kaspersky Security Center

Die in der Richtlinie konfigurierten Regeln für die Kontrolle des Programmstarts werden für alle Computer der Administrationsgruppe übernommen. Beinhaltet eine Administrationsgruppe Computer unterschiedlicher Typen, so können für die Kontrolle des Programmstarts für jeden davon individuelle Regellisten erforderlich werden. Um die Übernahme der Richtlinien für die Computer innerhalb einer Administrationsgruppe zu differenzieren, können Sie *Richtlinienprofile* verwenden.

Es wird empfohlen, Richtlinienprofile für die Konfiguration von Regeln für die Kontrolle des Programmstarts auf Computern unterschiedlicher Typen innerhalb einer Administrationsgruppe zu verwenden, die durch ein und dieselbe Richtlinie verwaltet wird. Dadurch wird der Computerschutz optimiert, da die festgelegten Regeln die Starts nur jener Programme kontrollieren, die für diesen Computertyp charakteristisch sind.

Richtlinienprofile werden für die Computer einer Administrationsgruppe in Übereinstimmung mit den für diese festgelegten *Tags* übernommen. Sie können Richtlinienprofile für alle Computer einer Gruppe, die ein gemeinsames Tag haben, einrichten.

Ausführliche Informationen über Tags und Richtlinienprofile sowie eine Anleitung für die Arbeit mit diesen finden Sie im *Hilfesystem von Kaspersky Security Center*.

► *Gehen Sie wie folgt vor, um ein Richtlinienprofil in der Aufgabe Kontrolle des Programmstarts zu verwenden:*

1. Öffnen Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für die Sie die Verwendung von Richtlinienprofilen einrichten möchten.
2. Weisen Sie jedem Computer der Administrationsgruppe in Übereinstimmung mit dem Computertyp ein Tag zu. Gehen Sie hierzu wie folgt vor:
   - Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Geräte** und wählen Sie den Computer aus, dem Sie Tags zuweisen möchten. Öffnen Sie im Fenster **Eigenschaften:<Name des Computers>** des ausgewählten Computers den Abschnitt **Tags** und erstellen Sie eine Liste von Tags. Klicken Sie auf **OK**.
3. Erstellen Sie ein Richtlinienprofil und konfigurieren Sie dessen Übernahme für den Computerschutz innerhalb der Administrationsgruppe. Gehen Sie hierzu wie folgt vor:
   - Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Richtlinien** und wählen Sie die Richtlinie aus, für die Sie die Verwendung von Profilen einrichten möchten. Öffnen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** der ausgewählten Richtlinie den Abschnitt **Richtlinienprofile** und klicken Sie auf **Hinzufügen**, um ein neues Profil zu erstellen. Das Fenster **Eigenschaften: <Profilname>** wird geöffnet. Führen Sie folgende Aktionen aus:
     a. Richten Sie im Abschnitt **Aktivierungsregeln** den Gültigkeitsbereich für das Profil ein und legen Sie die Bedingungen fest, bei deren Vorliegen das Profil aktiviert wird.
     b. Konfigurieren Sie im Abschnitt **Kontrolle des Programmstarts** die Listen der Regeln für die Kontrolle des Programmstarts für das zu bearbeitende Profil.
     c. Klicken Sie auf **OK**.
4. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Das konfigurierte Profil wird in der Richtlinie für die Aufgabe Kontrolle des Programmstarts übernommen.

Aufgabe Kontrolle des Programmstarts konfigurieren

Sie können die Standardwerte der Einstellungen der Aufgabe "Kontrolle des Programmstarts" ändern (s. Tabelle unten).

Tabelle 35. Standardeinstellungen der Aufgabe zur Kontrolle des Programmstarts

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	**Nur Statistik**. Die Aufgabe trägt Ereignisse, die auf Verbot und Start von Programmen basieren, gemäß den festgelegten Regeln in das Protokoll über Ausgabenausführung ein. Der Programmstart wird nicht explizit verboten.	Sie können den Modus **Aktiv** für den Schutz des Computers auswählen, nachdem die endgültige Liste der Regeln erstellt wurde.
Regelverwaltung	**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.	Sie können Dateitypen angeben, deren Start durch die Regeln kontrolliert werden soll.
Verwendung von KSN	Die Daten von KSN bezüglich der Reputation von Programmen 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 der unten gelisteten 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	Wird verwendet	Sie können die Installation oder das Update einer beliebigen Software erlauben, wenn der entsprechende Vorgang über Windows Installer ausgeführt wird.
Start von Kommandozeilen-interpretern ohne auszuführenden Befehl verbieten	Wird nicht verwendet.	Sie können den Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten.
Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Kontrolle des Programmstarts wird beim Start von Kaspersky Embedded Systems Security 2.2 nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

► *Gehen Sie wie folgt vor, um die Einstellungen der Aufgabe Kontrolle des Programmstarts zu konfigurieren:*

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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Kontrolle des Programmstarts**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.
4. Wählen Sie auf der Registerkarte **Allgemein** im Block **Modus** folgende Einstellungen:
   - Geben Sie in der Dropdown-Liste **Aufgabenmodus** den Ausführungsmodus der Aufgabe an.

     In dieser Dropdown-Liste können Sie einen Ausführungsmodus für die Aufgabe zur Kontrolle des Programmstarts auswählen:

     - **Aktiv**. Kaspersky Embedded Systems Security 2.2 kontrolliert alle Programmstarts mithilfe vorgegebener Regeln.
     - **Nur Statistik**. Kaspersky Embedded Systems Security 2.2 kontrolliert den Programmstart nicht mithilfe vorgegebener Regeln, sondern hält lediglich Informationen über den Start von Programmen im Protokoll über Ausgabenausführung fest. Der Start aller Programme ist erlaubt. Sie können diesen Modus für die Erstellung einer Liste der Regeln für die Kontrolle des Programmstarts auf Grundlage der im Protokoll über Ausgabenausführung enthaltenen Informationen 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 Präzedenzfälle.

     Ist das Kontrollkästchen aktiviert, so verbietet oder erlaubt Kaspersky Embedded Systems Security 2.2 die Ausführung eines wiederholt gestarteten Programms auf Grundlage der Entscheidung, die durch die Aufgabe zur Kontrolle des Programmstarts beim ersten Programmstart getroffen wurde. Wenn beispielsweise der erste Programmstart durch die Regeln für die Kontrolle des Programmstarts erlaubt wurde, so verbleibt der Eintrag über dieses Ereignis im Cache und der wiederholte Start dieses Programms wird erlaubt, ohne erneut zu überprüfen, ob Erlaubnisregeln vorliegen.

Ist das Kontrollkästchen deaktiviert, so untersucht Kaspersky Embedded Systems Security 2.2 das Programm bei jedem 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 2.2 den Start des Kommandozeileninterpreters auch dann, wenn der Start des Interpreters erlaubt ist. Die Befehlszeile ohne Befehle kann nur dann gestartet werden, wenn beide Bedingungen erfüllt sind:

  - Der Start des Kommandozeileninterpreters ist erlaubt.
  - Der ausgeführte Befehl ist erlaubt.

  Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security 2.2 für den Start der Befehlszeile nur die Erlaubnisregeln. Der Start wird verboten, wenn keine Erlaubnisregel übernommen wurde oder der ausführbare Prozess keinen vertrauenswürdigen KSN-Status hat. Wenn die Erlaubnisregel übernommen wird oder der Prozess einen vertrauenswürdigen KSN-Status hat, kann die Befehlszeile mit oder ohne Befehl zur Ausführung gestartet werden.

  Kaspersky Embedded Systems Security 2.2 erkennt die folgenden Kommandozeileninterpreter:

  - cmd.exe
  - powershell.exe
  - python.exe
  - perl.exe

5. Passen Sei im Block **Regeln** die Einstellungen für die Anwendung der Regeln an:

   a. Klicken Sie auf die Schaltfläche **Regelliste**, um Erlaubnisregeln zur Kontrolle des Aufgabenstarts hinzuzufügen.

   > Kaspersky Embedded Systems Security 2.2 erkennt keine Pfade, die einen Schrägstrich "/" 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 Erlaubnisregeln" bearbeiten.

     > Standardmäßig wendet Kaspersky Embedded Systems Security 2.2 zwei vordefinierte Regeln an, die den Start von Skripts, MSI-Paketen und Startdateien gemäß Zertifikat erlauben.

6. Nehmen Sie im Block **Gültigkeitsbereich der Regeln** die folgenden Einstellungen vor:

- **Regeln für ausführbare Dateien verwenden**.

  Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Starts ausführbarer Programmdateien.

  Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security 2.2 den Start ausführbarer Programmdateien mithilfe vorgegebener Regeln, in deren Einstellungen "Ausführbare Dateien" als Geltungsbereich angegeben ist.

  Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security 2.2 keine Kontrolle des Starts ausführbarer Programmdateien mithilfe vorgegebener Regeln. Der Start ausführbarer Programmdateien ist erlaubt.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Laden von DLL-Modulen überwachen**.

  Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Ladens von DLL-Modulen.

  Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security 2.2 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 2.2 keine Kontrolle des Ladens von DLL-Modulen mithilfe vorgegebener Regeln. Das 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.

  Die Kontrolle 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 2.2 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 2.2 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.

7. Passen Sie im Block **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 ihrer Reputation laut KSN.

     Ist das Kontrollkästchen aktiviert, verbietet Kaspersky Embedded Systems Security 2.2 den Start von Programmen, die laut KSN nicht vertrauenswürdig sind. Hierbei greifen die Erlaubnisregeln für die Kontrolle des Programmstarts, welche laut KSN zu den nicht vertrauenswürdigen Programmen gehören, nicht. Die Aktivierung des Kontrollkästchens gewährleistet zusätzlichen Schutz vor Schadsoftware.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security 2.2 die Reputation von Programmen, die laut KSN nicht vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die sich auf diese Programme erstrecken.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - **Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben**.

     Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß ihrer Reputation laut KSN.

     Ist das Kontrollkästchen aktiviert, erlaubt Kaspersky Embedded Systems Security 2.2 den Start von Programmen, die 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 das Programm von den KSN-Diensten als vertrauenswürdig eingestuft ist, aber von den Regeln für die Kontrolle des Programmstarts verboten ist, wird der Start eines solchen Programms blockiert.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security 2.2 die Reputation von Programmen, die laut KSN vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die sich auf diese Programme erstrecken.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - Benutzer und/oder Benutzergruppen, denen der Start von Programmen, die laut KSN vertrauenswürdig sind, erlaubt ist.

8. 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 199).
9. Passen Sie auf der Registerkarte **Aufgabenverwaltung** die geplanten Einstellungen für den Aufgabenstart an (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite 130).
10. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung gespeichert.

Über die Kontrolle für Installationspakete

Das Erstellen von Regeln für die Kontrolle des Programmstarts kann kompliziert sein, wenn Sie auf einem geschützten Computer außerdem die Kontrolle für Installationspakete berücksichtigen müssen. Dies ist zum Beispiel für Computer der Fall, auf denen installierte Software regelmäßig automatisch aktualisiert wird. In diesem Fall ist es erforderlich, die Liste der Erlaubnisregeln nach jedem Software-Update zu aktualisieren, damit neu erstellte Dateien in den Einstellungen der Aufgabe "Kontrolle des Programmstarts" berücksichtigt werden. Um die Startkontrolle bei Installationspakete-Szenarien zu vereinfachen, können Sie das Untersystem "Kontrolle des Programmstarts" verwenden.

Ein *Installationspaket* (auch "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 die Dekomprimierung dieses vertrauenswürdigen Pakets und den automatischen Start der Software, die von einem vertrauenswürdigen Paket erstellt oder modifiziert wird. Die extrahierten Dateien können das Attribut "Vertrauenswürdig" von einem primären Installationspaket erben. Ein *primäres Installationspaket* 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 2.2 kontrolliert nur vollständige Zyklen von Installationspaketen. Das Programm kann den Anfang 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 "Kontrolle des Programmstarts" deaktiviert ist.

