kaspersky

Kaspersky Embedded Systems Security

© 2024 AO Kaspersky Lab

Inhalt

Über Kaspersky Embedded Systems Security
Neuerungen
Informationsquellen über Kaspersky Embedded Systems Security
  Quellen für die selbstständige Informationssuche
  Diskussion über die Programme von Kaspersky in der Community
Kaspersky Embedded Systems Security
  Lieferumfang
  Hard- und Software-Voraussetzungen
  Funktionale Anforderungen und Einschränkungen
    Installation und Deinstallation
    Überwachung der Datei-Integrität
    Firewall-Verwaltung
    Andere Einschränkungen
Programm installieren und deinstallieren
  Codes der Programmkomponenten von Kaspersky Embedded Systems Security für den Dienst Windows Installer
    Die Programmkomponenten von Kaspersky Embedded Systems Security
    Programmkomponente "Administrations-Tools"
  Systemänderungen nach der Installation von Kaspersky Embedded Systems Security
  Prozesse von Kaspersky Embedded Systems Security
  Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer
  Installations- und Deinstallationsprotokolle für Kaspersky Embedded Systems Security
  Installation planen
    Administrations-Tools auswählen
    Installationstyp auswählen
  Installation und Deinstallation des Programms mit dem Assistenten
    Installation mit dem Installationsassistenten
      Installation von Kaspersky Embedded Systems Security
      Installation der Konsole für Kaspersky Embedded Systems Security
      Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Gerät
        Anonymen Remote-Zugriff auf COM-Anwendungen erlauben
        Netzwerkverbindungen für Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security erlauben
        Ausgehende Regel für die Windows-Firewall hinzufügen
      Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
        Aufgabe zum Update der Datenbank von Kaspersky Embedded Systems Security starten und anpassen
        Untersuchung wichtiger Bereiche
    Ändern des Pakets von Programmkomponenten und Reparieren von Kaspersky Embedded Systems Security
    Deinstallation mit dem Installationsassistenten
      Deinstallation von Kaspersky Embedded Systems Security
      Deinstallation der Konsole für Kaspersky Embedded Systems Security
  Installation und Deinstallation des Programms aus der Befehlszeile
    Über die Installation und Deinstallation von Kaspersky Embedded Systems Security aus der Befehlszeile
    Beispiele von Befehlen für die Installation von Kaspersky Embedded Systems Security
    Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
    Komponenten hinzufügen und entfernen. Beispiele für Befehle
    Deinstallation von Kaspersky Embedded Systems Security. Beispiele für Befehle
    Rückgabecodes

Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center
Allgemeine Informationen zur Installation über Kaspersky Security Center
Rechte zur Installation bzw. Deinstallation von Kaspersky Embedded Systems Security
Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center
Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
Installation der Programmkonsole über das Kaspersky Security Center
Deinstallation von Kaspersky Embedded Systems Security über Kaspersky Security Center
Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory
Installation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory
Aktionen, die nach der Installation von Kaspersky Embedded Systems Security ausgeführt werden müssen
Deinstallation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory
Überprüfung der Funktionen von Kaspersky Embedded Systems Security Verwendung des EICAR-Testvirus
EICAR-Testvirus
Echtzeitschutz für Dateien und Funktionen der Untersuchung auf Befehl testen
Programmoberfläche
Lizenzverwaltung für das Programm
Über den Endbenutzer-Lizenzvertrag
Über die Lizenz
Über das Lizenzzertifikat
Über den Schlüssel
Über die Schlüsseldatei
Über den Aktivierungscode
Über die Bereitstellung von Daten
Aktivieren des Programms mit einer Schlüsseldatei
Aktivieren des Programms mit einem Aktivierungscode
Anzeigen von Informationen über die aktive Lizenz
Funktionsbeschränkungen bei Ablauf der Lizenz
Verlängern der Lizenz
Löschen des Schlüssels
Arbeiten mit dem Verwaltungs-Plug-in
Verwaltung von Kaspersky Embedded Systems Security über Kaspersky Security Center
Programmeinstellungen verwalten
Navigation
Öffnen der allgemeinen Einstellungen über die Richtlinie
Öffnen der allgemeinen Einstellungen im Eigenschaftenfenster des Programms
Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center
Skalierbarkeit, Schnittstelle und Untersuchungseinstellungen im Kaspersky Security Center anpassen
Sicherheitseinstellungen in Kaspersky Security Center anpassen
Verbindungseinstellungen über Kaspersky Security Center anpassen
Zeitplan für den Start von lokalen Systemaufgaben anpassen
Quarantäne- und Backup-Einstellungen in Kaspersky Security Center anpassen
Erstellen und Einrichten von Richtlinien
Richtlinie erstellen
Abschnitte mit Richtlinieneinstellungen für Kaspersky Embedded Systems Security
Anpassen einer Richtlinie
Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center
Über die Erstellung von Aufgaben in Kaspersky Security Center
Aufgabe mithilfe von Kaspersky Security Center erstellen

Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen
Gruppenaufgaben in Kaspersky Security Center anpassen
Aufgabe Programm aktivieren
Update-Aufgaben
Integritätsprüfung für Programme
Anpassen der Einstellungen für die Fehlerdiagnose in Kaspersky Security Center
Arbeit mit dem Aufgabenzeitplan
Aufgaben planen
Start nach Zeitplan aktivieren und deaktivieren
Berichte in Kaspersky Security Center
Verwendung der Konsole für Kaspersky Embedded Systems Security
Über die Konsole für Kaspersky Embedded Systems Security
Benutzeroberfläche der Konsole für Kaspersky Embedded Systems Security
Fenster "Konsole für Kaspersky Embedded Systems Security"
Taskleistensymbol im Infobereich
Kaspersky Embedded Systems Security über die Programmkonsole auf einem anderen Gerät verwalten
Allgemeine Programmeinstellungen über die Programmkonsole konfigurieren
Aufgaben von Kaspersky Embedded Systems Security verwalten
Aufgabenkategorien von Kaspersky Embedded Systems Security
Manuelles Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe
Arbeit mit dem Aufgabenzeitplan
Einstellungen für den Aufgabenzeitplan anpassen
Start nach Zeitplan aktivieren und deaktivieren
Verwendung von Benutzerkonten für den Aufgabenstart
Über die Verwendung eines Benutzerkontos für den Aufgabenstart
Benutzerkonto für den Aufgabenstart festlegen
Import und Export von Einstellungen
Über den Import und Export von Einstellungen
Einstellungen exportieren
Einstellungen importieren
Verwendung von Vorlagen für Sicherheitseinstellungen
Über Vorlagen für Sicherheitseinstellungen
Vorlage für Sicherheitseinstellungen erstellen
Sicherheitseinstellungen in einer Vorlage aufrufen
Vorlage für Sicherheitseinstellungen anwenden
Vorlage für Sicherheitseinstellungen löschen
Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen
Arbeiten mit dem Web-Plug-in der Web-Konsole und der Cloud-Konsole
Kaspersky Embedded Systems Security über die Web Console und Cloud Console verwalten
Einschränkungen für Web Plug-in
Programmeinstellungen verwalten
Allgemeine Programmeinstellungen im Web-Plug-in konfigurieren
Skalierbarkeit und Schnittstelle und Untersuchungseinstellungen im Web-Plug-in anpassen
Anpassen der Sicherheitseinstellungen im Web-Plug-in
Anpassen der Verbindungseinstellungen im Web-Plug-in
Zeitplan für den Start von lokalen Systemaufgaben anpassen
Quarantäne- und Backup-Einstellungen im Web-Plug-in konfigurieren
Erstellen und Einrichten von Richtlinien

Richtlinie erstellen
Abschnitte mit Richtlinieneinstellungen für Kaspersky Embedded Systems Security
Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center
Zur Erstellung von Aufgaben im Web-Plug-in
Eine Aufgabe im Web-Plug-in erstellen
Gruppenaufgaben im Web-Plug-in anpassen
Aufgabe zum Aktivieren des Programms im Web-Plug-in anpassen
Updateaufgaben im Web-Plug-in anpassen
Einstellungen für die Fehlerdiagnose im Web-Plug-in anpassen
Arbeit mit dem Aufgabenzeitplan
Aufgaben planen
Start nach Zeitplan aktivieren und deaktivieren
Berichte in Kaspersky Security Center
Kompaktes Diagnosefenster
Über das kompakte Diagnosefenster
Status von Kaspersky Embedded Systems Security mithilfe des kompakten Diagnosefensters überprüfen
Überprüfung der Sicherheitsereignis-Statistik
Aktuelle Programmaktivität überprüfen
Erstellen von Dump-Dateien und Protokolldateien anpassen
Datenbanken und Programm-Module für Kaspersky Embedded Systems Security aktualisieren
Über Update-Aufgaben
Informationen zum Update der Programm-Module
Informationen zum Update der Programm-Datenbanken
Schemata für Updates der Antivirus-Programmdatenbanken und verwendeten Module in einem Unternehmen
Einstellung von Update-Aufgaben
Anpassen der Einstellungen für die Arbeit mit Update-Quellen für Kaspersky Embedded Systems Security
Optimierung des Festplatten-Subsystems bei der Ausführung der Aufgabe zum Update der Programm-Datenbanken
Einstellungen der Aufgabe zur Update-Verteilung anpassen
Einstellungen der Aufgabe Update der Programm-Module anpassen
Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security
Rollback des Updates für Programm-Module
Statistik zu Update-Aufgaben
Objekte isolieren und Backups kopieren
Isolierung möglicherweise infizierter Objekte. Quarantäne
Über die Isolierung möglicherweise infizierter Objekte
Quarantäneobjekte anzeigen
Quarantäneobjekte sortieren
Quarantäneobjekte filtern
Untersuchung von Quarantäne-Objekten
Wiederherstellung von Objekten aus der Quarantäne
Verschieben von Objekten in die Quarantäne
Objekte aus der Quarantäne löschen
Möglicherweise infizierte Quarantäneobjekte zur Analyse an Kaspersky einschicken
Anpassen der Quarantäne-Einstellungen
Quarantäne-Statistik
Backup-Kopien von Objekten erstellen. Backup
Über das Verschieben von Objekten vor der Desinfektion oder dem Löschen ins Backup
Objekte im Backup anzeigen

Dateien im Backup sortieren
Dateien im Backup filtern
Dateien aus Backup wiederherstellen
Dateien aus Backup löschen
Backup-Einstellungen anpassen
Backup-Statistik
Zugriff auf Netzwerkressourcen blockieren. Blockierte Hosts
Über den Speicher der blockierten Hosts
Blockierte Hosts über das Verwaltungs-Plug-in verwalten
Blockieren des Zugriffs auf Netzwerk-Dateiressourcen aktivieren
Einstellungen für blockierte Geräte anpassen
Blockierte Hosts über die Programmkonsole verwalten
Blockieren des Zugriffs auf Netzwerk-Dateiressourcen aktivieren
Einstellungen für blockierte Geräte anpassen
Blockierte Hosts über das Web-Plug-in verwalten
Blockieren von Hosts aktivieren
Einstellungen für blockierte Geräte anpassen
Registrierung von Ereignissen. Berichte in Kaspersky Embedded Systems Security
Möglichkeiten zur Registrierung der Dienste von Kaspersky Embedded Systems Security
Systemaudit-Protokoll
Ereignisse im Systemaudit-Protokoll sortieren
Ereignisse im Systemaudit-Protokoll filtern
Ereignisse aus dem Systemaudit-Bericht löschen
Protokolle der Aufgabenausführung
Über Protokolle der Aufgabenausführung
Ereignisliste in den Protokollen der Aufgabenausführung anzeigen
Protokolle der Aufgabenausführung sortieren
Protokolle der Aufgabenausführung filtern
Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in den Berichten über Aufgabenausführung anzeigen
Informationen aus einem Protokoll der Aufgabenausführung exportieren
Protokolle der Aufgabenausführung löschen
Sicherheitsprotokoll
Ereignisbericht von Kaspersky Embedded Systems Security in der Ereignisanzeige anzeigen
Anpassen der Protokolleinstellungen im Verwaltungs-Plug-in
Über die SIEM-Integration
Anpassen der Einstellungen der SIEM-Integration
Über die Konfiguration von Protokollen und Benachrichtigungen
Protokolleinstellungen anpassen
Sicherheitsprotokoll
Anpassen der Einstellungen der SIEM-Integration
Benachrichtigungseinstellungen anpassen
Konfigurieren der Interaktion mit dem Administrationsserver
Benachrichtigungen anpassen
Methoden zur Benachrichtigung von Administrator und Benutzer
Benachrichtigungen an Administrator und Benutzer anpassen
Starten und Beenden von Kaspersky Embedded Systems Security
Verwaltungs-Plug-in für Kaspersky Embedded Systems Security starten