Cache für Softwareverteilung

Kaspersky Embedded Systems Security 2.2 stellt mithilfe des dynamisch generierten *Caches für Installationspakete* (auch "Installations-Cache" genannt) eine Verbindung zwischen vertrauenswürdigen Paketen und Dateien her, die während des Installationsverfahrens erstellt wurden. Bei der ersten Ausführung des Pakets ermittelt Kaspersky Embedded Systems Security 2.2 alle Dateien, die während des Installationsverfahrens von diesem Paket erstellt wurden, und speichert die Prüfsummen und Pfade der Dateien im Installations-Cache. Anschließend ist das Ausführen aller Dateien, die im Installations-Cache gespeichert sind, standardmäßig erlaubt.

Sie können den Installations-Cache nicht über die Benutzeroberfläche überprüfen, löschen oder modifizieren. Der Cache wird von Kaspersky Embedded Systems Security 2.2 mit Daten gefüllt und kontrolliert.

Sie können den Installations-Cache in die Konfigurationsdatei exportieren (im xml-Format) und den Cache außerdem über die Befehlszeile löschen.

► *Um den Installations-Cache in eine Konfigurationsdatei zu exportieren, geben Sie folgenden Befehl ein:*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

► *Um den Installations-Cache zu löschen, geben Sie folgenden Befehl ein:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 2.2 aktualisiert den Installations-Cache alle 24 Stunden. Wenn der vollständige Pfad oder die Prüfsumme einer Datei, die zuvor zulässig war, geändert wird, wird der Datensatz dieser Datei vom Programm aus dem Installations-Cache gelöscht. Wenn die Aufgabe zur Kontrolle des Programmstarts im Modus Aktiv gestartet wurde, werden weitere Ausführungsversuche dieser Datei unterbunden.

Verarbeitung extrahierter Dateien

Beim ersten Start des Pakets wird das Attribut "Vertrauenswürdig" an alle extrahierten Dateien des vertrauenswürdigen Pakets vererbt. Wenn Sie das Kontrollkästchen nach dem ersten Start deaktivieren, behalten die geerbten Attribute aller extrahierten Dateien dieses Pakets weiterhin ihre Gültigkeit. Um eine bereits erfolgte Vererbung für alle extrahierten Dateien zurückzusetzen, müssen Sie den Installations-Cache löschen und das Kontrollkästchen **Den 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 primären Installationspaket erstellt wurden, erhalten das Attribut "Vertrauenswürdig", indem ihre Prüfsummen beim ersten Start des Installationspakets aus 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 für die Vererbung des Attributs "Vertrauenswürdig" nicht begrenzt.

Extrahierte Dateien behalten auch nach dem Neustart des Betriebssystems das Attribut "Vertrauenswürdig" bei.

Die Verarbeitung von Dateien wird in den Einstellungen der Überwachung von Installationspaketen angepasst (siehe Abschnitt "Konfiguration der Kontrolle für Installationspakete" auf S. 199). Aktivieren oder deaktivieren Sie dazu das Kontrollkästchen **Den Start von Dateien in allen Ebenen dieses Installationspakets erlauben**.

Angenommen, Sie fügen das Paket test.msi, das einige andere Pakete und Programme enthält, zur Ausnahmenliste 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 Ausnahmenliste hinzufügen und das Kontrollkästchen **Den Start von Dateien in allen Ebenen dieses Installationspakets erlauben** deaktivieren, weist das Programm das Attribut "Vertrauenswürdig" 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.

Interaktion 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 zur 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

Als "nicht vertrauenswürdig" bewertete KSN-Einstufungen haben eine höhere Priorität als die Ausnahmen bezüglich der Kontrolle für Installationspakete: Das Dekomprimieren eines vertrauenswürdigen Pakets oder das Ausführen von Dateien, die von diesem Paket erstellt oder modifiziert wurden, werden blockiert, wenn KSN eine als "nicht vertrauenswürdig" bewertete Einstufung für diese Dateien erhält.

Konfiguration der Kontrolle für Installationspakete

► *Um ein vertrauenswürdiges Installationspaket hinzuzufügen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Kontrolle des Programmstarts**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.
4. Aktivieren Sie auf der ausgewählten Registerkarte 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** in den Einstellungen der Aufgabe zur **Kontrolle des Programmstarts** aktiviert ist.

5. 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 des Subsystems Windows Installer gestartet werden, automatisch zu erstellen.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt das Programm immer den Start von Dateien, die von Windows Installer installiert wurden.

   Wenn das Kontrollkästchen deaktiviert ist, ist die Verwendung von Windows Installer für den Start des Programms kein Kriterium dafür, dass das Programm erlaubt wird.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Dieses Kontrollkästchen kann nicht bearbeitet werden, wenn das Kontrollkästchen **Verteilung von gelisteten Installationspaketen automatisch erlauben** deaktiviert ist.

Das Kontrollkästchen **Verteilung von Programmen mithilfe von Windows Installer immer erlauben** sollte nur deaktiviert werden, wenn dies absolut notwendig ist. Das Deaktivieren dieses Kontrollkästchens kann zu Problemen beim Update der Dateien des Betriebssystems führen und den Start von Dateien verbieten, die aus einem Installationspaket extrahiert wurden.

6. 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 2.2 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.

7. Um die Liste der vertrauenswürdigen Installationspakete zu bearbeiten, klicken Sie auf die Schaltfläche **Liste der Pakete bearbeiten** und wählen Sie im folgenden Menü 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**

          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 empfiehlt sich, wenn Sie den Start beliebiger Programme erlauben möchten, die im Betriebssystem als vertrauenswürdig eingestuft sind.

        - **SHA256-Hash verwenden**

          Wenn diese Option ausgewählt ist, wird in den Parametern 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 den angegebenen Werten der Prüfsumme.

          Diese Option wird empfohlen, wenn maximal sichere Regeln erstellt werden müssen: Die Prüfsumme, die nach dem Algorithmus SHA256 berechnet wird, ist eine eindeutige ID der Datei. Die Verwendung der erhaltenen SHA256-Prüfsumme als Auslösekriterium für die Regel engt den Gültigkeitsbereich der Regel bis auf eine Datei ein.

          Diese Variante gilt als Standard.

   - **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 2.2 untersucht den Hash und erlaubt dem Betriebssystems 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 gespeicherten Konfigurationsdatei importieren. Die von Kaspersky Embedded Systems Security 2.2 erkannte Datei muss folgende Voraussetzungen erfüllen:

  - Die Datei muss über eine Texterweiterung verfügen.
  - 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>:<Hash SHA256>.
    - <Hash SHA256>*<Dateiname>

  Geben Sie im Fenster **Öffnen** die Konfigurationsdatei mit der Liste der vertrauenswürdigen Installationspakete an.

8. 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.

9. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Aktivierung des Standarderlaubnismodus

Der Standarderlaubnismodus erlaubt den Start aller Programme, sofern sie nicht durch Regeln verboten oder von KSN als "nicht vertrauenswürdig" bewertet sind. Der Standarderlaubnismodus kann durch Hinzufügen bestimmter Erlaubnisregeln aktiviert werden. Sie können den Standarderlaubnismodus nur für Skripte oder für alle ausführbare Dateien aktivieren.

► *Um eine Standarderlaubnisregel hinzuzufügen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Kontrolle des Programmstarts**.
4. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.
5. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche die Option **Eine Regel hinzufügen**.

   Es öffnet sich das Fenster **Einstellungen der Regel**.
6. Geben Sie im Feld **Name** den Namen der Regel an.
7. Wählen Sie in der Dropdown-Liste **Typ** den Regeltyp **Erlaubnis**.
8. 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.
9. Wählen Sie im Block **Auslösekriterien für Regeln** eine Option für den **Dateipfad**.
10. Geben Sie die folgende Maske ein: **?:**
11. Klicken Sie im Fenster **Einstellungen der Regel** auf **OK**.

Kaspersky Embedded Systems Security 2.2 übernimmt den Standarderlaubnismodus.

Über die Erstellung von Regeln für die Kontrolle des Programmstarts für das gesamte Netzwerk über Kaspersky Security Center

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 empfiehlt sich, wenn sich im Unternehmensnetzwerk keine Referenzcomputer befinden und Sie keine Möglichkeit haben, mithilfe der Aufgabe zur automatischen Generierung von Erlaubnisregeln anhand der auf einem solchen Referenzcomputer installierten Programme eine allgemeine Regelliste zu erstellen.

Die Komponente zur Kontrolle des Programmstarts wird mit zwei vordefinierten Erlaubnisregel installiert:

- Erlaubnisregel für Skripte und MSI mit einem vom Betriebssystem als vertrauenswürdig eingestuften Zertifikat.
- Erlaubnisregel für ausführbare Dateien mit einem vom Betriebssystem als vertrauenswürdig eingestuften Zertifikat.

Sie können Listen mit Regeln für die Kontrolle des Programmstarts in der Konsole von Kaspersky Security Center auf zwei Arten erstellen:

- Mithilfe der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" für die Kontrolle des Programmstarts.

  Bei Verwendung dieser Option erstellt die Gruppenaufgabe für jeden Computer im Netzwerk eine eigene Liste der Regeln für die Kontrolle des Programmstarts und speichert diese Listen in der angegebenen Netzwerkfreigabe in Form einer XML-Datei. Danach können Sie die erstellten Listen mit Regeln manuell in die Aufgabe Kontrolle des Programmstarts in der Richtlinie von Kaspersky Security Center importieren. Sie können eine Richtlinie von Kaspersky Security Center so konfigurieren, dass die erstellten Regeln nach Abschluss der Gruppenaufgabe zum automatischen Erstellen von Erlaubnisregeln automatisch zur Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt werden.

  Es wird empfohlen, diese Option zu verwenden, wenn die kurzfristige Erstellung von Listen mit Regeln für die Kontrolle des Programmstarts erforderlich ist. Es wird empfohlen, den Start der Aufgabe "Automatisches Erstellen von Erlaubnisregeln" nur dann einzurichten, wenn der Gültigkeitsbereich der Erlaubnisregeln Ordner mit zweifelsfrei sicheren Dateien enthält.

  Stellen Sie bei der Übernahme der Richtlinie für die Kontrolle des Programmstarts im Netzwerk sicher, dass für alle geschützten Computer der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Anwendung der Netzwerkfreigabe in der Arbeit der Computer im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Computer-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

- Auf Grundlage des Ereignisberichts für die Aufgabe, der in Kaspersky Security Center anhand der Ausführung der Aufgabe "Kontrolle des Programmstarts" im Modus **Nur Statistik** erstellt wird.

  Bei Verwendung dieses Szenarios verbietet Kaspersky Embedded Systems Security 2.2 Programmstarts nicht, registriert jedoch im Abschnitt **Ereignisse** von Kaspersky Security Center alle erlaubten und verbotenen Programmstarts auf allen Computern des Netzwerks während der Ausführung der Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik**. Kaspersky Security Center erstellt auf der Grundlage des Protokolls über Aufgabenausführung eine einheitliche Liste der Ereignisse aufgrund von verbotenen Programmstarts.

  Sie müssen den Zeitraum für die Ausführung der Aufgabe so konfigurieren, dass während des Zeitraums alle möglichen Betriebsszenarien und mindestens ein Neustart der geschützten Computer und Computergruppen ausgeführt werden. Danach können Sie beim Hinzufügen von Regeln zur Aufgabe zur Kontrolle des Programmstarts Daten über Programmstarts aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (im Format TXT) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle des Starts der betreffenden Programme erstellen.

  Dieses Szenario wird empfohlen, wenn das Netzwerk des Unternehmens eine große Anzahl an Computern verschiedener Typen (siehe Abschnitt "Über die Verwendung von Profilen bei der Konfiguration der Aufgabe zur Kontrolle des Programmstarts in der Richtlinie von Kaspersky Security Center" auf S. 190) (mit unterschiedlichen Zusammenstellungen installierter Programme) enthält.

- Auf Grundlage der Ereignisse über den verbotenen Start von Programmen, die über Kaspersky Security Center erhalten wurden, ohne Erstellen und Importieren der Konfigurationsdatei.

  Um die vorliegende Möglichkeit zu nutzen, muss sich die 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, die Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts oder die Richtlinie zur Kontrolle des Programmstarts im Modus **Nur Statistik** zu verwenden, die auf Computern der Test-Administrationsgruppe ausgeführt werden, um eine aktualisierte Regelliste zu erstellen. Die Test-Administrationsgruppe beinhaltet Computer, die für den probeweisen Start der neuen Programme vor deren Installation auf den Computern des Netzwerks erforderlich sind.

Bevor Sie Erlaubnisregeln hinzufügen, wählen Sie einen der verfügbaren Modi zur Anwendung der Regeln aus (siehe Abschnitt "Aufgabe Kontrolle des Programmstarts konfigurieren" auf Seite 192). In der Regelliste der Richtlinie für Kaspersky Security Center werden nur jene Regeln angezeigt, die in dieser Richtlinie festgelegt sind, unabhängig vom Modus der Regelanwendung. In der Regelliste des lokalen Computers werden alle angewendeten Regeln angezeigt – sowohl lokale als auch durch die Richtlinie hinzugefügte.

In diesem Abschnitt

Erlaubnisregeln aus Ereignissen in Kaspersky Security Center erstellen

► *Um Erlaubnisregeln mithilfe der Option "Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center erstellen" zu erstellen, gehen Sie in den Einstellungen der Richtlinie zur Kontrolle des Programmstarts wie folgt vor:*

1. Öffnen Sie in der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Öffnen Sie die Administrationsgruppe, deren Richtlinieneinstellungen Sie anpassen möchten, und wählen Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.
3. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.

   Das Fenster **Eigenschaften: <Richtlinienname>** wird geöffnet.
4. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Kontrolle des Programmstarts**.
5. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.
6. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center erstellen**.

7. 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.

8. Passen Sie die folgenden Einstellungen für Anfragen an:

   - **Adresse des Administrationsservers**
   - **Port**
   - **Benutzer**
   - **Kennwort**

9. Wählen Sie die Ereignistypen aus, auf deren Grundlage Sie die Aufgabe erstellen möchten:

   - **Modus "Nur Statistik" Programmstart verboten**
   - **Programmstart verboten**

10. Wählen Sie den Zeitraum aus der Dropdown-Liste **In diesem Zeitraum erstellte Ereignisse anfordern**.
11. Klicken Sie auf die Schaltfläche **Regeln erstellen**.
12. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Kontrolle des Programmstarts**.

    Die Liste der Regeln in der Richtlinie zur Kontrolle des Programmstarts wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des Computers mit der installierten Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

    Wenn die Liste der Regeln für die Kontrolle des Programmstarts bereits in der Richtlinie festgelegt ist, fügt Kaspersky Embedded Systems Security 2.2 die ausgewählten Regeln aus den Blockierungsereignissen zu den schon angegebenen Regeln hinzu. Regeln mit identischem Hash werden nicht hinzugefügt, da alle Regeln in der Liste eindeutig sein müssen.

Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren

Sie können Berichte, die bei der Ausführung der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" erstellt wurden, importieren und als Liste mit Erlaubnisregeln in der konfigurierten Richtlinie verwenden.

Nach Abschluss der Gruppenaufgabe für die automatische Erstellung von Erlaubnisregeln exportiert das Programm die erstellten Erlaubnisregeln in Form von XML-Dateien in die Netzwerkfreigabe. Jede Datei mit einer Regelliste wird auf Grundlage einer 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 Erlaubnisregeln" gemachten Angaben entspricht.

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Embedded Systems Security 2.2 in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Programmkonsole. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Embedded Systems Security 2.2*.

► *Gehen Sie wie folgt vor, um Erlaubnisregeln zur Kontrolle des Programmstarts für Computergruppen auf Grundlage einer automatisch erstellten Liste von Erlaubnisregeln festzulegen.*

1. Erstellen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Computergruppe die Gruppenaufgabe Automatisches Erstellen von Erlaubnisregeln oder wählen Sie eine bereits erstellte Aufgabe aus.
2. Konfigurieren Sie in den Eigenschaften der erstellten Gruppenaufgabe für die automatische Erstellung von Erlaubnisregeln 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 den Bestand 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 Aktionen der Aufgabe während ihrer Ausführung und nach ihrem Abschluss fest. Geben Sie die Kriterien an, auf deren Grundlage die Regeln erstellt werden sollen, sowie den Namen der Datei, in welche die 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 2.2 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 zur automatischen Erstellung von Erlaubnisregeln aus und klicken Sie auf **Starten**, um die Aufgabe zu starten.

   Nach Abschluss der Aufgabe werden die automatisch erstellten Listen mit Erlaubnisregeln in Form von XML-Dateien in der Netzwerkfreigabe gespeichert.

Stellen Sie bei der Übernahme der Richtlinie für die Kontrolle des Programmstarts im Netzwerk sicher, dass für alle geschützten Computer der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Anwendung der Netzwerkfreigabe in der Arbeit der Computer im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Computer-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

4. Fügen Sie die erstellten Listen mit Erlaubnisregeln der Aufgabe zur Kontrolle des Programmstarts hinzu. Gehen Sie dazu in den Eigenschaften der zu konfigurierenden 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 **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 Erlaubnisregeln 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 für die Aufgabenausführung **Aktiv** 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. Für diese Computer erlaubt das Programm nur den Start derjenigen Programme, für die Erlaubnisregeln erstellt wurden.

Import von Regeln aus einer Berichtsdatei von Kaspersky Security Center über blockierte Programme

Sie können Daten über blockierte Programmstarts aus dem 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 über blockierte Programme aus einem Bericht in die Richtlinieneinstellungen davon, dass die verwendete Liste nur diejenigen Programme beinhaltet, deren Start Sie erlauben möchten.

► *Gehen Sie wie folgt vor, um Erlaubnisregeln zur Kontrolle des Programmstarts für Computergruppen auf Grundlage eines Berichts aus Kaspersky Security Center über die gesperrten Programme festzulegen:*

1. Wählen Sie in den Richtlinieneigenschaften in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts den Modus **Nur Statistik** aus.
2. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisse**, dass:
   - auf der Registerkarte **Kritische Ereignisse** für das Ereignis "Programmstart verboten" eine Dauer für die Speicherung des Ereignisses festgelegt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage),
   - auf der Registerkarte **Warnung** für das Ereignis *Nur Statistik: Programmstart verboten* eine Dauer für die Speicherung des Ereignisses festgelegt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage)

   Nach Ablauf des unter **Speicherdauer** angegebenen Zeitraums werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in die Protokolldatei aufgenommen. Vergewissern Sie sich vor dem Start der Aufgabe Kontrolle des Programmstarts im Modus **Nur Statistik**, dass die Ausführungsdauer der Aufgabe die festgelegte Speicherzeit für die angegebenen Ereignisse nicht überschreitet.
3. Exportieren Sie nach Abschluss der Aufgabe die protokollierten Ereignisse in eine TXT-Datei:
   a. Erweitern Sie dazu in den Eigenschaften der Aufgabe zur Kontrolle des Programmstarts den Knoten **Protokolle und Benachrichtigungen**.
   b. Erstellen Sie im untergeordneten Knoten **Ereignisse** 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 erstellten Auswahl auf den Link **Ereignisse exportieren**, um einen Bericht über die blockierten Geräte 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 Programme enthält, deren Start Sie erlauben möchten.
4. 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 **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 welche die Ereignisse aus dem Bericht über die gesperrten Programmstarts 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.

Verwaltung von Geräteverbindungen über Kaspersky Security Center

Sie können die Verbindung von Flash-Laufwerken und anderen Massenspeichern zu allen Computern im Netzwerk erlauben oder verbieten, indem Sie einheitliche Listen mit den Regeln für die Computer-Kontrolle auf Seiten Kaspersky Security Center für Computergruppen erstellen.

In diesem Abschnitt

Über die Aufgabe Gerätekontrolle

Kaspersky Embedded Systems Security 2.2 kontrolliert die Registrierung und die Verwendung von Massenspeichern 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 Massenspeicher ist ein externes Gerät, das zum Zweck des Kopierens und Speicherns von Daten mit einem Computer verbunden werden kann.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 "Gerätekontrolle" gestartet wurde, prüft Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 während der Erstellung von Regeln automatisch bestimmt.

Die Aufgabe Gerätekontrolle kann in einem der folgenden beiden Modi ausgeführt werden:

- **Aktiv**. Kaspersky Embedded Systems Security 2.2 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 2.2 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 über Ausgabenausführung. Die Verwendung aller externen Geräte wird erlaubt. Dieser Modus ist standardmäßig eingestellt.

  Sie können diesen Modus für die Erstellung von Regeln aufgrund von Informationen, die während der Aufgabenausführung aufgezeichnet wurden, verwenden.

Über die Erstellung von Regeln zur Gerätekontrolle für das gesamte Netzwerk über 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 zur Gerätekontrolle auf der Seite von Kaspersky Security Center auf zwei 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 2.2 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 in die Eigenschaften der Richtlinie Gerätekontrolle manuell 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 zur Gerätekontrolle nach Abschluss der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" einrichten.

  Es wird empfohlen, diese Option für die Erstellung einer Liste mit Erlaubnisregeln vor dem ersten Start der Richtlinie Gerätekontrolle im Modus der aktiven 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 Anwendung der Netzwerkfreigabe in der Arbeit der Computer im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Computer-Kontrolle auf einem Test- oder 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 2.2 den Anschluss der Massenspeichergeräte nicht, protokolliert aber im Abschnitt **Ereignisse** von Kaspersky Security Center alle Verbindungs- und Registrierungsversuche von Massenspeichergeräten auf allen Netzwerkcomputern während der Ausführung der Aufgabe zur Gerätekontrolle im Modus **Nur Statistik**. Daraufhin erstellt Kaspersky Security Center auf Grundlage des Protokolls über Aufgabenausführung eine einheitliche Liste der aufgrund von Blockierungen und Geräteverbindungen eingetretenen Ereignisse.

  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 zulässige Regeln 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 mobile Geräte.

- Auf Grundlage der Daten der System-Registry über die angeschlossenen Massenspeichergeräte (mithilfe der Option "Regel auf Grundlage der folgenden Systemdaten erstellen" in den Einstellungen der Richtlinie zur Gerätekontrolle)

  Bei Verwendung dieses Szenarios erstellt Kaspersky Embedded Systems Security 2.2 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 für momentan angeschlossene Geräte berücksichtigen**")

  Bei Verwendung dieses Szenarios erstellt Kaspersky Embedded Systems Security 2.2 die 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 2.2 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.

Erstellen von Regeln aufgrund der Systemdaten der externen Geräte, die an die Netzwerkcomputer angeschlossen sind

Sie können auf der Grundlage von Windows-Daten für alle Massenspeicher Regeln erstellen (siehe Abschnitt "Über die Erstellung von Regeln zur Gerätekontrolle für das gesamte Netzwerk über Kaspersky Security Center" auf Seite 212), 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 **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Richtlinie Gerätekontrolle. 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 für momentan angeschlossene Geräte berücksichtigen** in den Einstellungen der Richtlinie zur Gerätekontrolle und 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 2.2 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.