Konsole für Kaspersky Embedded Systems Security aus dem Startmenü starten
Kaspersky Security Service starten und anhalten
Start der Komponenten von Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems
Über Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems
Kaspersky Embedded Systems Security im abgesicherten Modus starten
Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security
Über die Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security
Schutz vor Änderungen an Ordnern mit installierten Komponenten von Kaspersky Embedded Systems Security
Schutz vor Änderungen der Registrierungsschlüssel von Kaspersky Embedded Systems Security
Kaspersky Security Service als geschützten Dienst registrieren
Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security
Über Rechte zur Verwaltung von Kaspersky Embedded Systems Security
Über die Rechte zur Verwaltung von registrierten Diensten
Über Zugriffsrechte für Kaspersky Security Management Service
Über die Rechte zur Verwaltung des Dienstes Kaspersky Security Service
Zugriffsrechte über das Verwaltungs-Plug-in verwalten
Konfiguration der Zugriffsrechte für Kaspersky Embedded Systems Security und Kaspersky Security Service
Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security
Zugriffsrechte über die Programmkonsole verwalten
Konfiguration der Zugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security und Kaspersky Security Service
Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security
Zugriffsrechte über das Web-Plug-in verwalten
Konfiguration der Zugriffsrechte für Kaspersky Embedded Systems Security und Kaspersky Security Service
Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security
Echtzeitschutz für Dateien
Über die Aufgabe zum Echtzeitschutz für Dateien
Über den Schutzbereich von Aufgaben und Sicherheitseinstellungen
Über virtuelle Schutzbereiche
Vordefinierte Schutzbereiche
Über vordefinierte Sicherheitsstufen
Dateierweiterungen, die in der Aufgabe zum Echtzeitschutz für Dateien standardmäßig untersucht werden
Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien
Aufgabe zum Echtzeitschutz für Dateien über das Verwaltungs-Plug-in verwalten
Navigation
Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen
Aufgabeneigenschaften für den Echtzeitschutz für Dateien öffnen
Aufgabe zum Echtzeitschutz für Dateien anpassen
Schutzmodus auswählen
Heuristische Analyse und Integration mit anderen Programmkomponenten
Aufgaben planen
Schutzbereich von Aufgaben erstellen und konfigurieren
Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen
Sicherheitseinstellungen manuell anpassen
Allgemeine Aufgabeneinstellungen anpassen
Aktionen anpassen
Leistung optimieren
Aufgabe zum Echtzeitschutz für Dateien über die Programmkonsole verwalten

Navigation
Aufgabeneinstellungen für den Echtzeitschutz für Dateien öffnen
Einstellungen für den Schutzbereich der Aufgabe zum Echtzeitschutz für Dateien öffnen
Aufgabe zum Echtzeitschutz für Dateien anpassen
Schutzmodus auswählen
Heuristische Analyse und Integration mit anderen Programmkomponenten
Einstellungen für den Aufgabenzeitplan anpassen
Schutzbereich erstellen
Einstellungen für die Anzeige der freigegebenen Netzwerkordner anpassen
Schutzbereich erstellen
Netzwerkobjekte in den Schutzbereich aufnehmen
Virtuellen Schutzbereich erstellen
Sicherheitseinstellungen manuell anpassen
Auswahl von vordefinierten Sicherheitsstufen für die Aufgabe Echtzeitschutz für Dateien
Allgemeine Aufgabeneinstellungen anpassen
Aktionen anpassen
Leistung optimieren
Statistik für die Aufgabe zum Echtzeitschutz für Dateien
Aufgabe zum Echtzeitschutz für Dateien über das Web-Plug-in verwalten
Konfigurieren der Aufgabe zum Echtzeitschutz für Dateien
Schutzbereich der Aufgabe anpassen
Verwendung von KSN
Über die Aufgabe "Verwendung von KSN"
Standardeinstellungen der Aufgabe "Verwendung von KSN"
Verwendung von KSN über das Verwaltungs-Plug-in verwalten
Konfiguration der Aufgabe Verwendung von KSN
Konfiguration der Datenverarbeitung
Verwendung von KSN über die Programmkonsole verwalten
Konfiguration der Aufgabe Verwendung von KSN
Konfiguration der Datenverarbeitung
Verwendung von KSN über das Web-Plug-in verwalten
Konfiguration des zusätzlichen Versands von Daten
Statistik für die Aufgabe Verwendung von KSN
Schutz vor Netzwerkbedrohungen
Informationen zur Aufgabe "Schutz vor Netzwerkbedrohungen"
Standardeinstellungen der Aufgabe "Schutz vor Netzwerkbedrohungen"
Aufgabe "Schutz vor Netzwerkbedrohungen" über die Programmkonsole konfigurieren
Allgemeine Aufgabeneinstellungen
Ausnahmen hinzufügen
Aufgabe "Schutz vor Netzwerkbedrohungen" über das Verwaltungs-Plug-in konfigurieren
Allgemeine Aufgabeneinstellungen
Ausnahmen hinzufügen
Aufgabe "Schutz vor Netzwerkbedrohungen" über das Web-Plug-in konfigurieren
Allgemeine Aufgabeneinstellungen
Ausnahmen hinzufügen
Kontrolle des Programmstarts
Über die Aufgabe zur Kontrolle des Programmstarts
Über die Regeln für die Kontrolle des Programmstarts

Über die Kontrolle für Installationspakete
Über die Verwendung von KSN mit der Aufgabe Kontrolle des Programmstarts
Über das Erstellen von Regeln für die Kontrolle des Programmstarts
Standardeinstellungen der Aufgabe "Kontrolle des Programmstarts"
Kontrolle des Programmstarts über das Verwaltungs-Plug-in verwalten
Navigation
Richtlinieneinstellungen für die Aufgabe zur Kontrolle des Programmstarts öffnen
Regelliste für die Kontrolle des Programmstarts öffnen
Assistent und Eigenschaften für die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen
Aufgabe Kontrolle des Programmstarts konfigurieren
Konfiguration der Kontrolle für Installationspakete
Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren
Konfiguration von Regeln für die Kontrolle des Programmstarts über das Kaspersky Security Center
Regel für die Kontrolle des Programmstarts hinzufügen
Standarderlaubnismodus aktivieren
Erlaubnisregeln aus Ereignissen in Kaspersky Security Center erstellen
Regeln aus einem Bericht von Kaspersky Security Center über blockierte Programme importieren
Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren
Programmstarts testen
Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" erstellen
Gültigkeitsbereich der Aufgabe einschränken
Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln
Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln
Kontrolle des Programmstarts über die Programmkonsole verwalten
Navigation
Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen
Fenster "Regeln für die Kontrolle des Programmstarts" öffnen
Einstellungen der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen
Aufgabe Kontrolle des Programmstarts konfigurieren
Modus der Aufgabe zur Kontrolle des Programmstarts auswählen
Modus der Aufgabe zur Kontrolle des Programmstarts konfigurieren
Verwendung von KSN konfigurieren
Kontrolle für Installationspakete
Regeln für die Kontrolle des Programmstarts konfigurieren
Regel für die Kontrolle des Programmstarts hinzufügen
Standarderlaubnismodus aktivieren
Erlaubnisregeln aus Ereignissen der Aufgabe zur Kontrolle des Programmstarts erstellen
Regeln für die Kontrolle des Programmstarts exportieren
Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren
Regeln für die Kontrolle des Programmstarts löschen
Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren
Gültigkeitsbereich der Aufgabe einschränken
Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln
Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln
Kontrolle des Programmstarts über das Web-Plug-in verwalten
Gerätekontrolle
Über die Aufgabe Gerätekontrolle
Über die Regeln zur Gerätekontrolle

- Über die Erstellung von Regeln für die Gerätekontrolle
- Über die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle
- Standardeinstellungen der Aufgabe zur Gerätekontrolle
- Gerätekontrolle über das Verwaltungs-Plug-in verwalten
  - Navigation
    - Richtlinieneinstellungen für die Aufgabe zur Gerätekontrolle öffnen
    - Regelliste für die Gerätekontrolle öffnen
    - Assistent und Eigenschaften für die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle öffnen
  - Aufgabe zur Gerätekontrolle konfigurieren
  - Aufgabe zum Erstellen von Regeln für die Gerätekontrolle konfigurieren
  - Regeln für die Gerätekontrolle über das Kaspersky Security Center konfigurieren
    - Erlaubnisregeln auf Grundlage von Systemdaten des Systems in einer Richtlinie von Kaspersky Security Center erstellen
    - Regeln für angeschlossene Geräte erstellen
    - Regeln aus dem Bericht von Kaspersky Security Center über blockierte Geräte importieren
    - Regeln mithilfe der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen
    - Erzeugte Regeln in die Regelliste für die Gerätekontrolle aufnehmen
- Gerätekontrolle über die Programmkonsole verwalten
  - Navigation
    - Einstellungen der Aufgabe zur Gerätekontrolle öffnen
    - Fenster "Regeln für die Gerätekontrolle" öffnen
    - Einstellungen für das Erstellen von Regeln für die Gerätekontrolle öffnen
  - Einstellungen der Aufgabe Gerätekontrolle anpassen
  - Regeln für die Gerätekontrolle konfigurieren
    - Regeln für die Gerätekontrolle aus einer XML-Datei importieren
    - Liste der Regeln nach den Ereignissen der Aufgabe Gerätekontrolle erstellen
    - Erlaubnisregel für ein oder mehrere externe Geräte hinzufügen
    - Regeln der Gerätekontrolle löschen
    - Regeln der Gerätekontrolle exportieren
    - Regeln zur Gerätekontrolle aktivieren und deaktivieren
    - Gültigkeitsbereich der Regeln zur Gerätekontrolle erweitern
  - Aufgabe "Erstellen von Regeln für die Gerätekontrolle"
- Gerätekontrolle über das Web-Plug-in der Programmkonsole verwalten

Firewall-Verwaltung

- Über die Aufgabe zur Firewall-Verwaltung
- Über Firewall-Regeln
- Standardeinstellungen der Aufgabe zur Firewall-Verwaltung
- Firewall-Regeln über das Verwaltungs-Plug-in verwalten
  - Firewall-Regeln aktivieren und deaktivieren
  - Firewall-Regeln manuell hinzufügen
  - Firewall-Regeln löschen
- Firewall-Regeln über die Programmkonsole verwalten
  - Firewall-Regeln aktivieren und deaktivieren
  - Firewall-Regeln manuell hinzufügen
  - Firewall-Regeln löschen
- Firewall-Regeln über das Web-Plug-in verwalten
  - Firewall-Regeln aktivieren und deaktivieren
  - Firewall-Regeln manuell hinzufügen
  - Firewall-Regeln löschen

Überwachung der Datei-Integrität
Über die Aufgabe "Überwachung der Datei-Integrität"
Über die Regeln zur Überwachung von Datei-Operationen
Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität
Überwachung der Datei-Integrität über das Verwaltungs-Plug-in verwalten
Aufgabe "Überwachung der Datei-Integrität" anpassen
Einstellungen der Überwachungsregeln anpassen
Überwachung der Datei-Integrität über die Programmkonsole verwalten
Einstellungen der Aufgabe Überwachung der Datei-Integrität anpassen
Einstellungen der Überwachungsregeln anpassen
Überwachung der Dateiintegrität über das Web-Plug-in verwalten
Aufgabe "Überwachung der Datei-Integrität" anpassen
Einstellungen der Überwachungsregeln anpassen
Überwachung des Registrierungszugriffs
Über die Aufgabe zur Überwachung des Registrierungszugriffs
Über die Regeln zur Überwachung der Systemregistrierung
Standardeinstellungen der Aufgabe zur Überwachung des Registrierungszugriffs
Überwachung des Registrierungszugriffs über das Verwaltungs-Plug-in verwalten
Einstellungen der Aufgabe zur Überwachung des Registrierungszugriffs anpassen
Einstellungen der Überwachungsregeln anpassen
Überwachung des Registrierungszugriffs über die Verwaltungskonsole verwalten
Einstellungen der Aufgabe zur Überwachung des Registrierungszugriffs anpassen
Einstellungen der Überwachungsregeln anpassen
Überwachung des Registrierungszugriffs über das Web-Plug-in verwalten
Einstellungen der Aufgabe zur Überwachung des Registrierungszugriffs anpassen
Einstellungen der Überwachungsregeln anpassen
Protokollanalyse
Über die Aufgabe Protokollanalyse
Standardeinstellungen der Aufgabe "Protokollanalyse"
Regeln für die Protokollanalyse über das Verwaltungs-Plug-in verwalten
Regeln für vorkonfigurierte Aufgaben anpassen
Regeln für die Protokollanalyse über das Verwaltungs-Plug-in hinzufügen
Regeln für die Protokollanalyse über die Programmkonsole verwalten
Regeln für vorkonfigurierte Aufgaben anpassen
Regeln für die Protokollanalyse über die Programmkonsole hinzufügen
Regeln für die Protokollanalyse über das Web-Plug-in verwalten
Untersuchung auf Befehl
Über Aufgaben zur Untersuchung auf Befehl
Über den Untersuchungsbereich von Aufgaben und Sicherheitseinstellungen
Vordefinierte Untersuchungsbereiche
Untersuchung von Online-Speicherdateien
Über vordefinierte Sicherheitsstufen
Über die Untersuchung von Wechseldatenträgern
Über die Aufgabe zur Überwachung der Baseline-Integrität
Aktivieren des Starts von Untersuchungen auf Befehl aus dem Kontextmenü heraus.
Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl
Aufgaben zur Untersuchung auf Befehl über das Verwaltungs-Plug-in verwalten
Navigation

Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen
Aufgabeneigenschaften für die Untersuchung auf Befehl öffnen
Erstellen einer Aufgabe zur Untersuchung auf Befehl
Zuweisen des Status "Aufgabe zur Untersuchung wichtiger Bereiche" an eine Aufgabe zur Untersuchung auf Befehl
Ausführung einer Aufgabe im Hintergrund zur Untersuchung auf Befehl
Registrierung der Ausführung der Untersuchung wichtiger Bereiche
Untersuchungsbereich der Aufgabe anpassen
Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen
Sicherheitseinstellungen manuell anpassen
Allgemeine Aufgabeneinstellungen anpassen
Aktionen anpassen
Leistung optimieren
Untersuchung von Wechseldatenträgern anpassen
Aufgabe zur Überwachung der Baseline-Integrität anpassen
Aufgaben zur Untersuchung auf Befehl über die Programmkonsole verwalten
Navigation
Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen
Einstellungen des Gültigkeitsbereichs für die Aufgabe zur Untersuchung auf Befehl öffnen
Aufgabe zur Untersuchung auf Befehl erstellen und anpassen
Untersuchungsbereich in den Aufgaben zur Untersuchung auf Befehl
Einstellungen für die Anzeige der freigegebenen Netzwerkordner anpassen
Untersuchungsbereich erstellen
Netzwerkobjekte in den Untersuchungsbereich aufnehmen
Virtuelle Untersuchungsbereiche erstellen
Sicherheitseinstellungen anpassen
Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen
Allgemeine Aufgabeneinstellungen anpassen
Aktionen anpassen
Leistung optimieren
Konfigurieren des hierarchischen Speichers
Wechseldatenträger untersuchen
Statistik von Aufgaben zur Untersuchung auf Befehl
Aufgabe zur Überwachung der Baseline-Integrität erstellen und anpassen
Aufgaben zur Untersuchung auf Befehl über das Web-Plug-in verwalten
Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen
Aufgabeneigenschaften für die Untersuchung auf Befehl öffnen
Untersuchungsbereich der Aufgabe anpassen
Passen Sie die Aufgabeneinstellungen an
Vertrauenswürdige Zone
Über die vertrauenswürdige Zone
Vertrauenswürdige Zone über das Verwaltungs-Plug-in verwalten
Navigation
Richtlinieneinstellungen der vertrauenswürdigen Zone öffnen
Einstellungsfenster der vertrauenswürdigen Zone öffnen
Einstellungen der vertrauenswürdigen Zone über das Verwaltungs-Plug-in anpassen
Ausnahme hinzufügen
Vertrauenswürdige Prozesse hinzufügen
Anwenden der Not-a-virus-Maske

Vertrauenswürdige Zone über die Programmkonsole verwalten
Vertrauenswürdige Zone für Aufgaben in der Programmkonsole übernehmen
Einstellungen der vertrauenswürdigen Zone in der Programmkonsole konfigurieren
Ausnahme zur vertrauenswürdigen Zone hinzufügen
Vertrauenswürdige Prozesse hinzufügen
Anwenden der Not-a-virus-Maske
Vertrauenswürdige Zone über das Web-Plug-in verwalten
Exploit-Prävention
Über die Exploit-Prävention
Exploit-Prävention über das Verwaltungs-Plug-in verwalten
Navigation
Richtlinieneinstellungen für die Exploit-Prävention öffnen
Einstellungsfenster der Exploit-Prävention öffnen
Einstellungen zum Schutz des Prozess-Speichers anpassen
Hinzufügen eines Prozesses zum Schutzbereich
Exploit-Prävention über die Programmkonsole verwalten
Navigation
Allgemeine Einstellungen der Exploit-Prävention öffnen
Einstellungen der Exploit-Prävention für den Schutz von Prozessen öffnen
Einstellungen zum Schutz des Prozess-Speichers anpassen
Hinzufügen eines Prozesses zum Schutzbereich
Exploit-Prävention über das Web-Plug-in verwalten
Einstellungen zum Schutz des Prozess-Speichers anpassen
Hinzufügen eines Prozesses zum Schutzbereich
Exploit-Präventionstechniken
Integration mit Dritthersteller-Systemen
Leistungsindikatoren für das Programm Systemmonitor
Über Leistungsindikatoren in Kaspersky Embedded Systems Security
Gesamtzahl der abgelehnten Anfragen (Total number of requests denied)
Gesamtzahl der übersprungenen Anfragen (Total number of requests skipped).
Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden
Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden
Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers
Maximale Anzahl der Datenströme des File-Interception-Dispatchers
Anzahl der Elemente in der Warteschlange für infizierte Objekte
Anzahl der pro Sekunde verarbeiteten Objekte
SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security
Über SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security
SNMP-Indikatoren in Kaspersky Embedded Systems Security
Leistungsindikatoren
Indikatoren für Quarantäne
Indikator für Backup
Allgemeine Indikatoren
Update-Indikatoren
Indikatoren für den Echtzeitschutz für Dateien
SNMP-Traps und ihre Optionen in Kaspersky Embedded Systems Security
Beschreibungen und mögliche Werte der Optionen von SNMP-Traps in Kaspersky Embedded Systems Security
Integration mit WMI

Arbeiten mit Kaspersky Embedded Systems Security aus der Befehlszeile
Befehle
Hilfe für Befehle in Kaspersky Embedded Systems Security anzeigen: KAVSHELL HELP
Kaspersky Security Service starten und anhalten KAVSHELL START: KAVSHELL STOP
Einen ausgewählten Bereich untersuchen: KAVSHELL SCAN
Aufgabe "Untersuchung wichtiger Bereiche" starten: KAVSHELL SCANCRITICAL
Aufgaben asynchron verwalten: KAVSHELL TASK
Das PPL-Attribut entfernen: KAVSHELL CONFIG
Aufgaben zum Echtzeit-Computerschutz starten und beenden: KAVSHELL RTP
Aufgabe "Kontrolle des Programmstarts" verwalten: KAVSHELL APPCONTROL /CONFIG
Erstellen von Regeln für die Kontrolle des Programmstarts: KAVSHELL APPCONTROL /GENERATE
Regelliste für die Kontrolle des Programmstarts füllen: KAVSHELL APPCONTROL
Liste der Regeln für die Gerätekontrolle füllen: KAVSHELL DEVCONTROL
Die Aufgabe "Update der Programm-Datenbanken" starten: KAVSHELL UPDATE
Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security ausführen: KAVSHELL ROLLBACK
Protokollanalyse verwalten: KAVSHELL TASK LOG-INSPECTOR
Programm aktivieren: KAVSHELL LICENSE
Erstellung von Protokollen zur Ablaufverfolgung aktivieren, anpassen und deaktivieren: KAVSHELL TRACE
Log-Dateien für Kaspersky Embedded Systems Security defragmentieren: KAVSHELL VACUUM
iSwift-Basis bereinigen: KAVSHELL FBRESET
Anlegen von Dump-Dateien aktivieren und deaktivieren: KAVSHELL DUMP
Einstellungen importieren: KAVSHELL IMPORT
Einstellungen exportieren: KAVSHELL EXPORT
Integration in Microsoft Operation Management Suite: KAVSHELL OMSINFO
Die Aufgabe zur Überwachung der Baseline-Integrität verwalten: KAVSHELL FIM /BASELINE
Rückgabecodes der Befehle
Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP
Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL
Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR
Rückgabecodes für den Befehl KAVSHELL TASK
Rückgabecodes für den Befehl KAVSHELL RTP
Rückgabecodes für den Befehl KAVSHELL UPDATE
Rückgabecodes für den Befehl KAVSHELL ROLLBACK
Rückgabecodes für den Befehl KAVSHELL LICENSE
Rückgabecodes für den Befehl KAVSHELL TRACE
Rückgabecodes für den Befehl KAVSHELL FBRESET
Rückgabecodes für den Befehl KAVSHELL DUMP
Rückgabecodes für den Befehl KAVSHELL IMPORT
Rückgabecodes für den Befehl KAVSHELL EXPORT
Rückgabecodes für den Befehl KAVSHELL FIM /BASELINE
Kontaktaufnahme mit dem Technischen Support
Wie Sie technischen Support erhalten
Technischer Support über Kaspersky CompanyAccount
Protokolldatei und AVZ-Skript verwenden
Glossar
Administrationsserver
Aktiver Schlüssel
Antiviren-Datenbanken

- Archiv
- Aufgabe
- Aufgabeneinstellungen
- Autostart-Objekte
- Backup
- Dateimaske
- Desinfektion
- Ereignispriorität
- Fehlalarm
- Heuristische Analyse
- Infizierbare Datei
- Infiziertes Objekt
- Kaspersky Security Network (KSN)
- Laufzeit der Lizenz
- Lokale Aufgabe
- OLE-Objekt
- Quarantäne
- Richtlinie
- Schutzstatus
- Schwachstelle
- Sicherheitsstufe
- SIEM
- Update

Informationen über den Code von Drittherstellern

Markenrechtliche Hinweise

Über Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security schützt Computer und andere eingebettete Systeme unter Microsoft® Windows® (im Folgenden als "geschütztes Gerät" bezeichnet) vor Viren und anderen Bedrohungen der Computer-Sicherheit. Als Benutzer von Kaspersky Embedded Systems Security gelten Netzwerkadministratoren des Unternehmens und Mitarbeiter, die für den Antiviren-Schutz des Unternehmensnetzwerks zuständig sind.

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

- Geldautomaten (ATM)
- Verkaufsorte (POS)

Kaspersky Embedded Systems Security kann auf folgende Arten verwaltet werden:

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

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

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

Komponenten und Funktionen von Kaspersky Embedded Systems Security

Im Lieferumfang des Programms sind folgende Komponenten enthalten:

- **Echtzeitschutz für Dateien** Kaspersky Embedded Systems Security untersucht Objekte, wenn darauf zugegriffen wird. Kaspersky Embedded Systems Security untersucht die folgenden Objekte:
  - Dateien
  - Alternative Datenströme der Dateisysteme (NTFS-Streams)
  - Master Boot Records und Bootsektoren von lokalen Festplatten und Wechseldatenträgern.
- **Untersuchung auf Befehl**/ Kaspersky Embedded Systems Security überprüft den angegebenen Bereich einmalig auf Viren und andere Bedrohungen der Computersicherheit. Das Programm prüft die Dateien, den Arbeitsspeicher sowie die Autostart-Objekte des geschützten Geräts.
- **Kontrolle des Programmstarts**. Diese Komponente überwacht die Versuche der Benutzer, Programme zu starten, und regelt den Programmstart auf einem geschützten Gerät.
- **Gerätekontrolle**. Die Komponente ermöglicht eine Kontrolle der Registrierung und der Verwendung von externen Geräten, um das Gerät vor Bedrohungen für die Computersicherheit zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können.

- **Firewall-Verwaltung**. Diese Komponente ermöglicht die Verwaltung der Windows Firewall: Sie erlaubt die Anpassung der Einstellungen und Regeln der Firewall des Betriebssystems und sperrt sämtliche Möglichkeiten zur externen Konfiguration der Firewall.

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

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

Das Programm verfügt über folgenden Funktionen:

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

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

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

- **Benachrichtigungen an den Administrator und die Benutzer**. Sie können die Benachrichtigung des Administrators und der Benutzer, die auf das geschützte Gerät zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Embedded Systems Security und dem Status des Antiviren-Schutzes auf dem Gerät zusammenhängen, anpassen.

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

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

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

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

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

- **Exploit-Prävention**. Sie können den Prozess-Speicher mithilfe des in die Prozesse eingebetteten Schutz-Agenten vor Exploits schützen.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Neuerungen

Die neue Version von Kaspersky Embedded Systems Security führt die folgenden neuen Funktionen und Verbesserungen ein:

- Die folgenden Betriebssysteme werden jetzt unterstützt:
  - Microsoft Windows 10 21H2
  - Microsoft Windows 11
- Lizenzverwaltung: Wenn der Lizenzschlüssel abläuft, bleiben alle Systemkomponenten funktionstüchtig, außer die Komponente zum Update der Programm-Datenbanken und dem Dienst von Kaspersky Security Network.
- Der Lizenzverwaltung wurde die Unterstützung von Aktivierungscodes hinzugefügt.
- Verbesserung in den Einstellungen der System-Diagnose: In der Aufgabe Überwachung der Dateiintegrität können Sie jetzt das Modifizieren von Dateien im ausgewählten Überwachungsbereich blockieren, nachdem Sie eine entsprechende Regel dafür erstellt haben. Außerdem können Sie die vertrauenswürdige Zone anwenden, um vertrauenswürdige Objekte und vertrauenswürdiger Benutzer aus dem Überwachungsbereich auszuschließen.
- Verbesserung in den Einstellungen der System-Diagnose: In der Aufgabe Überwachung des Registrierungszugriffs können Sie Statistiken erstellen oder Änderungen an den Schlüsseln und Werten der Systemregistrierung im ausgewählten Überwachungsbereich blockieren, nachdem Sie eine entsprechende Regel dafür erstellt haben. Außerdem können Sie die vertrauenswürdige Zone anwenden, um vertrauenswürdige Prozesse und vertrauenswürdiger Benutzer aus dem Überwachungsbereich auszuschließen.
- Es wurde die Option zur Aktivierung der Kontrolle des frühzeitigen Starts des Dienstes von Kaspersky Embedded Systems Security hinzugefügt.
- Für den in Kaspersky Security Center aufrufbaren Komponenten-Statusbericht wurden die Anzahl an standardmäßigen Statuswerten erweitert. Mit den neuen Statuswerten können Sie feststellen, ob sich eine Komponente im Modus "Aktiv" befindet, oder ob sie nur Statistiken erstellt und über Bedrohungen informiert.
- Verbesserung in den Einstellungen des Selbstschutzes: In den Einstellungen von Kaspersky Embedded Systems Security und dem Verwaltungs-Plug-in für Kaspersky Embedded Systems Security ist es jetzt möglich den Schutz der Dateien und Registrierungswerte von Kaspersky Embedded Systems Security gegen externe Bedrohungen zu aktiveren oder zu deaktivieren.
- Wenn Sie Kaspersky Embedded Systems Security starten, weist das Programm den geschützten Geräten individuelle Tags zu. Die Tags unterstützen Sie dabei, verschiedene Geräte, die in einem Pool aus geschützten Geräten mit dem gleichen Namen und der gleichen IP-Adresse registriert sind, zu unterscheiden.
- Die folgenden Dialoge des Web-Plug-ins des Programms stehen jetzt den Benutzern von Kaspersky Security Center zur Verfügung:
  - Überwachung der Datei-Integrität
  - Kontrolle des Programmstarts
  - Protokollanalyse
- Sie können Kaspersky Embedded Systems Security als Teil der Kaspersky Cloud Console verwenden.
- In Kaspersky Embedded Systems Security können Sie für die Dienste von Kaspersky Security Service den Modus für den verzögerten Start konfigurieren. In diesem Modus startet Kaspersky Security Service erst,

nachdem alle anderen Komponenten des Betriebssystems geladen sind.