In diesem Abschnitt

Regeln mithilfe der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen

► *Um Erlaubnisregeln für die Gerätekontrolle mithilfe der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle festzulegen, gehen Sie wie folgt vor.*

1. Erstellen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Computergruppe die Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" oder wählen Sie eine bereits erstellte Aufgabe aus.
2. Konfigurieren Sie in den Eigenschaften der erstellten Gruppenaufgabe für die automatische Erstellung von Erlaubnisregeln oder im Assistenten für neue Aufgaben die folgenden Einstellungen:
   - Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für die Speicherung des Berichts über die Aufgabenausführung.
   - Legen Sie im Abschnitt **Einstellungen** die Aktionen der Aufgabe nach ihrem Abschluss fest. Geben Sie den Namen der Datei an, in die die erstellten Regeln exportiert werden.
   - Konfigurieren Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenstart nach Zeitplan.
3. Wählen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Computergruppe in der Liste der Gruppenaufgaben die erstellte Aufgabe zum Erstellen von Regeln für die Gerätekontrolle und klicken Sie auf **Starten**, um die Aufgabe zu starten.

   Nach Abschluss der Aufgabe werden die automatisch erstellten Listen mit Erlaubnisregeln in Form von XML-Dateien in der Netzwerkfreigabe 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 Anwendung der Netzwerkfreigabe in der Arbeit der Computer im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Computer-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

4. Fügen Sie die erstellten Listen mit Erlaubnisregeln der Aufgabe zur Gerätekontrolle hinzu. Gehen Sie dazu in den Eigenschaften der zu konfigurierenden Richtlinie in den Einstellungen der Aufgabe Gerätekontrolle wie folgt vor:
   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.

   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 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.

d. Wählen Sie im erscheinenden Standardfenster von Windows die XML-Dateien aus, die nach Abschluss der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellt wurden.

e. Klicken Sie auf die Schaltfläche **OK** im Fenster "Regeln für die Gerätekontrolle" und im Fenster **Aufgabeneinstellungen**.

5. Wenn Sie die erstellten Regeln zur 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.

Erlaubnisregeln auf Grundlage der Daten des Systems in der Richtlinie von Kaspersky Security Center erstellen

► *Um die Erlaubnisregeln mithilfe der Option **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Richtlinie "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Wenn es erforderlich ist, schließen Sie an den Computer mit der installierten Verwaltungskonsole für Kaspersky Security Center den neuen Massenspeicher an, dessen Verwendung Sie erlauben möchten.
2. Öffnen Sie in der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
3. Öffnen Sie die Administrationsgruppe, deren Richtlinieneinstellungen Sie anpassen möchten, und wählen Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.
4. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.
5. Das Fenster **Eigenschaften: <Richtlinienname>** wird geöffnet.
6. Öffnen Sie in den Eigenschaften der Richtlinie das Fenster für die Anpassung der Einstellungen der Aufgabe Gerätekontrolle und gehen Sie wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regel auf Grundlage der folgenden Systemdaten erstellen**.

c. Wählen Sie das Prinzip aus, nach dem Erlaubnisregeln zur Liste der bereits festgelegten Regeln für die 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.

7. Klicken Sie auf die Schaltfläche **OK** im Fenster **Regeln für die Gerätekontrolle** und im Fenster **Aufgabeneinstellungen**.

Die Liste der Regeln in der Richtlinie zur 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 **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Richtlinie "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Öffnen Sie die Administrationsgruppe, deren Richtlinieneinstellungen Sie anpassen möchten, und wählen Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.
3. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.
4. Das Fenster **Eigenschaften: <Richtlinienname>** wird geöffnet.
5. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Gerätekontrolle**.
6. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.
7. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Kontextmenü den Punkt **Regeln für momentan angeschlossene Geräte berücksichtigen** aus.

   Das Fenster **Regel auf Grundlage der folgenden Systemdaten erstellen** wird geöffnet.
8. Wählen Sie in der Liste der gefundenen Geräte, die an den geschützten Computer angeschlossen sind, die Geräte aus, für die Sie Erlaubnisregeln erstellen möchten.
9. Klicken Sie auf die Schaltfläche Regel für ausgewählte Geräte **hinzufügen**.
10. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Gerätekontrolle**.

Die Liste der Regeln in der Richtlinie zur Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des Computers mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Import von Regeln aus einer Berichtsdatei von Kaspersky Security Center über blockierte Geräte

Sie können Daten über blockierte Massenspeicher aus dem Bericht importieren, der in Kaspersky Security Center nach der Ausführung der Aufgabe "Gerätekontrolle" im Modus **Nur Statistik** erstellt wurde, 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.

Vergewissern Sie sich beim Import von Daten über blockierte Geräte aus einem Bericht in die Richtlinieneinstellungen davon, dass die verwendete Liste nur diejenigen Geräte beinhaltet, deren Verbindung Sie erlauben möchten.

► *Gehen Sie wie folgt vor, um Erlaubnisregeln zur Gerätekontrolle für Computergruppen auf Grundlage eines Berichts aus Kaspersky Security Center über die blockierten Geräte festzulegen:*

1. Wählen Sie in den Richtlinieneigenschaften in den Einstellungen der Aufgabe "Gerätekontrolle" den Modus **Nur Statistik** aus.
2. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisse**, dass:
   - auf der Registerkarte **Kritische Ereignisse** für das Ereignis *Massenspeicher verboten* eine Dauer für die Speicherung des Ereignisses festgelegt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage),
   - auf der Registerkarte **Warnung** für das Ereignis *Nur Statistik: nicht vertrauenswürdiges Gerät gefunden* eine Dauer für die Speicherung des Ereignisses festgelegt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage).

   Nach Ablauf des unter **Speicherdauer** angegebenen Zeitraums 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.
3. Exportieren Sie nach Abschluss der Aufgabe die protokollierten Ereignisse in eine TXT-Datei. Erweitern Sie hierfür den untergeordneten Knoten **Protokolle** und erstellen Sie im untergeordneten Knoten **Ereignisse** eine Auswahl von Ereignissen anhand der Eigenschaft *Verboten*, um zu sehen, welche Gerätestarts durch die Aufgabe Gerätekontrolle blockiert werden. Klicken Sie im Ergebnisbereich der erstellten Auswahl auf den Link **Ereignisse exportieren**, um einen Bericht über die blockierten Geräte 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.
4. Importieren Sie die Daten über die blockierten Verbindungsversuche der Geräte in die Richtlinie zur Gerätekontrolle. Gehen Sie dazu in den Eigenschaften der Richtlinie in den Einstellungen der Aufgabe Gerätekontrolle wie folgt vor:
   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.
   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 **OK** im Fenster **Regeln für die Gerätekontrolle** und im Fenster **Aufgabeneinstellungen**.

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.

Netzwerküberwachung

Dieser Abschnitt enthält Informationen über die Aufgaben zur Firewall-Verwaltung.

In diesem Kapitel

Firewall-Verwaltung

Dieser Abschnitt informiert über die Aufgabe zur Firewall-Verwaltung und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

Über die Aufgabe zur Firewall-Verwaltung

Kaspersky Embedded Systems Security 2.2 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 2.2 zu verwalten. Während der Ausführung der Aufgabe zur Firewall-Verwaltung übernimmt Kaspersky Embedded Systems Security 2.2 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 2.2 vorgenommen werden.

Wenn die Windows-Firewall bei der Installation von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 Folgendes:

- Status der Funktion der Windows-Firewall.
- Status der Regeln, die nach der Installation von Kaspersky Embedded Systems Security 2.2 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 2.2 einen Satz von Gruppenregeln für Kaspersky Security im **Windows Firewall**-Snap-in. Dieser Regelsatz vereint alle Regeln, die von Kaspersky Embedded Systems Security 2.2 mithilfe der Aufgabe zur Firewall-Verwaltung erstellt werden. 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 2.2 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 zur 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 2.2 alle Erlaubnisregeln für den eingehenden Datenverkehr, die in den Einstellungen der Windows-Firewall festgelegt sind, und kopiert sie in die Einstellungen der Aufgabe zur 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 2.2 diese Regel.
- Wenn in den Einstellungen der Windows-Firewall eine bereits vorhandene Regel gelöscht wird, stellt Kaspersky Embedded Systems Security 2.2 diese Regel wieder her.
- Wenn in den Einstellungen der Windows-Firewall die Einstellungen einer vorhandenen Regel geändert werden, verwirft Kaspersky Embedded Systems Security 2.2 die Änderungen.
- Wenn in den Einstellungen der Aufgabe zur Firewall-Verwaltung eine neue Regel erstellt wird, erzwingt Kaspersky Embedded Systems Security 2.2 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 2.2 das Löschen dieser Regel aus den Einstellungen der Windows-Firewall.

Kaspersky Embedded Systems Security 2.2 funktioniert nicht mit Verbotsregeln sowie mit Regeln, die den ausgehenden Datenverkehr kontrollieren. Zum Zeitpunkt des Starts der Aufgabe zur Firewall-Verwaltung löscht Kaspersky Embedded Systems Security 2.2 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 2.2 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.

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 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Firewall-Verwaltung.**
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Regelliste** wird geöffnet.

5. Wählen Sie je nach Art der Regel, deren Status Sie ändern möchten, die Registerkarte **Programme** oder **Ports** aus.
6. Suchen Sie in der Liste der Regeln die Regel, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:
   - Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird aktiviert.
   - Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird deaktiviert.
7. Klicken Sie im Fenster **Regellise** auf die Schaltfläche **Speichern**.

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 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Firewall-Verwaltung**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Regelliste** wird geöffnet.

5. 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**.

6. 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.

7. Klicken Sie im Fenster **Regel für Programm anpassen** oder **Regel für Port anpassen** auf **OK**.
8. 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. 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Firewall-Verwaltung.**
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Regelliste** wird geöffnet.
5. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
6. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
7. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählte Regel wird gelöscht.
8. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen für die Firewall-Verwaltung werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

System-Diagnose

Dieser Abschnitt enthält Informationen über die Aufgabe zur Überwachung der Datei-Integrität und die Möglichkeiten der Analyse des Systemprotokolls des Betriebssystems.

In diesem Kapitel

Überwachung der Datei-Integrität

Dieser Abschnitt enthält Informationen über den Start und das Anpassen der Aufgabe zur Überwachung der Datei-Integrität.

In diesem Abschnitt

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 geschütztes Gerät nicht physisch auf einem geschützten Computer vorhanden ist. Kaspersky Embedded Systems Security 2.2 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 Speicher 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 vom Überwachungsbereich erstellen (siehe Abschnitt "Einstellungen der Überwachungsregeln anpassen" auf Seite 231). 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 Ereigniskategorie für gefundene Dateioperationen bestimmen, die im Protokoll über 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 Ereigniskategorien 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 2.2 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 über 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 2.2 Dateioperationen findet, die von einem vertrauenswürdigen Benutzer ausgeführt wurden, protokolliert die Aufgabe zur Überwachung der Datei-Integrität ein Informatives Ereignis im Protokoll über Aufgabenausführung.

Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 über Aufgabenausführung.

Datei-Operations-Marker

Während der Ausführung der Aufgabe zur Überwachung der Datei-Integrität ermittelt Kaspersky Embedded Systems Security 2.2 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 Ereigniskategorie der protokollierten Ereignisse hängt nicht von den ausgewählten Datei-Operations-Markern oder ihrer Anzahl ab.

Standardmäßig werden von Kaspersky Embedded Systems Security 2.2 alle verfügbaren Datei-Operations-Marker berücksichtigt. Sie können Datei-Operations-Marker manuell in den Einstellungen der Aufgabenregeln auswählen (s. Tabelle unten).

Tabelle 36. 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

ID der Dateioperation	Datei-Operations-Marker	Unterstützte Dateisysteme
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
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

Aufgabe "Überwachung der Datei-Integrität" anpassen

Sie können die Standard-Einstellungen der Aufgabe Überwachung der Datei-Integrität anpassen (s. Tabelle unten).