- Anpassungen für die Aufgabe zur Gerätekontrolle: Die Aufgabe kann jetzt für verbundene USB-Geräte, welche die UAS-Technologie unterstützen, Statistiken erstellen oder die Geräte blockieren.
- In der Online-Dokumentation wurde jetzt die Tabelle mit Programmlebenszyklen verlinkt.
- Bugs aus den Vorgängerversionen wurden behoben: Das Programm enthält Fehlerbehebungen, die für die Vorgängerversionen herausgegeben wurden.

Informationsquellen über Kaspersky Embedded Systems Security

Dieser Abschnitt enthält die Beschreibung von Informationsquellen zum Programm.

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

Quellen für die selbstständige Informationssuche

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

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

Sollten Sie ein aufgetretenes Problem nicht selbst lösen können, wenden Sie sich bitte an den Technischen Support von Kaspersky.

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

Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky

Auf der Seite von Kaspersky Embedded Systems Security stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

Auf der Seite für Kaspersky Embedded Systems Security befindet sich ein Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite von Kaspersky Embedded Systems Security in der Wissensdatenbank

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

Auf der Seite von Kaspersky Security für Windows Server in der Wissensdatenbank finden Sie Artikel, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Erwerb, zur Installation und zur Anwendung des Programms enthalten.

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

Dokumentation für Kaspersky Embedded Systems Security

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

Diskussion über die Programme von Kaspersky in der Community

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie diese mit den Spezialisten von Kaspersky und mit anderen Benutzern in unserer Community diskutieren.

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

Kaspersky Embedded Systems Security

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

Lieferumfang

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

- Installationsassistent für Kaspersky Embedded Systems Security starten.
- Installationsassistent für die Konsole für Kaspersky Embedded Systems Security starten.
- Starten Sie den Installationsassistenten für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security, um das Programm über Kaspersky Security Center zu verwalten.
- Das Administratorhandbuch lesen.
- Zur Seite von Kaspersky Embedded Systems Security auf der Website von Kaspersky wechseln.
- Website des Technischen Supports aufrufen.
- Informationen über die aktuelle Version von Kaspersky Embedded Systems Security lesen.

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

Der Ordner \product enthält Folgendes:

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

Der Ordner \product_no_avbases enthält Installationsdateien für Kaspersky Embedded Systems Security-Komponenten und das Verwaltungs-Plug-in 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).

Dateien im Lieferumfang von Kaspersky Embedded Systems Security

Datei	Ziel
autorun.inf	Autostart-Datei des Installationsassistenten von Kaspersky Embedded Systems Security bei der Programminstallation von Wechseldatenträgern.
release_notes.txt	Datei enthält Ausgabedaten.

migration.txt	Diese Datei beschreibt die Migration von vorherigen Programmversionen.
setup.exe	Startdatei des Begrüßungsprogramms (startet setup.hta).
\console\esstools_x86.msi	Windows Installer-Paket; installiert die Programmkonsole auf dem geschützten Gerät, auf dem die 32-Bit-Version eines Microsoft Windows-Betriebssystems ausgeführt wird.
\console\esstools_x64.msi	Windows Installer-Paket; installiert die Programmkonsole auf dem geschützten Gerät, auf dem die 64-Bit-Version eines Microsoft Windows-Betriebssystems ausgeführt wird.
\console\setup.exe	Startdatei für den Assistenten zur Installation des Komponentensatzes "Administrationswerkzeuge" (dazu gehört die Programmkonsole). Sie 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	Datei für die Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät über den Assistenten. Sie startet die Datei des Installationspakets ess.msi mit den im Assistenten angegebenen Installationseinstellungen.
\product\ess_x86.msi	Windows-Installer-Paket - Installiert die Konfiguration von Kaspersky Embedded Systems Security zum **Schützen des Computers mit Antiviren-Datenbanken** auf dem geschützten Gerät mit einem 32-Bit-Microsoft Windows-Betriebssystem. Wenn die Konfiguration zum "Schützen des Computers mit Antiviren-Datenbanken" ausgewählt ist, sind standardmäßig alle Komponenten von Kaspersky Embedded Systems Security enthalten, mit Ausnahme der Komponenten zur Firewall-Verwaltung und für die Leistungsindikatoren. Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit Antiviren-Datenbanken über eine Programmversion" installieren, die keine Signaturanalyse und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, werden die Programmkomponenten automatisch um die folgenden Module erweitert: • Echtzeitschutz für Dateien • Untersuchung auf Befehl • Schutz vor Netzwerkbedrohungen
\product\ess_x64.msi	Windows-Installer-Paket - Installiert Kaspersky Embedded Systems Security in der **Konfiguration für den Schutz des Computers mit Antiviren-Datenbanken** auf dem geschützten Gerät mit einem 64-Bit-Microsoft Windows-Betriebssystem.

	Wenn die Konfiguration zum "Schützen des Computers mit Antiviren-Datenbanken" ausgewählt ist, sind standardmäßig alle Komponenten von Kaspersky Embedded Systems Security enthalten, mit Ausnahme der Komponenten zur Firewall-Verwaltung und für die Leistungsindikatoren. Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit Antiviren-Datenbanken über eine Programmversion" installieren, die keine Signaturanalyse und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, werden die Programmkomponenten automatisch um die folgenden Module erweitert: • Echtzeitschutz für Dateien • Untersuchung auf Befehl • Schutz vor Netzwerkbedrohungen
\product\ess.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center.
\product\klcfginst.exe	Installationsprogramm für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security über das Kaspersky Security Center. Installieren Sie das Verwaltungs-Plug-in auf dem geschützten Gerät, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist, wenn Sie Kaspersky Embedded Systems Security mit dieser Konsole verwalten möchten.
\product\license.txt	Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
\product_long_term\setup.exe	Datei für die Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät über den Assistenten. Sie startet die Datei des Installationspakets ess.msi mit den im Assistenten angegebenen Installationseinstellungen.
\product_long_term\ess_x86.msi	Windows-Installer-Paket: Installiert die Konfiguration von Kaspersky Embedded Systems Security zum **Schützen des Computers mit der Technologie des standardmäßigen Verbots** auf dem geschützten Gerät mit einem 32-Bit-Microsoft Windows-Betriebssystem.

	Die Komponenten, die Updates ermöglichen, sind nicht enthalten in der Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen". Wenn die Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen" ausgewählt ist, sind folgende Komponenten standardmäßig enthalten: • core • Exploit-Prävention • Kontrolle des Programmstarts • Taskleistensymbol Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit der Technologie des standardmäßigen Verbots" über die Programmversion installieren, die Signaturanalyse- und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz von Programmkomponenten automatisch reduziert, indem die folgende Komponente entfernt wird: • Echtzeitschutz für Dateien • Untersuchung auf Befehl • die Komponenten, die Updates ermöglichen Diese Konfiguration ist empfohlen für den Schutz von Systemen mit begrenzten Ressourcen. In diesem Fall können Sie das Programm langfristig aktivieren und die Komponente Kontrolle des Programmstarts bietet Computerschutz.
\product_long_term\ess_x64.msi	Windows-Installer-Paket: Installiert Kaspersky Embedded Systems Securit in der **Konfiguration für den Schutz des Computers mit der Technologie des standardmäßigen Verbots** (Default Deny) auf dem geschützten Gerät mit einem 64-Bit-Microsoft Windows-Betriebssystem.

	Die Komponenten, die Updates ermöglichen, sind nicht enthalten in der Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen". Wenn die Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen" ausgewählt ist, sind folgende Komponenten standardmäßig enthalten: • core • Exploit-Prävention • Kontrolle des Programmstarts • Taskleistensymbol Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit der Technologie des standardmäßigen Verbots" über die Programmversion installieren, die Signaturanalyse- und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz von Programmkomponenten automatisch reduziert, indem die folgende Komponente entfernt wird: • Echtzeitschutz für Dateien • Untersuchung auf Befehl • die Komponenten, die Updates ermöglichen Diese Konfiguration ist empfohlen für den Schutz von Systemen mit begrenzten Ressourcen. In diesem Fall können Sie das Programm langfristig aktivieren und die Komponente Kontrolle des Programmstarts bietet Computerschutz.
\product_long_term\ess_light.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center.
\product_long_term\klcfginst.exe	Installationsprogramm für das Verwaltungs-Plug-in für Kaspersky Embedded Systems Security über das Kaspersky Security Center. Installieren Sie das Verwaltungs-Plug-in auf dem geschützten Gerät, auf dem die Kaspersky Security Center Verwaltungskonsole installiert ist, wenn Sie Kaspersky Embedded Systems Security mit dieser Konsole verwalten möchten.
\product_long_term\license.txt	Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
\setup\setup.hta	Datei für den Start des Begrüßungsprogramms.

Hard- und Software-Voraussetzungen

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

Softwarevoraussetzungen für das geschützte Gerät

Sie können die Programmkonsole auf einem Gerät installieren, dass mit einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows arbeitet.

Windows Installer 3.1 ist erforderlich, damit das Programm ordnungsgemäß auf einem geschützten Gerät unter Microsoft Windows XP installiert und ausgeführt werden kann.

Für die Installation und Verwendung von Kaspersky Embedded Systems Security auf geschützten Geräten mit eingebetteten Betriebssystemen ist die Komponente "Filter Manager" erforderlich.

Stellen Sie vor der Installation von Kaspersky Embedded Systems Security sicher, dass die benötigten Updates für die Unterstützung von SHA-2 auf für die Betriebssysteme der geschützten Geräte installiert ist. Bei fehlender Unterstützung für SHA-2 kann es passieren, das die installierten Programm-Module nicht ordnungsgemäß ausgeführt werden, was zu Fehlfunktionen des Betriebssystems führt. Informationen dazu finden Sie hier: https://support.kaspersky.com/de/15728.

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

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

- Windows 10 version 1607 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 version 1703 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 version 1709 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 version 1803 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 version 1809 Professional / Enterprise / IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 19H2 Professional/Enterprise/IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 21H2 Professional/Enterprise/IoT Enterprise (32-Bit, 64-Bit)
- Windows 10 Enterprise LTSC 2016 (32-Bit, 64-Bit)
- Windows 10 Enterprise LTSC 2019 (32-Bit, 64-Bit)
- Windows 10 Enterprise LTSC 2021 (32-Bit, 64-Bit)
- Windows 11 21H2 Professional / Enterprise (64-Bit)

Hardwarevoraussetzungen für das geschützte Gerät

Die Hardwarevoraussetzungen für das geschützte Gerät richten sich nach dem installierten Windows-Betriebssystem:

- Hardwarevoraussetzungen für ein Gerät unter dem Betriebssystem Windows XP (32-/64-Bit), Windows Embedded XP, Windows Embedded POSReady 2009 oder Windows Embedded POSReady 7:
  - Minimalkonfiguration:
    - Benötigter Speicherplatz:
      - Für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB.
      - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 2 GB.
    - RAM:
      - 256 MB für die alleinige Installation der Komponente zur Kontrolle des Programmstarts unter einem Microsoft Windows-Betriebssystem.
      - 512 MB für die vollständige Installation aller Komponenten.
    - Anforderungen an den Prozessor:
      - Für 32-Bit-Microsoft Windows-Betriebssysteme:

        1,4 GHz Einkernprozessor

        Intel® Pentium® III.
      - Für 64-Bit-Microsoft Windows-Betriebssysteme:

1,4 GHz Einkernprozessor

Intel Pentium IV

- Empfohlene Konfiguration:
  - Benötigter Speicherplatz:
    - Für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB.
    - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 4 GB.
  - RAM: 2 GB.
  - Anforderungen an den Prozessor: 2,4 GHz Vierkernprozessor

- Hardwarevoraussetzungen für ein Gerät unter dem Betriebssystem Windows Embedded 7, Windows Embedded 8 oder Windows Embedded 10:
  - Minimalkonfiguration:
    - Benötigter Speicherplatz:
      - Für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB.
      - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 2 GB.
    - RAM: 1 GB.
    - Anforderungen an den Prozessor: 1,4 GHz Intel Pentium IV Einkernprozessor.
  - Empfohlene Konfiguration:
    - Benötigter Speicherplatz:
      - Für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB.
      - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 4 GB.
    - RAM: 2 GB.
    - Anforderungen an den Prozessor: 2,4 GHz Vierkernprozessor

- Hardwarevoraussetzungen für ein Gerät unter dem Betriebssystem Windows 7 (64-Bit), Windows 8 (64-Bit), Windows 10 (64-Bit) oder Windows 11 (64-Bit):
  - Minimalkonfiguration:
    - Benötigter Speicherplatz:
      - Für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB.
      - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 2 GB.
    - RAM:

- 1 GB für die alleinige Installation der Komponente zur Kontrolle des Programmstarts unter einem Microsoft Windows-Betriebssystem.
- 2 GB für die vollständige Installation aller Komponenten.

- Anforderungen an den Prozessor:

  1,4 GHz Einkernprozessor

  Intel Pentium IV.

- Empfohlene Konfiguration:
  - Benötigter Speicherplatz:
    - Für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB.
    - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 4 GB.
  - RAM:
    - 2 GB für die alleinige Installation der Komponente zur Kontrolle des Programmstarts unter einem Microsoft Windows-Betriebssystem.
    - 4 GB für die vollständige Installation aller Komponenten.
  - Anforderungen an den Prozessor: 2,4 GHz Vierkernprozessor

- Hardwarevoraussetzungen für ein Gerät unter dem Betriebssystem Windows 7 (32-Bit), Windows 8 (32-Bit) oder Windows 10 (32-Bit):
  - Minimalkonfiguration:
    - Benötigter Speicherplatz:
      - Für die Installation der Komponente zur Kontrolle des Programmstarts: 50 MB.
      - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 2 GB.
    - RAM:
      - 256 MB für die alleinige Installation der Komponente zur Kontrolle des Programmstarts unter einem Microsoft Windows-Betriebssystem.
      - 1 GB für die vollständige Installation aller Komponenten.
    - Anforderungen an den Prozessor:
      - Für 32-Bit-Microsoft Windows-Betriebssysteme:

        1,4 GHz Einkernprozessor

        Intel Pentium III.

      - Für 64-Bit-Microsoft Windows-Betriebssysteme:

1,4 GHz Einkernprozessor

Intel Pentium IV

- Empfohlene Konfiguration:
  - Benötigter Speicherplatz:
    - Für die Installation der Komponente zur Kontrolle des Programmstarts: 2 GB.
    - Für die Installation aller Komponenten von Kaspersky Embedded Systems Security: 4 GB.
  - RAM: 2 GB.
  - Anforderungen an den Prozessor: 2,4 GHz Vierkernprozessor

Funktionale Anforderungen und Einschränkungen

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

Installation und Deinstallation

- Während der Programminstallation erscheint eine Warnung, wenn der neue Pfad zum Installationsordner von Kaspersky Embedded Systems Security mehr als 150 Zeichen enthält. Die Warnung hat keine Auswirkung auf den Installationsvorgang: Kaspersky Embedded Systems Security wird ordnungsgemäß installiert und ausgeführt.
- Um die Komponente "Unterstützung des SNMP-Protokolls" zu installieren, muss der SNMP-Dienst neu gestartet werden, falls dieser läuft.
- Für die Installation und den Betrieb von Kaspersky Embedded Systems Security auf einem Gerät, auf dem ein Embedded-Betriebssystem ausgeführt wird, muss die Komponente "Filter Manager" installiert sein.
- Die Administrations-Tools für Kaspersky Embedded Systems Security können nicht über die Gruppenrichtlinien von Microsoft Active Directory® installiert werden.
- Bei der Installation des Programms auf geschützten Geräten mit älteren Betriebssystemen, die keine regelmäßigen Updates beziehen können, sollten Sie die folgenden Stammzertifikate überprüfen: DigiCert Assured ID Root CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Wenn diese Zertifikate nicht vorhanden sind, wird das Programm möglicherweise nicht korrekt ausgeführt. Wir empfehlen Ihnen, diese Zertifikate mit einer beliebigen, Ihnen verfügbaren Methode zu installieren.

Überwachung der Datei-Integrität

Standardmäßig werden keine Änderungen an Systemordnern oder an den Housekeeping-Dateien des Dateisystems von der Komponente "Überwachung der Datei-Integrität" erfasst, damit Aufgabenberichte nicht mit Informationen über regelmäßige Dateiänderungen überladen werden, die das Betriebssystem ausführt. Der Benutzer kann solche Ordner nicht manuell zum Überwachungsbereich hinzufügen.

Die folgenden Ordner/Dateien werden aus dem Überwachungsbereich ausgeschlossen.

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

Das Programm schließt Verzeichnisse der obersten Ebene aus.

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

Firewall-Verwaltung

- Die Verwendung von IPv6-Adressen ist nicht verfügbar, wenn der festgelegte Regelbereich aus einer einzigen Adresse besteht.
- Die vorkonfigurierten Richtlinienregeln der Firewall unterstützen grundlegende Interaktionsszenarien zwischen den geschützten Geräten und dem Administrationsserver. Um alle Funktionen von Kaspersky Security Center

zu verwenden, müssen die Portregeln manuell eingerichtet werden. Weitere Informationen über Portnummern, Protokolle und deren Funktionen unter https://support.kaspersky.com/KSC/13.2/de-DE/158830.htm.

- Das Programm kontrolliert während der Aufgabe "Firewall-Verwaltung" keine Änderungen in den Windows Firewall-Regeln und Regelgruppen, wenn diese Regeln während der Programminstallation nicht zur Konfiguration der Aufgabe hinzugefügt wurden. Um den Status zu aktualisieren und solche Regeln einzuschließen, muss die Aufgabe "Firewall-Verwaltung" neu gestartet werden.

- Wenn die Aufgabe "Firewall-Verwaltung" gestartet wird, werden die folgenden Regeltypen automatisch aus den Einstellungen des Betriebssystems entfernt:

  - Verbotsregeln

  - Regeln zur Überwachung von ausgehendem Datenverkehr

Andere Einschränkungen

Untersuchung auf Befehl, **Echtzeitschutz für Dateien**:

- Die Untersuchung von über das MTP-Protokoll angeschlossenen Geräten ist nicht verfügbar.

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

- Wenn das Kontrollkästchen **Tiefere Analyse startender Prozesse (Blockiert den Start eines Prozesses, bis die Analyse abgeschlossen ist)** und der Dienst **Verwendung von KSN** gleichzeitig aktiviert sind, wird jeder gestartete Prozess, der URL-Web-Adressen als Argument erhält, selbst dann blockiert, wenn der Modus "Nur Statistik" ausgewählt wurde. Um ein Blockieren des Prozesses zu vermeiden, wählen Sie eine der folgenden Optionen aus:

  - Deaktivieren Sie den Dienst **Verwendung von KSN**

  - Deaktivieren Sie das Kontrollkästchen **Tiefere Analyse startender Prozesse (Blockiert den Start eines Prozesses, bis die Analyse abgeschlossen ist)**

  Empfohlene Option: Das Deaktivieren des Kontrollkästchens für die tiefere Analyse startender Prozesse

Lizenzverwaltung:

- Die Aktivierung des Programms mit einem Schlüssel über den Installationsassistenten ist nicht möglich, wenn der Schlüssel auf einem Laufwerk gespeichert ist, das mithilfe des Befehls SUBST erstellt wurde, oder wenn für die Schlüsseldatei ein Netzwerkpfad eingegeben wurde.

Updates:

- Nach der Installation von Updates für kritische Module von Kaspersky Embedded Systems Security wird das Programmsymbol standardmäßig ausgeblendet.

- KLRAMDISK wird auf geschützten Geräten unter Windows XP oder Windows Server 2003 nicht unterstützt.

Oberfläche:

- Beachten Sie die Groß- und Kleinschreibung bei der Verwendung der Filterfunktion in der Programmkonsole für die Bereiche Quarantäne, Backup, Systemaudit-Protokoll oder Protokoll der Aufgabenausführung.

- Wenn Sie einen Schutz- oder Untersuchungsbereich in der Programmkonsole konfigurieren, können Sie nur eine Maske verwenden und sie nur am Pfadende platzieren. Dies sind einige Beispiele für richtige Masken: "C:\Temp\Temp*" oder "C:\Temp\Temp???.doc" und "C:\Temp\Temp*.doc". Diese Einschränkung betrifft nicht die Konfiguration der vertrauenswürdigen Zone.

Sicherheit:

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

- Das Programm kann nicht über das Microsoft Windows-Fenster **Programme und Funktionen** deinstalliert werden, wenn die Benutzerkontensteuerung aktiviert ist.

Integration in Kaspersky Security Center:

- Der Administrationsserver prüft Updates der Programm-Datenbanken, wenn Update-Pakete empfangen wurden, bevor die Updates an die geschützten Geräte im Netzwerk weitergeleitet werden. Der Administrationsserver prüft keine Updates der Programm-Module.

- Stellen Sie sicher, dass die Kontrollkästchen in den Einstellungen für "Interaktion mit Administrationsserver" aktiviert sind, wenn Sie Komponenten verwenden, die mithilfe von Netzwerklisten (Quarantäne, Backup) dynamische Daten an Kaspersky Security Center übermitteln.

Exploit-Prävention:

- Die Exploit-Prävention ist nicht verfügbar, wenn die Bibliotheken apphelp.dll in der aktuellen Umgebungskonfiguration nicht geladen sind.

- Die Komponente "Exploit-Prävention" ist auf geschützten Geräten mit dem Betriebssystem Microsoft Windows 10 nicht mit dem Microsoft-Dienstprogramm EMET kompatibel: Kaspersky Embedded Systems Security blockiert EMET, wenn die Komponente "Exploit-Prävention" auf einem geschützten Gerät installiert wird, auf dem EMET bereits installiert ist.

Programm installieren und deinstallieren

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

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

Die Dateien \product_long_term\ess_x86.msi und \product_long_term\ess_x64.msi dienen zur Installation der Konfiguration von Kaspersky Embedded Systems Security für das **Schützen des Computers mit der Technologie des standardmäßigen Verbots**. Die Dateien \product\ess_x86.msi und \product\ess_x64.msi wurden entwickelt, um die Konfiguration von Kaspersky Embedded Systems Security für das **Schützen des Computers mit Antiviren-Datenbanken** zu installieren.

Wenn die Konfiguration zum "Schützen des Computers mit Antiviren-Datenbanken" ausgewählt ist, sind standardmäßig alle Komponenten von Kaspersky Embedded Systems Security enthalten, mit Ausnahme der Komponenten zur Firewall-Verwaltung und für die Leistungsindikatoren.

Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit Antiviren-Datenbanken über eine Programmversion" installieren, die keine Signaturanalyse und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, werden die Programmkomponenten automatisch um die folgenden Module erweitert:

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

Die Komponenten, die Updates ermöglichen, sind nicht enthalten in der Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen".

Wenn die Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen" ausgewählt ist, sind folgende Komponenten standardmäßig enthalten:

- core
- Exploit-Prävention
- Kontrolle des Programmstarts
- Taskleistensymbol

Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit der Technologie des standardmäßigen Verbots" über die Programmversion installieren, die Signaturanalyse- und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz von Programmkomponenten automatisch reduziert, indem die folgende Komponente entfernt wird:

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

Diese Konfiguration ist empfohlen für den Schutz von Systemen mit begrenzten Ressourcen. In diesem Fall können Sie das Programm langfristig aktivieren und die Komponente Kontrolle des Programmstarts bietet Computerschutz.

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

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

Die Programmkomponenten von Kaspersky Embedded Systems Security

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

Beschreibung der Programmkomponenten von Kaspersky Embedded Systems Security

Komponente	Kennzeichnung	Ausgeführte Funktion
Hauptfunktionen	core	Diese Komponente beinhaltet ein Paket von Basisfunktionen des Programms und gewährleistet deren Ausführung. Wenn Sie beim Installieren von Kaspersky Embedded Systems Security aus der Befehlszeile andere Komponenten von Kaspersky Embedded Systems Security angeben, ohne die Core-Komponente anzugeben, wird die Core-Komponente automatisch installiert.
Kontrolle des Programmstarts	AppCtrl	Diese Komponente überwacht die Versuche von Benutzern, Programme zu starten, und erlaubt oder verbietet den

		Programmstart in Übereinstimmung mit den angegebenen Regeln für die Kontrolle des Programmstarts. Die Komponente wird in der Aufgabe "Kontrolle des Programmstarts" realisiert.
Gerätekontrolle	DevCtrl	Diese Komponente überwacht die Verbindungsversuche von externen Geräten auf einem geschützten Gerät und verbietet oder erlaubt deren Verwendung entsprechend den festgelegten Regeln für die Gerätekontrolle. Die Komponente wird in der Aufgabe Gerätekontrolle realisiert.
Antiviren-Schutz	AVProtection	Diese Komponente stellt den Antiviren-Schutz bereit und beinhaltet die folgenden Komponenten: • Untersuchung auf Befehl • Echtzeitschutz für Dateien • Schutz vor Netzwerkbedrohungen
Schutz vor Netzwerkbedrohungen	IDS	Diese Komponente untersucht eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind. Wird ein versuchter Netzwerkangriff erkannt, der auf den Computer abzielt, blockiert Kaspersky Embedded Systems Security die Netzwerkaktivitäten vom angreifenden Computer.
Untersuchung auf Befehl	Ods	Diese Komponente installiert die Systemdateien von Kaspersky Embedded Systems Security und stellt Aufgaben zur Untersuchung auf Befehl bereit (Untersuchung von Objekten des geschützten Geräts auf Anforderung).
Echtzeitschutz für Dateien	Oas	Diese Komponente führt auf dem geschützten Gerät eine Untersuchung von Dateien auf Viren durch, sobald auf diese Dateien zugegriffen wird. Sie setzt die Aufgabe Echtzeitschutz für Dateien um.
Verwendung von Kaspersky Security Network.	KSN	Diese Komponente gewährleistet den Schutz auf Basis der Cloud-Technologien von Kaspersky. 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.
Überwachung des Registrierungszugriffs	RegMonitor	Diese Komponente ermöglicht das Überwachen von Vorgängen, die in Registrierungszweigen und -schlüsseln durchgeführt wurden, welche im Überwachungsbereich der Aufgabeneinstellungen festgelegt wurden. Mithilfe der Aufgabe können Sie Änderungen erkennen, die eventuell auf eine Verletzung der Sicherheit auf dem geschützten Gerät hindeuten. Die Komponente implementiert die Aufgabe "Überwachung des Registrierungszugriffs".