Tabelle 37. Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Standardwert	Beschreibung
Überwachungsbereiche	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 Verzeichnissen 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.
Ausgeschlossene Überwachungsbereiche berücksichtigen	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 2.2 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 2.2 ein Systemaudit-Ereignis.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Gehen Sie wie folgt vor, um die Einstellungen der Aufgabe zur Überwachung der Datei-Integrität anzupassen:

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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. Klicken Sie im Abschnitt **System-Diagnose** im Block **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung der Datei-Integrität** wird geöffnet.

4. 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 2.2 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 231) hinzu, die von der Aufgabe überwacht werden sollen.

5. Starten Sie auf der Registerkarte **Aufgabenverwaltung** die Aufgabe auf der Grundlage eines Zeitplans (siehe Abschnitt "Arbeit mit dem Aufgabenzeitplan" auf Seite 130).

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Einstellungen der Überwachungsregeln anpassen

Standardmäßig ist kein Überwachungsbereich angegeben: Die Aufgabe überwacht in keinem einzigen Verzeichnis die Ausführung von Dateioperationen.

► *Um einen Überwachungsbereich hinzuzufügen, 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. 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. 95).

   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. 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.

4. Klicken Sie im Block **Überwachungsbereich** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Überwachungsbereich** wird geöffnet.

5. Fügen Sie den Überwachungsbereich auf eine der folgenden Arten hinzu:

   - Wenn Sie im Standarddialog von Microsoft Windows Ordner auswählen möchten:

     a. Klicken Sie auf **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 Verzeichnis <\dir>
     - <\dir*\name.ext> – alle Dateien mit dem Namen "name" und der Erweiterung <ext> im Verzeichnis <\dir> und allen Unterverzeichnissen

   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 2.2 den angegebenen Überwachungsbereich nicht hinzu.

6. Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

   Das Microsoft-Windows-Standardfenster **Auswählen: Benutzer oder Gruppen** wird geöffnet.

7. 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 2.2 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 227) und erstellt für sie kritische Ereignisse.

8. Wählen Sie die Registerkarte **Datei-Operations-Marker** aus.

9. 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 227) die Kontrollkästchen neben den Operationen, die Sie überwachen möchten.

   Standardmäßig überwacht Kaspersky Embedded Systems Security 2.2 alle verfügbaren Dateioperationen, wenn die Option **Dateioperationen anhand von allen identifizierbaren Markern erkennen** ausgewählt ist.

10. Wenn Sie möchten, dass Kaspersky Embedded Systems Security 2.2 die Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:
    a. Aktivieren Sie im Block **Berechnung der Prüfsumme** das Kontrollkästchen **Prüfsumme der geänderten Datei berechnen, wenn möglich**.

       Wenn das Kontrollkästchen aktiviert ist, ermittelt Kaspersky Embedded Systems Security 2.2 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 2.2 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**

11. 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 227) die Kontrollkästchen neben den Operationen, die Sie überwachen möchten.
12. 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 **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 2.2 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 2.2 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.

13. Klicken Sie im Fenster **Überwachungsbereich** auf **OK**.

    Die angegebenen Einstellungen der Regeln werden im ausgewählten Überwachungsbereich der Aufgabe "Überwachung der Datei-Integrität" gelten.

Protokollanalyse

Dieser Abschnitt enthält Informationen über die Aufgabe zur Protokollanalyse und die Aufgabeneinstellungen.

In diesem Abschnitt

Über die Aufgabe Protokollanalyse

Während der Ausführung der Aufgabe zur Protokollanalyse überwacht Kaspersky Embedded Systems Security 2.2 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 2.2 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
- Verarbeitung der Netzwerkanmeldung

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 2.2 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 über Ausgabenausführung 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 2.2 ein "Kritisches Ereignis" im Protokoll über Ausgabenausführung der Protokollanalyse.

Standardmäßig übernimmt die Aufgabe zur Protokollanalyse keine benutzerdefinierten 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.

Regeln für vorkonfigurierte Aufgaben anpassen

► *Um die vorkonfigurierten Regeln für die Aufgabe zur Protokollanalyse anzupassen, 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

   Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **System-Diagnose** im Block **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Einstellungen der Protokollanalyse** wird geöffnet.
4. Wählen Sie die Registerkarte **Vorkonfigurierte Regeln** aus.
5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Vorkonfigurierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security 2.2 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 2.2 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 ausgewählten Regeln anzupassen, klicken Sie auf die Schaltfläche **Erweiterte Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

8. Geben Sie im Block **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 Block **Netzwerk-Anmeldungserkennung** den Anfang und das Ende der Zeitspanne an, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security 2.2 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 **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**.
13. Die angegebene IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.
14. Passen Sie auf der Registerkarte **Aufgabenverwaltung** den geplanten Aufgabenstart an (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite 130).
15. 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. 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. 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. 95).
   - Um das Programm für einen einzelnen Computer zu konfigurieren, 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 107) .

Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.

3. Klicken Sie im Abschnitt **System-Diagnose** im Block **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

4. Deaktivieren oder aktivieren Sie auf der Registerkarte **Regeln für die Protokollanalyse** das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security 2.2 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 2.2 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 hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regeln für die Protokollanalyse** wird geöffnet.

6. Geben Sie im Block **Allgemein** die folgenden Daten der neuen Regel ein:

   - **Name**
   - **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.

7. Geben Sie im Block **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.

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 2.2 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 107).
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 Verwaltungskonsolenstruktur den Hauptknoten **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 (siehe Abschnitt "Verwaltung des Programmstarts aus Kaspersky Security Center" auf Seite 190) 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 Servern 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 "Aufgabe Kontrolle des Programmstarts konfigurieren" auf Seite 192).
2. Wählen Sie in der Verwaltungskonsolenstruktur den Hauptknoten **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 "Aufgabe Kontrolle des Programmstarts konfigurieren" auf Seite 192).
2. Wählen Sie in der Verwaltungskonsolenstruktur den Hauptknoten **Administrationsserver <Computername>**.
3. Öffnen Sie die Registerkarte **Berichte**.
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.

Arbeiten mit Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile.

In diesem Kapitel

Befehle der Befehlszeile

Sie können die Basisbefehle zur Verwaltung von Kaspersky Embedded Systems Security 2.2 aus der Befehlszeile des geschützten Computers erteilen, wenn Sie bei der Installation von Kaspersky Embedded Systems Security 2.2 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 2.2 zugriffsberechtigt sind.

Bestimmte Befehle von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 ausführen (siehe Tabelle unten).

Tabelle 38. Befehle für Kaspersky Embedded Systems Security 2.2

Befehl	Beschreibung
KAVSHELL APPCONTROL (siehe Abschnitt "Ergänzen der Regelliste für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL" auf Seite 255)	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 252).	Verwaltung des Ausführungsmodus der Aufgabe zur Kontrolle des Programmstarts.
KAVSHELL APPCONTROL /GENEARTE (siehe Abschnitt "Automatisches Erstellen von Erlaubnisregeln. KAVSHELL APPCONTROL /GENERATE" auf Seite 253).	Erstellt eine Aufgabe zum automatischen Erstellen von Erlaubnisregeln für die Kontrolle des Programmstarts.
KAVSHELL VACUUM (siehe Abschnitt "Log-Dateien für Kaspersky Embedded Systems Security 2.2 defragmentieren. KAVSHELL VACUUM" auf S. 264)	Defragmentiert die Log-Dateien für Kaspersky Embedded Systems Security 2.2.
KAVSHELL PASSWORD	Verwaltet die Einstellungen des Kennwortschutzes.
KAVSHELL HELP (siehe Abschnitt "Hilfe für Befehle in Kaspersky Embedded Systems Security 2.2 anzeigen. KAVSHELL HELP" auf S. 244)	Zeigt die Hilfe für Befehle in Kaspersky Embedded Systems Security 2.2 an.
KAVSHELL START (siehe Abschnitt "Kaspersky Security Service starten und anhalten. KAVSHELL START, KAVSHELL STOP" auf Seite 245)	Startet den Dienst von Kaspersky Embedded Systems Security 2.2.
KAVSHELL STOP (siehe Abschnitt "Kaspersky Security Service starten und anhalten. KAVSHELL START, KAVSHELL STOP" auf Seite 245)	Stoppt den Dienst von Kaspersky Embedded Systems Security 2.2.
KAVSHELL SCAN (siehe Abschnitt "Ausgewählten Bereich untersuchen. KAVSHELL SCAN" auf Seite 245)	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 S. 249)	Startet die Systemaufgabe Untersuchung wichtiger Bereiche.
KAVSHELL TASK (siehe Abschnitt "Angegebene Aufgabe asynchron verwalten. KAVSHELL TASK" auf Seite 250)	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 251)	Startet oder beendet alle Echtzeitschutz-Aufgaben.
KAVSHELL UPDATE (siehe Abschnitt "Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security 2.2 starten. KAVSHELL UPDATE" auf S. 257)	Startet die Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security 2.2 mit den festgelegten Befehlszeilenparametern.

Befehl	Beschreibung
KAVSHELL ROLLBACK (siehe Abschnitt "Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK" auf S. 260)	Kehrt zur vorherigen Version der Datenbanken zurück.
KAVSHELL LICENSE (siehe Abschnitt "Programm aktivieren. KAVSHELL LICENSE" auf Seite 261)	Verwaltet Schlüssel.
KAVSHELL TRACE (siehe Abschnitt "Protokoll zur Ablaufverfolgung aktivieren, anpassen und deaktivieren. KAVSHELL TRACE" auf S. 262)	Aktiviert oder deaktiviert das Führen des Protokolls zur Ablaufverfolgung, Verwalten der Parameter für das Protokolls zur Ablaufverfolgung.
KAVSHELL DUMP (siehe Abschnitt "Anlegen von Dump-Dateien ein- und ausschalten. KAVSHELL DUMP" auf Seite 265)	Aktiviert bzw. deaktiviert die Erstellung von Dump-Dateien für Prozesse von Kaspersky Embedded Systems Security 2.2 bei einem Absturz von Prozessen.
KAVSHELL IMPORT (siehe Abschnitt "Einstellungen importieren. KAVSHELL IMPORT" auf S. 267)	Importiert die allgemeinen Einstellungen, Funktionen und Aufgaben für Kaspersky Embedded Systems Security 2.2 aus einer zuvor erstellten Konfigurationsdatei.
KAVSHELL EXPORT (siehe Abschnitt "Einstellungen exportieren. KAVSHELL EXPORT" auf S. 267)	Exportiert alle Einstellungen und vorhandene Aufgaben von Kaspersky Embedded Systems Security 2.2 in eine Konfigurationsdatei.
KAVSHELL DEVCONTROL (siehe Abschnitt "Liste der Regeln für die Gerätekontrolle ergänzen. KAVSHELL DEVCONTROL" auf S. 256)	Ergänzt die Liste der erstellten Regeln für die Gerätekontrolle entsprechend dem ausgewählten Prinzip für das Hinzufügen.

Hilfe für Befehle in Kaspersky Embedded Systems Security 2.2 anzeigen. KAVSHELL HELP

Um eine Liste aller Befehle für Kaspersky Embedded Systems Security 2.2 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 über 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 S. 250).