Exploit-Prävention	AntiExploit	Diese Komponente ermöglicht die Verwaltung der Einstellungen zum Schutz des Prozess-Speichers im Speicher des Geräts.
Firewall-Verwaltung	Firewall	Diese Komponente ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Embedded Systems Security zu verwalten. Die Komponente wird in der Aufgabe Firewall-Verwaltung umgesetzt.
Modul für die Integration in den Administrationsagenten von Kaspersky Security Center	AKIntegration	Diese Komponente stellt eine Verbindung zwischen Kaspersky Embedded Systems Security und dem Administrationsagenten von Kaspersky Security Center bereit. Sie können diese Komponente auf dem geschützten Gerät installieren, wenn Sie vorhaben, das Programm über Kaspersky Security Center zu verwalten.
Protokollanalyse	LogInspector	Diese Komponente führt eine Integritätsprüfung des geschützten Mittwochs auf Grundlage der Ergebnisse der Protokollanalyse von Windows-Ereignissen aus.
Satz von Leistungsindikatoren der Anwendung "Systemmonitor"	PerfMonCounters	Diese Komponente installiert Leistungsindikatoren des Programms Systemmonitor. Leistungsindikatoren messen die Leistungsfähigkeit von Kaspersky Embedded Systems Security und finden mögliche Engpässe bei gleichzeitiger Ausführung von Kaspersky Embedded Systems Security und anderen Programmen.
SNMP-Indikator und Traps	SnmpSupport	Die Komponente veröffentlicht die Indikatoren und Traps für Kaspersky Embedded Systems Security über den Dienst Simple Network Management Protocol (SNMP) von Microsoft Windows. Sie können diese Komponente nur auf dem geschützten Gerät installieren, wenn der SNMP-Dient von Microsoft auf diesem geschützten Gerät installiert ist.
Benarchitigungssymbol von Kaspersky Embedded Systems Security im Infobereich	TrayApp	Die Komponente zeigt das Symbol für Kaspersky Embedded Systems Security im Infobereich der Taskleiste des geschützten Geräts an. Das Symbol für Kaspersky Embedded Systems Security zeigt den Status des Schutzes auf dem Gerät an und erlaubt, die Konsole für Kaspersky Embedded Systems Security in der Microsoft Management Console (falls installiert) und das Fenster **Über das Programm** zu öffnen.

Programmkomponente "Administrations-Tools"

Die folgende Tabelle enthält den Code und die Beschreibung der Programmkomponente "Administrations-Tools".

Beschreibung der Programmkomponente "Administrations-Tools"

Komponente	Code	Funktionen der Komponente
Snap-ins von Kaspersky Embedded Systems Security	MmcSnapin	Die Komponente installiert das Microsoft Management Console Snap-in für die Verwaltung der Anwendung mittels der Konsole für Kaspersky Embedded Systems Security. Wenn Sie beim Installieren von "Administrations-Tools" aus der Befehlszeile andere Komponenten angeben, ohne die MmcSnapin-Komponente zu nennen, wird die Komponente automatisch installiert.

Systemänderungen nach der Installation von Kaspersky Embedded Systems Security

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

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

Diese Änderungen sind nachfolgend beschrieben.

Ordner für Kaspersky Embedded Systems Security auf einem geschützten Gerät

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

- Standardinstallationsordner für Kaspersky Embedded Systems Security mit den ausführbaren Dateien von Kaspersky Embedded Systems Security, abhängig vom Bit-Satz des Betriebssystems. Daher lauten die Installationsordner wie folgt:
  - In der 32-Bit-Version von Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - In der 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- Dateien für die Management Information Base (MIB) mit einer Beschreibung der Indikatoren und Traps, die von Kaspersky Embedded Systems Security mit dem SNMP-Protokoll veröffentlicht werden.
  - %Kaspersky Embedded Systems Security%\mibs
- 64-Bit-Version der ausführbaren Dateien von Kaspersky Embedded Systems Security (dieser Ordner wird nur erstellt, wenn Kaspersky Embedded Systems Security unter einer 64-Bit-Version von Microsoft Windows installiert wird):
  - %Kaspersky Embedded Systems Security%\x64
- Dienstdateien für Kaspersky Embedded Systems Security:
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Dskm

Für Microsoft Windows XP lautet der Pfad zum Kaspersky-Lab-Ordner %ALLUSERSPROFILE%\Application Data

- Dateien mit Einstellungen für Update-Quellen:

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update

- Datenbanken-Updates und Updates der Programm-Module, die mithilfe der Aufgabe zur Update-Verteilung empfangen wurden (der Ordner wird erstellt, wenn zum ersten Mal Updates mithilfe der Aufgabe zur Update-Verteilung empfangen werden).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update\Distribution

- Berichte über Aufgabenausführung und Systemaudit-Bericht.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Reports

- Derzeit verwendetes Datenbankpaket.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Bases\Current

- Backup-Kopien der Datenbanken; werden bei jedem Datenbanken-Update überschrieben.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Bases\Backup

- Temporäre Dateien, die beim Ausführen der Update-Aufgabe angelegt werden.

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Bases\Temp

- Objekte in der Quarantäne (standardmäßiger Ordner).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Quarantine

- Objekte im Backup (standardmäßiger Ordner).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Backup

- Objekte, die aus Backup oder Quarantäne wiederhergestellt wurden (standardmäßiger Ordner für die Wiederherstellung von Objekten).

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Restored

Ordner, der bei der Installation der Programmkonsole erstellt wird

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

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

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

Dienste von Kaspersky Embedded Systems Security

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

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

Gruppe in Kaspersky Embedded Systems Security

"ESS-Administratoren" ist eine Gruppe auf dem geschützten Gerät, deren Benutzer Vollzugriff auf Kaspersky Security Management Service sowie Zugriff auf alle Funktionen von Kaspersky Embedded Systems Security haben.

Schlüssel der Systemregistrierung

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

- Eigenschaften von Kaspersky Embedded Systems Security:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Einstellungen des Ereignisprotokolls von Kaspersky Embedded Systems Security (Ereignisprotokoll "Kaspersky"):
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Eigenschaften des Management Service von Kaspersky Embedded Systems Security:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- Einstellungen für den Leistungsindikator:
  - In der 32-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - In der 64-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- Parameter für die Komponente Unterstützung des SNMP-Protokolls:
  - In der 32-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\SnmpAgent]
  - In der 64-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\SnmpAgent]
- Einstellungen für die Dump-Datei:
  - In der 32-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\CrashDump]
  - In der 64-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\CrashDump]

- Einstellungen für Protokolldateien:
  - In der 32-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\Trace]
  - In der 64-Bit-Version von Microsoft Windows:
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\Trace]
- Konfiguration der Aufgaben und Funktionen des Programms:
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\Environment]

Prozesse von Kaspersky Embedded Systems Security

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

Prozesse von Kaspersky Embedded Systems Security

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

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

Dieser Abschnitt enthält Beschreibungen der Einstellungen für die Installation und Deinstallation von Kaspersky Embedded Systems Security, ihrer Standardwerte und der Schlüssel für die Änderung der Einstellungswerte sowie deren mögliche Werte. Sie können diese Schlüssel gemeinsam mit den Standardschlüsseln für den Befehl `msiexec` des Dienstes Windows Installer verwenden, wenn Sie Kaspersky Embedded Systems Security aus der Befehlszeile installieren.

Installationseinstellungen und Optionen für die Befehlszeile im Windows Installer

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

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

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

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

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

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

- Die Installation von Kaspersky Embedded Systems Security erlauben, wenn das Update KB4528760 nicht installiert ist. Detaillierte Informationen über das Update KB4528760 finden Sie auf der Microsoft-Website.

  Die möglichen Werte für die Befehlszeilenoption `SKIPCVEWINDOWS10=<Wert>` lauten wie folgt:

  - `0` – Installation von Kaspersky Embedded Systems Security abbrechen, wenn das Update KB4528760 nicht installiert ist (Standardwert).
  - `1` – Installation von Kaspersky Embedded Systems Security zulassen, wenn das Update KB4528760 nicht installiert ist.

  Das Update KB4528760 schließt die Sicherheitsschwachstelle CVE-2020-0601. Detaillierte Informationen über die Sicherheitsschwachstelle CVE-2020-0601 finden Sie auf der Microsoft-Website.

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

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

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

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

  Die Standardwerte für die Befehlszeilenoption `INSTALLDIR=<vollständiger Pfad des Ordners>` lauten wie folgt:

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

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

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

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

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

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

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

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

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

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

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

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

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

- Pfad der Schlüsseldatei (`LICENSEKEYPATH`)

  Der Windows Installer sucht standardmäßig in dem im Lieferumfang enthaltenen Ordner \product nach einer Datei mit der Erweiterung .key. Wenn der Ordner \product mehrere Schlüsseldateien enthält, wählt der Windows Installer die Schlüsseldatei aus, deren Gültigkeitsdauer zuletzt abläuft. Sie können die Schlüsseldatei zuvor im Ordner \product speichern oder mit dem Installationsparameter **Schlüssel hinzufügen** einen anderen Pfad für die Schlüsseldatei angeben. Sie können nach der Installation von Kaspersky Embedded Systems Security einen Schlüssel mithilfe der von Ihnen gewählten Administrations-Tools hinzufügen, zum Beispiel mit der Programmkonsole. Wenn Sie während der Programminstallation keinen Programmschlüssel hinzufügen, funktioniert Kaspersky Embedded Systems Security nicht.

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

  Der Standardwert für `CONFIGPATH=<Name der Konfigurationsdatei>` ist nicht festgelegt.

- Die Option "Netzwerkverbindungen für die Programmkonsole aktivieren" wird verwendet, um die Konsole für Kaspersky Embedded Systems Security auf einem anderen Gerät zu installieren. Mit der Konsole für Kaspersky Embedded Systems Security können Sie den Geräteschutz über ein anderes Gerät ferngesteuert verwalten. Auf dem Computer wird in der Microsoft-Windows Firewall Port 135 (TCP) geöffnet, Netzwerkverbindungen werden für die ausführbare Datei kavfsrcn.exe zur Fernverwaltung von Kaspersky Embedded Systems Security erlaubt und der Zugriff auf DCOM-Programme wird zugelassen. Wenn die Installation abgeschlossen ist, fügen

Sie Benutzer zur Gruppe der ESS-Administratoren hinzu, damit diese das Programm ferngesteuert verwalten können, und erlauben Sie Netzwerkverbindungen für Kaspersky Security Management Service (Datei kavfsgt.exe) auf dem geschützten Gerät. Erfahren Sie mehr über die weitere Konfiguration bei Installation der Konsole für Kaspersky Embedded Systems Security auf einem anderen Gerät.

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

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

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

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

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

Deinstallationsparameter und Optionen für die Befehlszeile für den Dienst Windows Installer

- Wiederherstellung von Objekten aus der Quarantäne

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

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

- Wiederherstellen des Backup-Inhalts

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

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

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

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

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

  Der Standardwert für die Befehlszeilenoption `RESTOREPATH=<vollständiger Pfad des Ordners>` lautet %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Restored

Installations- und Deinstallationsprotokolle für Kaspersky Embedded Systems Security

Wenn Sie die Installation oder Deinstallation von Kaspersky Embedded Systems Security mit Hilfe des Assistenten zur Installation (Deinstallation) starten, erstellt der Dienst Windows Installer ein Protokoll über die Installation (Deinstallation). Eine Log-Datei mit dem Namen ess_v3.1_install_<uid>.log (wobei <uid> eine eindeutige Protokoll-ID mit 8 Zeichen ist) wird im Ordner %temp% des Benutzers gespeichert, dessen Konto für den Start der Datei setup.exe verwendet wurde.

Wenn Sie für die Programmkonsole oder für Kaspersky Embedded Systems Security über das Menü **Start** die Option **Ändern oder Löschen** ausführen, wird im Ordner %temp% automatisch eine Log-Datei mit dem Namen "ess_3.1_maintenance.log" erstellt.

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

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

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

Installation planen

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

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

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

Administrations-Tools auswählen

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

Konsole für Kaspersky Embedded Systems Security

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

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

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

Befehlszeilen-Utility

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

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

Kaspersky Security Center

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

Die folgenden Programmkomponenten müssen installiert werden:

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

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

- **Kaspersky Embedded Systems Security 3.1 Verwaltungs-Plug-in** Installieren Sie auf dem geschützten Gerät, auf dem die Verwaltungskonsole für Kaspersky Security für Windows Server installiert ist, zusätzlich das Verwaltungs-Plug-in für den Kaspersky Security Center-Administrationsserver. Dadurch wird eine Schnittstelle zur Programmverwaltung über Kaspersky Security Center bereitgestellt. Die Installationsdatei für das Verwaltungs-Plug-in \product\klcfginst.exe gehört zum Lieferumfang von Kaspersky Embedded Systems Security.