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 über Ausgabenausführung>] [/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 39. 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 2.2 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 2.2 die Objekte nach Format.	
/FA	Alle Objekte untersuchen.
/FC	Objekte, die nach Format untersucht werden (Standard). Kaspersky Embedded Systems Security 2.2 untersucht nur Objekte, die dem Format nach als infizierbar gelten.
/FE	Objekte nach Erweiterung untersuchen. Kaspersky Embedded Systems Security 2.2 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 2.2 alle Objekte.
/AI: **Aktion für infizierte und andere Objekte**. Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Embedded Systems Security 2.2 die Aktion **Überspringen** aus.	
DISINFECT	Desinfizieren, irreparable Objekte überspringen
DISINFDEL	Desinfizieren, irreparable Objekte überspringen
DELETE	Löschen Die Einstellungen DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 die Aktion **Überspringen** aus.	
QUARANTINE	Quarantäne
DELETE	Löschen
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen

Schlüssel	Beschreibung
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 überschreitet, von Untersuchung ausschließen. Kaspersky Embedded Systems Security 2.2 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 heuristischen 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 2.2 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 2.2 einmalig sein. Wenn dieser Schlüssel nicht vorgegeben ist, erhält die Aufgabe den alternativen Name scan_<kavshell_pid> (z.B. scan_1234). In der Programm-Konsole 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 Ausgabenausführung (Report settings)	

Schlüssel	Beschreibung
/W:<Name des Protokolls über Ausgabenausführung >	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Embedded Systems Security 2.2 das Protokoll über Ausgabenausführung 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 Bericht werden die Ereignisse aufgezeichnet, die durch die Einstellungen für das Protokoll über Ausgabenausführung und den Ereignisbericht von Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung" der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung 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 der Protokoll über Ausgabenausführung 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 über Ausgabenausführung>]
```

Beispiele für den Befehl KAVSHELL SCANCRITICAL

Um die Aufgabe zur Untersuchung auf Befehl Untersuchung wichtiger Bereiche auszuführen und das Protokoll über Ausgabenausführung 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 über Ausgabenausführung je nach Syntax des Schlüssels /W einstellen (s. Tabelle unten).

Tabelle 40. Syntax des Schlüssels /W des Befehls KAVSHELL SCANCRITICAL

Schlüssel	Beschreibung
/W:<Name des Protokolls über Ausgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Embedded Systems Security 2.2 das Protokoll über Ausgabenausführung 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 Bericht werden die Ereignisse aufgezeichnet, die durch die Parameter für das Protokoll über Ausgabenausführung und den Ereignisbericht des Programms in der Konsole "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 über Ausgabenausführung** der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security 2.2 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 aktuellen 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 41. Schlüssel des Befehls KAVSHELL TASK

Schlüssel	Beschreibung
Ohne Schlüssel	Gibt eine Liste aller vorhandenen Serveraufgaben in Kaspersky Embedded Systems Security 2.2 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 2.2 an Aufgaben vergibt. Um die alternativen Namen der Aufgaben von Kaspersky Embedded Systems Security 2.2 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.

Rückgabecodes für den Befehl KAVSHELL TASK (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TASK" auf Seite 270)

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 42. 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 43. 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.

Schlüssel	Beschreibung
/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 Erlaubnisregeln. 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 44. Schlüssel des Befehls KAVSHELL APPCONTROL/GENERATE

Schlüssel	Beschreibung
Gültigkeitsbereich der Regeln mit dem Status "erlaubt"	
<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.

Schlüssel	Beschreibung
/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 Verarbeitungsbereich der zu erstellenden 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 der automatischen Erstellung von Erlaubnisregeln	
/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 45. 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 46. 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 2.2 starten. KAVSHELL UPDATE

Mit dem Befehl `KAVSHELL UPDATE` können Sie die Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security 2.2 im Synchronmodus starten.

Die Aufgabe zum Datenbanken-Update von Kaspersky Embedded Systems Security 2.2, die mit dem Befehl `KAVSHELL UPDATE` gestartet wird, ist temporär. Sie wird nur während ihrer Ausführung in der Programmkonsole angezeigt. Das Protokoll über Ausgabenausführung wird gleichzeitig erzeugt. Es wird in den **Protokollen über 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 2.2 auf Computer mithilfe der Anwendung Kaspersky Security Center verwaltet wird, finden Sie im Abschnitt "Verwaltung von Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung>] [/ALIAS:<Alias des Aufgabennamens>]
```

Der Befehl KAVSHELL UPDATE enthält sowohl obligatorische als auch Reserveschlüssel, deren Verwendung optional ist (s. Tabelle unten).

Beispiele für den Befehl KAVSHELL UPDATE

► *Um eine benutzerdefinierte Aufgabe zum Datenbanken-Update zu starten, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE
```

► *Um eine Aufgabe zum Datenbanken-Update 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
```

► *Um die Datenbanken-Updates von Kaspersky Embedded Systems Security 2.2 vom Update-Computer von Kaspersky Lab zu erhalten und die Verbindung mit der Update-Quelle über einen Proxyserver herzustellen (Proxyserver-Adresse: proxy.company.com, Port: 8080) sowie zur Verwendung der integrierten Authentizitätsprüfung von Microsoft Windows (NTLM-authentication) für den Computerzugriff führen Sie unter dem Benutzerkonto (Benutzername: inetuser, Kennwort: 123456) folgenden Befehl aus:*

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

Tabelle 47. Schlüssel des Befehls KAVSHELL UPDATE

Schlüssel	Beschreibung
Update-Quelle (obligatorischer Schlüssel). Geben Sie eine oder mehrere Quellen an. Kaspersky Embedded Systems Security 2.2 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.
<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 2.2 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 2.2 greift unter dem Benutzerkonto **Lokales System** (**SYSTEM**) auf den Proxyserver zu; **1** – integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Embedded Systems Security 2.2 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.

Schlüssel	Beschreibung
/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 2.2 den FTP-Computer im aktiven Modus für eine Verbindung zum geschützten Computer. Wenn dieser Schlüssel nicht angegeben ist, verwendet Kaspersky Embedded Systems Security 2.2 nach Möglichkeit den passiven Modus des FTP-Computers.
/TIMEOUT:<Anzahl der Sekunden>	Wartezeit für Verbindung mit einem FTP- oder HTTP-Server. Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Embedded Systems Security 2.2 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 2.2 optimiert den Update-Download auf den geschützten Computer, indem der geografisch am nächsten liegenden Update-Computer 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 2.2 den Ort des geschützten Computers entsprechend den regionalen Einstellungen des Computers auf dem die Programmkonsole installiert ist.

Schlüssel	Beschreibung
/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 2.2 einmalig sein. Wenn dieser Schlüssel nicht angegeben wird, erhält die Aufgabe den Alias update_<kavshell_pid> (z.B. update_1234) In der Programm-Konsole 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 über Ausgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Embedded Systems Security 2.2 das Protokoll über Ausgabenausführung 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 Bericht werden die Ereignisse aufgezeichnet, die durch die Einstellungen für das Protokoll über Ausgabenausführung und den Ereignisbericht von Kaspersky Embedded Systems Security 2.2 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 über Ausgabenausführung** der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security 2.2 keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen oder es erfolgt aber eine Fehlermeldung.

Rückgabecodes für den Befehl KAVSHELL UPDATE (auf S. 271)

Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK

Mit dem Befehl `KAVSHELL ROLLBACK` können Sie die Systemaufgabe Rollback des Datenbank-Updates von Kaspersky Embedded Systems Security 2.2 ausführen. Dadurch werden die Datenbanken von Kaspersky Embedded Systems Security 2.2 mit den zuvor installierten Updates wiederhergestellt. Der Befehl wird synchron ausgeführt.

Syntax des Befehls

```
KAVSHELL ROLLBACK
```

Rückgabecodes für den Befehl KAVSHELL ROLLBACK (auf S. 271)

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 48. 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 270).

Programm aktivieren. KAVSHELL LICENSE

Mit dem Befehl `KAVSHELL LICENSE` können Sie in Kaspersky Embedded Systems Security 2.2 Schlüssel und Aktivierungscodes verwalten.

> 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 LICENSE

```
KAVSHELL LICENSE [/ADD:<Schlüsseldatei | Aktivierungscode> [/R] | /DEL:<Schlüssel | Nummer des Aktivierungscodes>]
```

Beispiele für den Befehl KAVSHELL LICENSE

► *Führen Sie zur Programmaktivierung den folgenden Befehl aus:*

```
KAVSHELL.EXE LICENSE / ADD: <Aktivierungscode oder Schlüssel>
```

► *Um Informationen über die hinzugefügten Schlüssel zu erhalten, führen Sie folgenden Befehl aus:*

```
KAVSHELL LICENSE
```

► *Um einen hinzugefügten Schlüssel mit der Nummer 0000-000000-00000001 zu entfernen, führen Sie folgenden Befehl aus:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

Der Befehl `KAVSHELL LICENSE` kann sowohl mit als auch ohne Schlüssel ausgeführt werden (s. Tabelle unten).

Tabelle 49. Schlüssel des Befehls KAVSHELL LICENSE

Schlüssel	Beschreibung
Ohne Schlüssel	Der Befehl gibt folgende Informationen über die hinzugefügten Schlüssel zurück: • Schlüssel. • Lizenztyp (kommerziell). • Gültigkeitsdauer der Lizenz, die zum Schlüssel gehört. • Status des Schlüssels (aktiv oder Reserve) Wenn der Wert * angegeben ist, wurde der Schlüssel als Reserveschlüssel hinzugefügt.
/ADD:<Name der Schlüsseldatei oder Aktivierungscode>	Fügt den Schlüssel mithilfe der angegebenen Datei oder des Aktivierungscodes hinzu. Wenn Sie den Pfad einer Schlüsseldatei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable sind dagegen nicht zugelassen.
/R	Der Aktivierungscode oder der Schlüssel /R ergänzt den Aktivierungscode oder Schlüssel /ADD und weist darauf hin, dass der Aktivierungscode bzw. Schlüssel als Reserve hinzugefügt wird.
/DEL:<Schlüssel oder Aktivierungscode>	Löscht den Schlüssel mit der angegebenen Nummer oder den angegebenen Aktivierungscode.

Rückgabecodes für den Befehl KAVSHELL LICENSE (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL LICENSE" auf Seite 272)

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 2.2 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 2.2 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 mit den Schlüsselwerten /S und /LVL an (s. Tabelle unten).

Tabelle 50. 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. Sie können Netzwerkpfade im UNC-Format (Universal Naming Convention) angeben. Pfade von Ordnern auf Netzlaufwerken des geschützten Computers sind nicht zulässig. 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 2.2, die Daten in eine neue Datei zu schreiben. Die bisherige Protokolldatei 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.

Beispiele 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 272)

Log-Dateien für Kaspersky Embedded Systems Security 2.2 defragmentieren. KAVSHELL VACUUM

Mithilfe des Befehls `KAVSHELL VACUUM` können Sie Log-Dateien für Ereignisse des Programms defragmentieren. Damit können Fehler bei der Ausführung des Systems bzw. von Kaspersky Embedded Systems Security 2.2 verhindert werden, die entstehen, wenn Sie Protokolle dauerhaft speichern.

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 Protokolldateien 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 2.2 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 2.2\2.2\Reports gespeichert. Wenn Sie manuell einen anderen Pfad angegeben haben, an dem Sie Protokolle speichern, defragmentiert der Befehl `KAVSHELL VACUUM` die Dateien im Ordner, der in den Einstellungen der Berichte von Kaspersky Embedded Systems Security 2.2 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 die Protokolle von Kaspersky Embedded Systems Security 2.2 und verbietet ein Protokollieren von Ereignissen. Damit das Schutzniveau 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 2.2 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 2.2 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 2.2 erstellt im Systemverzeichnis %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 2.2 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 2.2 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 2.2 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 2.2 verursachte Belastung des Computers erhöhen. Dabei untersucht Anti-Virus alle Dateien, auf die nach dem Leeren der Datei klamfb.dat zum ersten Mal zugegriffen wird. Nach der Untersuchung trägt Kaspersky Embedded Systems Security 2.2 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 2.2 erstellt werden, aktivieren oder deaktivieren (siehe folgende Tabelle). Außerdem können Sie jederzeit Speicher-Images der von Kaspersky Embedded Systems Security 2.2 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>
```

Beispiele 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 /P:1234
```

► *Um die Erstellung einer Dump-Datei zu aktivieren, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /OFF
```

Tabelle 51. 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. Wenn Sie den Pfad eines nicht vorhandenen Ordners angeben, wird keine Dump-Datei erstellt. Sie können die Netzwerkpfade im UNC-Format (Universal Naming Convention) verwenden. Pfade von Ordnern auf Netzlaufwerken des geschützten Computers sind nicht zulässig. 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 eines bestimmten laufenden Prozesses von Kaspersky Embedded Systems Security 2.2 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 273)

Einstellungen importieren. KAVSHELL IMPORT

Mit dem Befehl `KAVSHELL IMPORT` können Sie Einstellungen, Funktionen und Aufgaben von Kaspersky Embedded Systems Security 2.2 aus einer Konfigurationsdatei in Kaspersky Embedded Systems Security 2.2 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>
```

Beispiele für den Befehl KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tabelle 52. 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 273)

Einstellungen exportieren. KAVSHELL EXPORT

Mit dem Befehl `KAVSHELL EXPORT` können Sie alle Einstellungen von Kaspersky Embedded Systems Security 2.2 und die aktuellen Aufgaben in eine Konfigurationsdatei exportieren, um sie auf anderen Computern in Kaspersky Embedded Systems Security 2.2 zu importieren.

Syntax des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiele für den Befehl KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tabelle 53. 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 274)

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 Ereignisberichten entnommen.

Syntax des Befehls KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <vollständiger Pfad zur erstellten Datei samt Dateiname>
```

Beispiele für den Befehl KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabelle 54. 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 55. 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 2.2 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 2.2 unter dem Systemkonto).
-99	Unbekannter Fehler

Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL

Tabelle 56. 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 über Ausgabenausführung ist fehlgeschlagen.
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR

Tabelle 57. 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 2.2 bereits gestartet oder schon beendet)
402	Aufgabe ist schon gestartet (für Schlüssel /STATE)

Rückgabecodes für den Befehl KAVSHELL TASK

Tabelle 58. 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 59. Rückgabecodes für den Befehl KAVSHELL RTP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler

Feedback-Code	Beschreibung
-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 60. 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 2.2 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 61. Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet

Feedback-Code	Beschreibung
-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 62. 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 63. 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 64. Rückgabecodes für den Befehl KAVSHELL FBRESET

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL DUMP

Tabelle 65. 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 66. 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

Feedback-Code	Beschreibung
501	Der Vorgang wurde erfolgreich ausgeführt. Bei der Befehlsausführung ist jedoch ein Fehler bzw. Kommentar aufgetreten (z. B. Kaspersky Embedded Systems Security 2.2 hat die Einstellungen einer bestimmten funktionellen Komponente nicht importiert).
-502	Zu importierende Datei ist nicht vorhanden oder hat ein unbekanntes Format
-503	Inkompatible Einstellungen (Konfigurationsdatei aus einem anderen Programm oder einer höhere oder inkompatiblen Version von Kaspersky Embedded Systems Security 2.2 exportiert)

Rückgabecodes für den Befehl KAVSHELL EXPORT

Tabelle 67. 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 2.2 hat die Einstellungen einer bestimmten funktionellen Komponente nicht exportiert).

Integration mit Drittanbietersystemen

Dieser Abschnitt beschreibt die Integration von Kaspersky Embedded Systems Security 2.2 mit Drittanbieterfunktionen und -technologien.

In diesem Kapitel

Leistungskontrolle. Indikatoren in Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt informiert über die Indikatoren von Kaspersky Embedded Systems Security 2.2: Leistungsindikatoren für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps.

In diesem Kapitel

Leistungsindikatoren für das Programm Systemmonitor

Dieser Abschnitt enthält Informationen über Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows, die von Kaspersky Embedded Systems Security 2.2 während der Installation registriert werden.

In diesem Abschnitt

Über SNMP-Indikatoren in Kaspersky Embedded Systems Security 2.2

Die Komponente **Leistungsindikatoren** gehört zu den standardmäßig installierten Komponenten von Kaspersky Embedded Systems Security 2.2. Während der Installation registriert Kaspersky Embedded Systems Security 2.2 seine Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows.

Mit den Indikatoren von Kaspersky Embedded Systems Security 2.2 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 2.2 und Abstürze diagnostizieren.

Sie können die Leistungsindikatoren für Kaspersky Embedded Systems Security 2.2 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 2.2 bei Grenzwertüberschreitungen gegeben.

Gesamtzahl der abgelehnten Anfragen

Tabelle 68. 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 2.2 gezählt. Das Programm überspringt Objekte, deren Verarbeitungsanfragen von aktiven Prozessen durch Kaspersky Embedded Systems Security 2.2 zurückgewiesen werden.
Ziel	Ein Indikator kann überwachen: • Qualitätsverluste beim Echtzeitschutz wegen hoher Belastung der Arbeitsprozesse von Kaspersky Embedded Systems Security 2.2 • 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 2.2 waren vollständig ausgelastet, deshalb konnte Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 untersucht Objekte nicht beim Öffnen. Kaspersky Embedded Systems Security 2.2 neu starten

Gesamtzahl der übersprungenen Anfragen

Tabelle 69. 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 2.2 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 2.2 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 2.2 neu, um die angehaltenen Datenströme wiederherzustellen.

Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Tabelle 70. 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 2.2 gezählt. Kaspersky Embedded Systems Security 2.2 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 2.2 für die Anfragenbearbeitung einen größeren Arbeitsspeicher. Es ist möglich, dass es andere Prozesse gibt, die den ganzen Arbeitsspeicher in Anspruch nehmen.

Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Tabelle 71. 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 2.2 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 72. 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 2.2 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 2.2 überspringt das Objekt. Vergrößern Sie die Anzahl der Prozesse von Kaspersky Embedded Systems Security 2.2 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 2.2 verwenden.

Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Tabelle 73. 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 2.2 die Belastung ungleichmäßig auf die ausführenden Prozesse. Kaspersky Embedded Systems Security 2.2 neu starten

Anzahl der Elemente in der Warteschlange der infizierten Objekte

Tabelle 74. 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 2.2 • Virenepidemien
Normalwert / Grenzwert	Der Indikatorwert kann von Null abweichen, wenn Kaspersky Embedded Systems Security 2.2 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 2.2 verarbeitet keine Objekte (möglicherweise aufgrund eines Absturzes des File-Interception-Dispatchers) Kaspersky Embedded Systems Security 2.2 neu starten • Es steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security 2.2 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 infizierte Objekten in der Aufgabe Echtzeitschutz für Dateien. Informationen über die Anzahl der gefundenen Objekte können Sie der Aufgabenstatistik oder dem Protokoll über Ausgabenausführung entnehmen.

Anzahl der pro Sekunde verarbeiteten Objekte

Tabelle 75. 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 2.2 oder wegen Fehler bei der Ausführung von Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security 2.2 zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Computerbelastung durch andere Anwendungen senken). • Kaspersky Embedded Systems Security 2.2 ist abgestürzt (mehrere Datenströme stehen still). Kaspersky Embedded Systems Security 2.2 neu starten

SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security 2.2

Dieser Abschnitt enthält Informationen zu den Indikatoren und Traps in Kaspersky Embedded Systems Security 2.2.

In diesem Abschnitt

Über SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security 2.2

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 2.2 mithilfe des SNMP-Protokolls (Simple Network Management Protocol) anzeigen.

Um die Indikatoren und Traps für Kaspersky Embedded Systems Security 2.2 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 2.2

Dieser Abschnitt enthält eine Tabelle mit einer Beschreibung der Einstellungen der SNMP-Indikatoren von Kaspersky Embedded Systems Security 2.2.

In diesem Abschnitt

Leistungsindikatoren

Tabelle 76. Leistungsindikatoren

Indikatoren	Definition
currentRequestsAmount	Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden (auf S. 278)
currentInfectedQueueLength	Anzahl der Elemente in der Warteschlange für infizierte Objekte (siehe Abschnitt "Anzahl der Elemente in der Warteschlange der infizierten Objekte" auf Seite 280)
currentObjectProcessingRate	Anzahl der pro Sekunde verarbeiteten Objekte (auf S. 281)
currentWorkProcessesNumber	Aktuelle Anzahl von Arbeitsprozessen, die von Kaspersky Embedded Systems Security 2.2 genutzt werden

Indikatoren für Quarantäne

Tabelle 77. 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)

Indikatoren für Backup

Tabelle 78. Indikatoren für Backup

Indikatoren	Definition
currentBackupStorageSize	Volumen der Daten im Backup-Ordner (MB)

Allgemeine Indikatoren

Tabelle 79. 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*)
licenseExpirationDate	Gültigkeitsdauer der Lizenz. Wenn ein aktiver Schlüssel und Reserveschlüssel hinzugefügt wurden, wird das Ablaufdatum der Lizenz des Reserveschlüssels angezeigt.
currentApplicationUptime	Ausführungszeit von Kaspersky Embedded Systems Security 2.2 seit dem letzten Start, in Hundertstelsekunden
currentFileMonitorTaskStatus	Status der Aufgabe Echtzeitschutz für Dateien: **On** – wird ausgeführt; **Off** – wurde beendet oder angehalten.

Update-Indikatoren

Tabelle 80. 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 81. 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 2.2 in die Quarantäne verschoben wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien.

Indikatoren	Definition
totalObjectsNotQuarantined	Anzahl der infizierten oder möglicherweise infizierten Objekte, die Kaspersky Embedded Systems Security 2.2 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 2.2 desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotDisinfected	Anzahl der infizierten und anderen Objekte, deren Desinfektion durch Kaspersky Embedded Systems Security 2.2 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 2.2 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 2.2 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 2.2 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 2.2 erfolglos versuchte, ins Backup zu verschieben. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien

SNMP-Traps

Die Einstellungen von SNMP-Traps in Kaspersky Embedded Systems Security 2.2 sind in nachstehender Tabelle beschrieben.

Tabelle 82. SNMP-Traps in Kaspersky Embedded Systems Security 2.2

Trap	Beschreibung	Einstellungen
eventThreatDetected	Objekt gefunden.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

Trap	Beschreibung	Einstellungen
eventBackupStorageSizeExceeds	Die maximale Größe des Backups wurde 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 2.2 erstellt weiterhin Backups für infizierte Objekte.	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 2.2 erstellt weiterhin Backups für infizierte Objekte.	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 2.2 verschiebt möglicherweise infizierte Objekte weiterhin in die Quarantäne.	eventDateAndTime eventSeverity eventSource

Trap	Beschreibung	Einstellungen
eventThresholdQuarantineStorageSizeExceeds	Maximale Größe der Quarantäne ist erreicht. Die Größe des freien Speicherplatzes im Quarantäne-Ordner, die mit der Einstellung **Grenzwert für verfügbaren Speicherplatz (MB)** eingegeben wurde, liegt unter dem angegebenen Wert. Kaspersky Embedded Systems Security 2.2 verschiebt möglicherweise infizierte Objekte weiterhin in die Quarantäne.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Quarantänefehler.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Fehler beim Speichern einer Kopie des Objekts im Backup.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Quarantänefehler.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Backup-Fehler.	eventSeverity eventDateAndTime eventSource eventReason

Trap	Beschreibung	Einstellungen