Installationstyp auswählen

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

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

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

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

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

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

Installationsassistent starten

Mit dem Installationsassistenten können Sie installieren:

- Die Komponenten von Kaspersky Embedded Systems Security auf einem geschützten Gerät aus der Datei \product\setup.exe, die im Lieferumfang enthalten ist.
- Konsole für Kaspersky Embedded Systems Security aus der Datei console\setup.exe aus dem Lieferumfang auf dem geschützten Gerät oder einem anderen LAN-Host.

Datei des Installationspaketes mit den erforderlichen Installationseinstellungen aus der Befehlszeile starten

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

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

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

Zentrale Installation über Kaspersky Security Center

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

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

Zentrale Installation über Gruppenrichtlinien des Active Directory

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

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

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

Installation und Deinstallation des Programms mit dem Assistenten

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

Installation mit dem Installationsassistenten

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

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

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

Installation von Kaspersky Embedded Systems Security

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

1. Vergewissern Sie sich, dass auf dem geschützten Gerät keine anderen Antiviren-Programme installiert sind.
2. Vergewissern Sie sich, dass das Benutzerkonto, mit dessen Berechtigungen Sie den Installationsassistenten starten, zur Administratorengruppe auf dem geschützten Gerät gehört.

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

Erfahren Sie mehr über die Installations- bzw. Deinstallationseinstellungen.

So installieren Sie Kaspersky Embedded Systems Security mithilfe des Installationsassistenten:

1. Starten Sie auf dem geschützten Gerät die Datei setup.exe.

2. Klicken Sie im folgenden Fenster im Abschnitt **Installation** entweder auf den Link zum **Computer mittels Default Deny-Technologie schützen** oder auf den Link zum **Computer mittels Antiviren-Datenbanken schützen**.

   Wenn die Konfiguration zum "Schützen des Computers mit Antiviren-Datenbanken" ausgewählt ist, sind standardmäßig alle Komponenten von Kaspersky Embedded Systems Security enthalten, mit Ausnahme der Komponenten zur Firewall-Verwaltung und für die Leistungsindikatoren.

   Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit Antiviren-Datenbanken über eine Programmversion" installieren, die keine Signaturanalyse und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, werden die Programmkomponenten automatisch um die folgenden Module erweitert:

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

   Die Komponenten, die Updates ermöglichen, sind nicht enthalten in der Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen".

   Wenn die Konfiguration "Computer mit der Technologie des standardmäßigen Verbots (Default Deny) schützen" ausgewählt ist, sind folgende Komponenten standardmäßig enthalten:

   - core
   - Exploit-Prävention
   - Kontrolle des Programmstarts
   - Taskleistensymbol

   Wenn Sie die Konfiguration von Kaspersky Embedded Systems Security zum "Schützen des Computers mit der Technologie des standardmäßigen Verbots" über die Programmversion installieren, die Signaturanalyse- und Antiviren-Datenbanken zum Schutz Ihres Computers verwendet, wird der Satz von Programmkomponenten automatisch reduziert, indem die folgende Komponente entfernt wird:

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

   Diese Konfiguration ist empfohlen für den Schutz von Systemen mit begrenzten Ressourcen. In diesem Fall können Sie das Programm langfristig aktivieren und die Komponente Kontrolle des Programmstarts bietet Computerschutz.

3. Klicken Sie im Begrüßungsfenster des Installationsassistenten von Kaspersky Embedded Systems Security auf die Schaltfläche **Weiter**.

   Das Fenster **Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie** wird geöffnet.

4. Lesen Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.

5. Wenn Sie den Bedingungen des Endbenutzer-Lizenzvertrags zustimmen, aktivieren Sie die Kontrollkästchen **Ich bestätige, dass ich alle Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe, und sie**

verstehe und akzeptiere und **Ich bin mir bewusst und damit einverstanden, dass meine Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Ich bestätige, dass ich die Datenschutzrichtlinie vollständig gelesen habe und sie verstehe**, um mit der Installation fortzufahren.

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

6. Klicken Sie auf **Weiter**.

   Das Fenster **Benutzerdefinierte Installation** wird geöffnet.

7. Wählen Sie die Komponente, die Sie installieren wollen.

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

8. Um alle Änderungen im Fenster **Benutzerdefinierte Installation** zu verwerfen, klicken Sie auf die Schaltfläche **Zurücksetzen**. Klicken Sie auf **Weiter**.

9. Gehen Sie im Fenster **Zielordner auswählen** wie folgt vor:

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

   Klicken Sie auf **Weiter**.

10. Passen Sie im Fenster **Erweiterte Einstellungen für die Installation** folgende Installationseinstellungen an:

    - **Echtzeitschutz nach der Installation des Programms aktivieren**.
    - **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**.
    - **Dateien, die von Kaspersky empfohlen werden, zu Ausnahmen hinzufügen**.

      Klicken Sie auf **Weiter**.

11. Gehen Sie im Fenster **Einstellungen aus einer Konfigurationsdatei importieren** wie folgt vor:

    a. Um die Einstellungen für Kaspersky Embedded Systems Security aus einer vorhandenen Konfigurationsdatei zu importieren, die in einer kompatiblen Vorgängerversion der Anwendung erstellt wurde, geben Sie die Konfigurationsdatei an.

    b. Klicken Sie auf **Weiter**.

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

    - Wenn Sie das Programm aktivieren möchten, geben Sie die Schlüsseldatei für Kaspersky Embedded Systems Security zur Aktivierung des Programms an.
    - Wenn Sie das Programm später aktivieren möchten, klicken Sie auf die Schaltfläche **Weiter**.

- Wenn zuvor eine Schlüsseldatei im Ordner \product (der zum Lieferumfang gehört) gespeichert wurde, wird der Name dieser Datei im Feld **Schlüssel** angezeigt.

  Um einen Schlüssel aus der Datei, die in einem anderen Ordner gespeichert ist, hinzuzufügen, geben Sie die Schlüsseldatei an.

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

  Klicken Sie auf die Schaltfläche **Weiter**, um die Schlüsseldatei für das Programm zu übernehmen.

13. Klicken Sie im Fenster **Bereit zur Installation** auf die Schaltfläche **Installieren**. Der Assistent installiert nun die Komponenten von Kaspersky Embedded Systems Security.

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

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

16. Klicken Sie auf **Fertig**.

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

Installation der Konsole für Kaspersky Embedded Systems Security

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

So installieren Sie die Programmkonsole:

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

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

   Das Fenster des Willkommen-Programms wird geöffnet.

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

   Es öffnet sich das Begrüßungsfenster des Installationsassistenten.

4. Klicken Sie auf **Weiter**.

5. Lesen Sie sich die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie im geöffneten Fenster durch und aktivieren Sie das Kontrollkästchen unter der Zeile **Ich bestätige, dass ich alle Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe, und sie verstehe und akzeptiere**, um mit der Installation fortzufahren.

6. Klicken Sie auf **Weiter**.

   Das Fenster **Erweiterte Einstellungen für die Installation** wird geöffnet.

7. Gehen Sie im folgenden Fenster **Erweiterte Einstellungen für die Installation** wie folgt vor:

   - Wenn Sie planen, Kaspersky Embedded Systems Security auf einem Remote-Gerät mithilfe der Programmkonsole zu verwalten, aktivieren Sie das Kontrollkästchen **Remote-Zugriff erlauben**.
   - Um das Fenster **Benutzerdefinierte Installation** zu öffnen und Komponenten auszuwählen, gehen Sie wie folgt vor:

     a. Klicken Sie auf die Schaltfläche **Erweitert**.

     Das Fenster **Benutzerdefinierte Installation** wird geöffnet.

     b. Wählen Sie die "Administrations-Tools" aus der Liste aus.

     Standardmäßig werden alle Komponenten installiert.

     c. Klicken Sie auf **Weiter**.

   Lesen Sie detailliertere Informationen über die Komponenten von Kaspersky Embedded Systems Security.

8. Gehen Sie im Fenster **Zielordner auswählen** wie folgt vor:

   a. Geben Sie bei Bedarf einen anderen Ordner an, in dem die zu installierenden Dateien gespeichert werden sollen.

   b. Klicken Sie auf **Weiter**.

9. Klicken Sie im Fenster **Bereit zur Installation** auf die Schaltfläche **Installieren**.

   Der Assistent installiert nun die ausgewählten Komponenten.

10. Klicken Sie auf **Fertig**.

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

Wenn Sie das Paket "Administrations-Tools" nicht auf dem geschützten Gerät, sondern auf einem anderen Netzwerkgerät installiert haben, passen Sie die erweiterten Einstellungen an.

Erweiterte Einstellungen nach der Installation der Programmkonsole auf einem anderen Gerät

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

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

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

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

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

  Das Gerät, auf dem die Programmkonsole installiert ist, verwendet TCP-Port 135, um auf das geschützte Gerät zuzugreifen und eine Antwort zu empfangen.
- Konfigurieren Sie eine ausgehende Regel für die Windows-Firewall, um die Verbindung zu erlauben.

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

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

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

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

   Die neuen Verbindungseinstellungen werden übernommen.

Anonymen Remote-Zugriff auf COM-Anwendungen erlauben

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

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

1. Öffnen Sie auf dem Remote-Gerät, auf dem die Konsole für Kaspersky Embedded Systems Security installiert ist, die Komponentendienste-Konsole.
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 geschützten Geräts den Knoten **Computer**.
6. Öffnen Sie das Kontextmenü im Knoten **Arbeitsplatz**.
7. Wählen Sie den Menüpunkt **Eigenschaften**.
8. Klicken Sie auf der Registerkarte **COM-Sicherheit** im Fenster **Eigenschaften** auf die Schaltfläche **Beschränkungen ändern** in der Einstellungsgruppe **Zugriffsrechte**.
9. Vergewissern Sie sich im Fenster **Remote-Zugriff erlauben**, dass für den Benutzer ANONYMOUS LOGON das Kontrollkästchen **Remote-Zugriff erlauben** aktiviert ist.
10. Klicken Sie auf **OK**.

Netzwerkverbindungen für Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security erlauben

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

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

1. Schließen Sie die Konsole für Kaspersky Embedded Systems Security auf dem Remote-Gerät.
2. Führen Sie eine der Aktionen durch:
   - In Microsoft Windows XP SP2 oder höher:
     a. Wählen Sie **Start** > **Windows Firewall** aus.
     b. Klicken Sie im Fenster **Windows-Firewall** (oder Einstellungen für Windows-Firewall) auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Port hinzufügen**.
     c. Geben Sie im Feld **Name** den Portnamen RPC (TCP/135) an, oder geben Sie einen anderen Namen an, z. B. DCOM für Kaspersky Embedded Systems Security. Geben Sie im Feld **Portnummer** die Nummer des Ports (135) an.
     d. Wählen Sie das Protokoll **TCP**.
     e. Klicken Sie auf **OK**.
     f. Klicken Sie auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Hinzufügen**.
   - In Microsoft Windows 7 und höher:
     a. Wählen Sie **Start** > **Systemsteuerung** > **Windows Firewall**.
     b. Wählen Sie im Fenster **Windows-Firewall** den Punkt **Ein Programm oder Feature durch die Windows-Firewall zulassen**.

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

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

4. Klicken Sie auf **OK**.

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

Ausgehende Regel für die Windows-Firewall hinzufügen

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

So fügen Sie die ausgehende Regel für die Windows-Firewall hinzu:

1. Wählen Sie **Start** > **Systemsteuerung** > **Windows Firewall**.

2. Klicken Sie im Fenster **Windows-Firewall** auf den Link **Erweiterte Einstellungen**.

   Das Fenster **Windows-Firewall mit erweiterter Sicherheit** wird geöffnet.

3. Aktivieren Sie den untergeordneten Knoten **Ausgehende Regeln**.

4. Klicken Sie im Bereich **Aktionen** auf die Option **Neue Regel**.

5. Wählen Sie im nächsten Fenster des **Assistenten für neue Ausgangsregeln** die Option **Port** aus und klicken Sie auf **Weiter**.

6. Wählen Sie das Protokoll **TCP**.

7. Geben Sie im Feld **Bestimmte Remote-Ports** den folgenden Bereich für Ports an, um ausgehende Verbindungen zuzulassen: 1024-65535.

8. Wählen Sie im Fenster **Aktion** die Option **Verbindung zulassen** aus.

9. Speichern Sie die neue Regel und schließen Sie das Fenster **Windows-Firewall mit erweiterter Sicherheit**.

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

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

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

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

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

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

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

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

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

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

So aktualisieren Sie die Programm-Datenbank nach der Installation:

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

2. Start der Aufgabe zum Update der Programm-Datenbanken.

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

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

1. Öffnen Sie das Kontextmenü des Knotens **Kaspersky Embedded Systems Security**.

2. **Wählen Sie das** Element Eigenschaften aus.

   Das Fenster **Programmeinstellungen** wird geöffnet.

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

4. Wählen Sie im Abschnitt **Proxyserver-Einstellungen** das Kontrollkästchen **Angegebenen Proxyserver verwenden**.

5. Geben Sie die Proxyserver-Adresse in das Feld **Adresse** ein und geben Sie die Portnummer für den Proxyserver in das Feld **Port** ein.