eventAVBasesOutdated	Antiviren-Datenbanken sind veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Datenbanken-Update zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Antiviren-Datenbanken sind stark veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Datenbanken-Update zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Embedded Systems Security 2.2 läuft	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Embedded Systems Security 2.2 wurde beendet	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerform ForALongTime	Untersuchung wichtiger Bereiche liegt lange zurück. Berechnet als Anzahl der Tage seit dem letzten Abschluss der *Aufgabe zur Untersuchung wichtiger Bereiche*	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Die Lizenz ist abgelaufen!	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	wenn die Gültigkeitsdauer der Lizenz bald abläuft Es werden die Tage gezählt, die bis zum Ablauf der Lizenz verbleiben.	eventSeverity eventDateAndTime eventSource days

Trap	Beschreibung	Einstellungen
eventTaskInternalError	Fehler bei Ausgabenausführung.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Fehler bei Ausführung einer Update-Aufgabe.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

In der Tabelle unten werden die Trap-Parameter und die entsprechenden Parameterwerte beschrieben.

Tabelle 83. Parameterwerte von SNMP-Traps

Einstellung	Beschreibung und mögliche Werte
eventDateAndTime	Zeitpunkt, zu dem ein Ereignis eingetreten ist.
eventSeverity	Ereigniskategorie des Ereignisses. Der Parameter nimmt die folgenden Werte an: • critical (1) – kritisch • warning (2) – Warnung • info (3) – informativ.
userName	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: Funktionalkomponente, bei der ein Ereignis aufgetreten ist. Der Parameter nimmt die folgenden Werte an: • unknown (0) – Die Komponente ist unbekannt • quarantine (1) – Quarantäne • backup (2) – Backup • reporting (3) – Protokolle über Ausgabenausführung • 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 2.2 als Ganzem zu tun hat • systemAudit (8) – Systemaudit-Protokoll

Einstellung	Beschreibung und mögliche Werte
eventReason	Grund für Ereigniseintritt. Der Parameter nimmt die folgenden Werte an: • 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 2.2 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 Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Embedded Systems Security 2.2 beim Fund eines Objekts zurückgibt. Sie können den vollständigen Namen eines gefundenen Objekts im Bericht über Aufgabenausführung einsehen (siehe Abschnitt "Protokolleinstellungen anpassen" auf Seite 151).
detectType	Typ des gefundenen Objekts. Der Parameter nimmt die folgenden Werte an: • 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 die Daten zu schädigen
detectCertainty	Gewissheit für Erkennung einer Bedrohung. Der Parameter nimmt die folgenden Werte an: • Suspicion (möglicherweise infiziert) – Kaspersky Embedded Systems Security 2.2 hat erkannt, dass ein Codeabschnitt des Objekts teilweise mit einem bekannten Schadcode übereinstimmt. • Sure (infiziert)– Kaspersky Embedded Systems Security 2.2 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	Fehlercode.
knowledgeBaseId	Adresse des Artikels in der Wissensdatenbank (beispielsweise Adresse des Artikels, der einen Fehler beschreibt).
taskName	Aufgabenname.

Einstellung	Beschreibung und mögliche Werte
updaterErrorEventReason	Grund, aus dem das Update nicht übernommen wurde. Der Parameter nimmt die folgenden Werte an: • 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.

Einstellung	Beschreibung und mögliche Werte
storageObjectNotAddedEventReason	Grund für Nichtverschieben eines Objektes in Backup oder Quarantäne. Der Parameter nimmt die folgenden Werte an: • reasonUnknown(0) – der Grund ist unbekannt • reasonStorageInternalError – Datenbankfehler, bitte stellen Sie Kaspersky Embedded Systems Security 2.2 wieder her. • reasonStorageReadOnly – Datenbankfehler, bitte stellen Sie Kaspersky Embedded Systems Security 2.2 wieder her. • reasonStorageIOError – Ein-/Ausgabefehler: a) Kaspersky Embedded Systems Security 2.2 ist beschädigt, bitte stellen Sie Kaspersky Embedded Systems Security 2.2 wieder her; b) das Laufwerk mit Kaspersky Embedded Systems Security 2.2 ist beschädigt. • reasonStorageCorrupted – der Speicher ist beschädigt, bitte stellen Sie Kaspersky Embedded Systems Security 2.2 wieder her. • reasonStorageFull – Die Datenbank ist voll. Bitte geben Sie Speicherplatz auf dem Datenträger frei. • reasonStorageOpenError – Die Datenbankdatei konnte nicht geöffnet werden. Bitte stellen Sie Kaspersky Embedded Systems Security 2.2 wieder her. • reasonStorageOSFeatureError – Einige Funktionen des Betriebssystems entsprechen nicht den Anforderungen von Kaspersky Embedded Systems Security 2.2. • 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.

WMI-Integration

Kaspersky Embedded Systems Security 2.2 unterstützt die Integration mit Windows Management Instrumentation (WMI): Sie können Client-Systeme mit WMI verwenden, um Daten über den Standard "Web-Based Enterprise Management" (WBEM) zu empfangen und auf diese Weise Informationen über den Status von Kaspersky Embedded Systems Security 2.2 und dessen Komponenten zu sammeln.

Bei der Installation von Kaspersky Embedded Systems Security 2.2 wird das proprietäre Modul im System registriert, was die Erstellung eines Namespace für Kaspersky Embedded Systems Security 2.2 im WMI-Stammnamespace auf dem lokalen Computer erleichtert. Ein Namespace für Kaspersky Embedded Systems Security 2.2 ermöglicht Ihnen die Verwendung von Klassen und Instanzen von Kaspersky Embedded Systems Security 2.2 samt ihren Eigenschaften.

Die Werte einiger Instanzeneigenschaften 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 eine Aufgabe zum Echtzeitschutz des Computers). 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 Tools zur Erstellung von WMI-Namespace-Abfragen und zum Abrufen von dynamischen Daten von WMI-Namespaces in ihrem Unternehmensnetzwerk verwenden, können Sie Informationen über den aktuellen Zustand des Programms empfangen (siehe nachfolgende Tabelle).

Tabelle 84. Informationen über den Programmzustand

Eigenschaft der Instanz	Beschreibung	Werte
ProductName	Name des installierten Programms.	Vollständiger Name des Programms ohne Versionsnummer.
ProductVersion	Volle Version des installierten Programms.	Volle Versionsnummer des Programms, einschließlich Build-Nummer.
InstalledPatches	Liste mit Anzeigenamen der Patches, die zusammen mit dem Programm installiert werden.	Liste mit kritischen Fehlerbehebungen, die für das Programm installiert werden.
IsLicenseInstalled	Aktivierungsstatus des Programms.	Status des Schlüssels, mit dem das Programm aktiviert wurde. Mögliche Werte: • False – im Programm wurde kein Schlüssel oder Aktivierungscode angegeben. • True – im Programm wurde ein Schlüssel oder Aktivierungscode hinzugefügt.
LicenseDaysLeft	Zeigt an, wie viele Tage bis zum Ablauf der aktuellen Lizenz verbleiben.	Anzahl der Tage bis zum Ablauf der aktuellen Lizenz. Mögliche nichtpositive Werte: • 0 – Die Lizenz ist abgelaufen • -1 – zum aktuellen Schlüssel können momentan keine Informationen abgerufen werden oder der angegebene Schlüssel kann nicht zur Aktivierung des Programms verwendet werden (z. B. weil er auf der schwarzen Liste steht und deshalb blockiert wurde).

Eigenschaft der Instanz	Beschreibung	Werte
AVBasesDatetime	Zeitstempel der aktuellen Version der Antiviren-Datenbanken.	Datum und Uhrzeit der Erstellung der Antiviren-Datenbanken, die momentan verwendet werden. Wenn das installierte Programm keine Antiviren-Datenbanken verwendet, erhält das Feld den Wert "Nicht installiert".
IsExploitPreventionEnabled	Status der Komponente "Exploit-Prävention".	Status der Komponente "Exploit-Prävention". Mögliche Werte: • True – die Komponente "Exploit-Prävention" ist aktiviert und bietet Schutz. • False – die Komponente "Exploit-Prävention" bietet keinen Schutz. Zum Beispiel: deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
ProtectionTasksRunning	Liste mit allen Schutzaufgaben, die momentan ausgeführt werden.	Liste mit Schutz-, Kontroll- und Überwachungsaufgaben, die momentan ausgeführt werden. Dieses Feld bezieht sich auf alle laufenden nicht-periodischen Aufgaben. Wenn keine einzige nicht-periodische Aufgabe aufgeführt wird, erhält das Feld den Wert "Nein".
IsAppControlRunning	Status der Aufgabe "Kontrolle des Programmstarts".	Status der Aufgabe "Kontrolle des Programmstarts". • True – die Aufgabe "Kontrolle des Programmstarts" wird momentan ausgeführt. • False – die Aufgabe "Kontrolle des Programmstarts" wird momentan nicht ausgeführt oder die Komponente "Kontrolle des Programmstarts" ist nicht installiert.
AppControlMode	Modus der Aufgabe "Kontrolle des Programmstarts".	Beschreibung des aktuellen Status der Komponente "Kontrolle des Programmstarts" samt Beschreibung des ausgewählten Modus für die entsprechende Aufgabe. Mögliche Werte: • Aktiv – in den Aufgabeneinstellungen wurde der Modus **Aktiv** ausgewählt. • Nur Statistik – in den Aufgabeneinstellungen wurde der Modus **Nur Statistik** ausgewählt. • Nicht installiert – die Komponente "Kontrolle des Programmstarts" ist nicht installiert.

Eigenschaft der Instanz	Beschreibung	Werte
AppControlRulesNumber	Gesamtanzahl der Regeln für die Kontrolle des Programmstarts.	Anzahl der Regeln, die momentan in den Einstellungen der Aufgabe "Kontrolle des Programmstarts" angegeben sind.
AppControlLastBlocking	Zeitstempel für das letzte Verbot des Programmstarts durch die Aufgabe "Kontrolle des Programmstarts" in einem beliebigen Modus.	Datum und Uhrzeit des letzten Verbots eines Programmstarts durch die Komponente "Kontrolle des Programmstarts". Dieses Feld enthält alle blockierten Programme unabhängig vom Aufgabenmodus. Wenn zum Zeitpunkt der Verarbeitung der WMI-Abfrage keine Instanzen von Verboten des Programmstarts registriert wurden, erhält das Feld den Wert "Nein".
PeriodicTasksRunning	Liste mit allen periodischen Aufgaben, die momentan ausgeführt werden.	Liste der Aufgaben zur Untersuchung auf Befehl, zum Update und zur Inventarisierung, die momentan ausgeführt werden. Dieses Feld bezieht sich auf alle laufenden periodischen Aufgaben. Wenn momentan keine einzige periodische Aufgabe aufgeführt wird, erhält das Feld den Wert "Nein".
ConnectionState	Status der Verbindung zwischen der Komponente "WMI Provider" und Kaspersky Security Service (KAVFS).	Informationen zum Status der Verbindung zwischen dem Modul "WMI Provider" und Kaspersky Security Service. Mögliche Werte: • Erfolg – die Verbindung wurde erfolgreich hergestellt: der WMI-Client kann Informationen zum Programmstatus abrufen. • Fehlgeschlagen. Fehlercode: <code> – die Verbindung konnte aufgrund eines Fehlers mit dem angegebenen Code nicht hergestellt werden.

Diese Daten repräsentieren die Instanzeigenschaften KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, wobei gilt:

- KasperskySecurity_ProductInfo ist der Name der Klasse für Kaspersky Embedded Systems Security 2.2
- .ProductName=Kaspersky Embedded Systems Security ist der Schlüsselparameter für Kaspersky Embedded Systems Security 2.2

Die Instanz wird im Namespace ROOT\Kaspersky\Security erstellt.

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).

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 registrierter 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/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 2.2 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.

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
Viren-Labor:	https://virusdesk.kaspersky.com/de (zur Untersuchung verdächtiger Dateien und Webseiten)
Webforum von Kaspersky Lab:	https://forum.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 Marken der Intel Corporation in den USA und/oder anderen Ländern.

Active Directory, Excel, Internet Explorer, Microsoft, Outlook, Windows, Windows Server und Windows Vista sind registrierte Marken der Microsoft Corporation, die in den USA und anderen Ländern eingetragen sind.

Linux ist ein registriertes Warenzeichen von Linus Torvalds in den USA und anderen Ländern.

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 Datenbanken-Update.

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

Die Richtlinie bestimmt die Einstellungen eines Programms und verwaltet den Zugriff auf die Konfiguration eines Programms, das auf Computern innerhalb einer Administrationsgruppe installiert ist. 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 Richtlinien erstellen; allerdings kann nur eine einzige Richtlinie gleichzeitig auf ein Programm innerhalb einer Administrationsgruppe angewendet 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.

Sachregister

S

V