6. Wählen Sie im Abschnitt **Einstellungen für die Authentifizierung auf dem Proxyserver** die erforderliche Authentifizierungsmethode aus der Dropdown-Liste:

   - **NTLM-Authentifizierung verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung (NTLM-authentication) unterstützt. Kaspersky Embedded Systems Security benutzt für den Zugriff auf den Proxyserver das Benutzerkonto, das in den Aufgabeneinstellungen angegeben ist (standardmäßig läuft die Aufgabe unter dem Benutzerkonto **Lokales System** (**SYSTEM**)).

   - **NTLM-Authentifizierung mit Benutzername und Kennwort verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung unterstützt. Kaspersky Embedded Systems Security verwendet das von Ihnen vorgegebene Benutzerkonto für den Zugriff auf den Proxyserver. Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.

   - **Benutzername und Kennwort verwenden**, um die übliche Authentifizierung auszuwählen (Basic authentication). Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.

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

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

1. Starten Sie die Programmkonsole mit einer der folgenden Methoden:

   - Öffnen Sie die Programmkonsole auf dem geschützten Gerät. Wählen Sie dazu **Start** > **Alle Programme** > **Kaspersky Embedded Systems Security** > **Administrations-Tools** > **Konsole für Kaspersky Security 11 für Windows Server**.

   - Wenn die Programmkonsole nicht auf dem geschützten, sondern auf einem anderen Gerät gestartet wurde, stellen Sie eine Verbindung mit dem geschützten Gerät her:

     a. Öffnen Sie das Kontextmenü des Knotens **Kaspersky Embedded Systems Security** in der Struktur der Programmkonsole.

     b. Wählen Sie den Punkt **Verbindung mit anderem Computer herstellen** aus.

     c. Wählen Sie im Fenster **Geschütztes Gerät auswählen** die Option **Anderes Gerät** und geben Sie im Eingabefeld den Netzwerknamen des geschützten Geräts an.

     Wenn das Benutzerkonto, mit dem Sie sich in Microsoft Windows angemeldet haben, über keine Zugriffsrechte für den Verwaltungsdienst Kaspersky Security Management Service verfügt, geben Sie ein Benutzerkonto mit den erforderlichen Rechten an.

   Das Fenster "Programmkonsole" wird geöffnet.

2. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.

3. Wählen Sie den untergeordneten Knoten **Update der Programm-Datenbanken** aus.

4. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

5. Öffnen Sie im nächsten Fenster **Aufgabeneinstellungen** die Registerkarte **Verbindungseinstellungen**.

6. Aktivieren Sie **Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Update-Servern verwenden**.

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

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

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

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.

2. Wählen Sie im Kontextmenü des untergeordneten Knotens **Update der Programm-Datenbanken** den Punkt **Starten**.

Die Aufgabe zum Update der Programm-Datenbanken wird gestartet.

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

Untersuchung wichtiger Bereiche

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

So führen Sie die Aufgabe "Untersuchung wichtiger Bereiche" aus:

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie im Kontextmenü des untergeordneten Knotens **Untersuchung wichtiger Bereiche** den Befehl **Starten**.

Die Aufgabe wird gestartet. Im Ergebnisfenster wird der Aufgabenstatus **Läuft** angezeigt.

Um das Protokoll der Aufgabenausführung anzuzeigen, machen Sie Folgendes,

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

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

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

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

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

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

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

2. Wählen Sie **Auswahl der Programmkomponenten ändern** aus. Klicken Sie auf **Weiter**.

   Das Fenster **Benutzerdefinierte Installation** wird geöffnet.

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

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

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

     - **Die Komponente und ihre Teilkomponenten werden auf der lokalen Festplatte installiert**, wenn Sie eine Gruppe von Komponenten installieren möchten.

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

   Klicken Sie auf **Weiter**.

4. Bestätigen Sie im Fenster **Bereit zur Installation** den Vorgang zur Änderung der Zusammensetzung der Programmkomponenten, indem Sie auf die Schaltfläche **Installieren** klicken.

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

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

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

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

1. Wählen Sie im Menü **Start** die Option **Alle Programme** aus.

2. Wählen Sie **Kaspersky Embedded Systems Security** aus.

3. Wählen Sie **Kaspersky Embedded Systems Security ändern oder löschen** aus.

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

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

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

5. Aktivieren Sie im Fenster **Installierte Komponenten reparieren** das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**, wenn Sie die Einstellungen des Programms zurücksetzen und Kaspersky Embedded Systems Security mit den vorinstallierten Standardeinstellungen wiederherstellen möchten. Klicken Sie auf **Weiter**.

6. Bestätigen Sie im Fenster **Bereit zur Wiederherstellung** den Vorgang zur Wiederherstellung der Zusammensetzung des Programms, indem Sie auf die Schaltfläche **Installieren** klicken.

7. Klicken Sie im Fenster, das nach Abschluss des Reparaturvorgangs geöffnet wird, auf **OK**.

Kaspersky Embedded Systems Security wird gemäß den angegebenen Einstellungen repariert.

Deinstallation mit dem Installationsassistenten

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

Deinstallation von Kaspersky Embedded Systems Security

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der angegeben wurde bei dem Erstellen von Dump-Dateien und Protokolldateien anpassen.

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

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

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

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

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

So deinstallieren Sie Kaspersky Embedded Systems Security:

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

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

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

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

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

   c. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie den Ordner an, in den Sie die Objekte exportieren möchten. Standardmäßig erfolgt der Export von Objekten in den Ordner: %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall.

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

Kaspersky Embedded Systems Security wird vom geschützten Gerät deinstalliert.

Deinstallation der Konsole für Kaspersky Embedded Systems Security

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

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

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

Um die Programmkonsole zu deinstallieren:

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

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

4. Wählen Sie die Variante **Entfernen von Programmkomponenten** und klicken Sie auf **Weiter**.
5. Das Fenster **Bereit zur Deinstallation** wird geöffnet. Klicken Sie auf die Schaltfläche **Entfernen**.

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

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

Installation und Deinstallation des Programms aus der Befehlszeile

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

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

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der angegeben wurde bei dem Erstellen von Dump-Dateien und Protokolldateien anpassen.

Sie können Kaspersky Embedded Systems Security installieren oder deinstallieren, sowie seine Komponenten hinzufügen oder entfernen, indem Sie die Dateien des Installationspakets \product\ess_x86.msi oder \product\ess_x64.msi aus der Befehlszeile starten und die Installationseinstellungen mithilfe von Schlüsseln angeben.

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

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

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

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

Beispiele von Befehlen für die Installation von Kaspersky Embedded Systems Security

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

Starten Sie Dateien auf einem geschützten Gerät mit der 32-Bit-Version von Microsoft Windows mit dem Suffix x86 des Lieferumfangs. Starten Sie auf geschützte Geräten mit 64-Bit-Version von Microsoft Windows die Dateien aus dem Lieferumfang, die den Suffix x64 besitzen.

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

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

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

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

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

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

Um dies zu tun, geben Sie den folgenden Befehl ein:

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

Beispiele für Befehle zur Installation: eine msi-Datei starten

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Komponenten hinzufügen und entfernen. Beispiele für Befehle

Die Komponente für die Kontrolle des Programmstarts wird automatisch installiert.

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

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

oder

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

Nachdem Sie die Komponenten zur Liste hinzugefügt haben, installiert Kaspersky Embedded Systems Security die bestehenden Komponenten neu, mitsamt den angegebenen Komponenten.

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

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

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

```
msiexec /i ess.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

Wenn Sie die Komponenten, die Sie installieren oder deinstallieren möchten, aufgelistet haben, installiert und deinstalliert Kaspersky Embedded Systems Security die Komponenten entsprechend.

Deinstallation von Kaspersky Embedded Systems Security. Beispiele für Befehle

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

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

oder

- Für 32-Bit-Betriebssysteme:
  ```
  msiexec /x {941B0F6E-2DFA-4557-90AE-D9DF81E985C2} /qn
  ```
- Für 64-Bit-Betriebssysteme:
  ```
  msiexec /x {6BF23C65-7BE8-44F8-8B7F-3A6B419F6816} /qn
  ```

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

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

oder

```
msiexec /x {71FB9E57-9F23-4D72-B762-E0314EF3C814} /qn
```

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

- Für 32-Bit-Betriebssysteme:
  ```
  msiexec /x {941B0F6E-2DFA-4557-90AE-D9DF81E985C2} UNLOCK_PASSWORD=*** /qn
  ```
- Für 64-Bit-Betriebssysteme:
  ```
  msiexec /x {6BF23C65-7BE8-44F8-8B7F-3A6B419F6816} UNLOCK_PASSWORD=*** /qn
  ```

Rückgabecodes

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

Rückgabecodes

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

27301	Der Treiber kann nicht gelöscht werden.
27302	Die Netzwerkkomponente kann nicht installiert werden. Der obere Grenzwert der unterstützten Anzahl der Geräte zur Filterung wurde erreicht.
27303	Die Antiviren-Datenbanken wurden nicht gefunden.

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

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

Allgemeine Informationen zur Installation über Kaspersky Security Center

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

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

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

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

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

Rechte zur Installation bzw. Deinstallation von Kaspersky Embedded Systems Security

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

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

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

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

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

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

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

Installation von Kaspersky Embedded Systems Security über Kaspersky Security Center

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

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

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

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

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

1. Starten Sie die Verwaltungskonsole von Kaspersky Security Center.
2. Öffnen Sie in Kaspersky Security Center den Knoten **Erweitert**.

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

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

5. Wählen Sie als Installationspakettyp **Installationspaket für ein Kaspersky-Programm erstellen** aus.

6. Geben Sie den Namen des Installationspakets ein.

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

   Das Fenster **Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie** wird geöffnet.

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

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

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

   a. Erweitern Sie in Kaspersky Security Center den Knoten **Remote-Installation**.

   b. Öffnen Sie im Ergebnisbereich des untergeordneten Knotens **Installationspakete** das Kontextmenü für das neu erstellte Installationspaket von Kaspersky Embedded Systems Security. Wählen Sie dort den Befehl **Eigenschaften**.

   c. Öffnen Sie im Fenster **Eigenschaften: <Name des Installationspakets>** den Abschnitt **Einstellungen**.

      Aktivieren Sie in der Einstellungsgruppe **Zu installierende Komponenten** die Kontrollkästchen neben den Namen der Komponenten von Kaspersky Embedded Systems Security, die Sie installieren möchten.

   d. 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 geschützten Gerät nicht existiert, wird er erstellt.

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

      - **Geschütztes Gerät vor der Installation auf Viren untersuchen**
      - **Echtzeitschutz nach der Installation des Programms aktivieren**
      - **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**
      - **Dateien, die von Kaspersky empfohlen werden, zu Ausnahmen hinzufügen**
      - **Aktivieren Sie für die Dienste von Kaspersky Security Service den verzögerten Start beim Hochfahren des Betriebssystems**

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

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

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

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

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

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

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

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

1. Für die Gruppe der geschützten Geräte, auf denen Sie Kaspersky Embedded Systems Security installiert haben, eine Aufgabe zum Update der Programm-Datenbanken erstellen. Geben Sie den Kaspersky Security Center-Administrationsserver als Update-Quelle an.

2. Eine Gruppenaufgabe zur Untersuchung auf Befehl mit dem Status Untersuchung wichtiger Bereiche erstellen. Das Programm Kaspersky Security Center bewertet den Sicherheitszustand jedes geschützten Geräts der Gruppe dann aufgrund der Ergebnisse dieser Gruppe, nicht nach den Ergebnissen der Systemaufgabe Untersuchung wichtiger Bereiche.

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

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

Installation der Programmkonsole über das Kaspersky Security Center

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

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

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

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

3. Klicken Sie im Ergebnisfenster des untergeordneten Knotens "Installationspakete" auf die Schaltfläche **Installationspaket erstellen**. Während Sie das neue Installationspaket erstellen:

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

   b. Geben Sie den Namen des neuen Installationspakets ein.

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

   d. Falls erforderlich, ändern Sie im Feld **Starteinstellungen für ausführbare Datei (optional)** mithilfe der Einstellung ADDLOCAL die Auswahl der zu installierenden Komponenten und ändern Sie den Zielordner.

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

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

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

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

5. Starten Sie die Aufgabe zur Remote-Installation.

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

Deinstallation von Kaspersky Embedded Systems Security über Kaspersky Security Center

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der angegeben wurde bei dem Erstellen von Dump-Dateien und Protokolldateien anpassen.

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

So deinstallieren Sie Kaspersky Embedded Systems Security:

1. Erstellen und starten Sie in der 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; siehe vorhergehender Abschnitt) und geben Sie das Benutzerkonto an, unter dem der Administrationsserver auf die geschützten Geräte zugreifen soll. Sie können Kaspersky Embedded Systems Security nur mit den Standardinstallationseinstellungen deinstallieren.

Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory

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

Installation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory

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

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

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

Sie müssen über Administratorrechte auf der Domain verfügen.

Um Kaspersky Embedded Systems Security zu installieren, verwenden Sie das Installationspaket ess_x86.msi oder ess_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 (oder die Programmkonsole) zu installieren, gehen Sie wie folgt vor:

1. Speichern Sie die msi-Datei, die der Bit-Version (32-Bit oder 64-Bit) des installierten Microsoft Windows-Betriebssystems entspricht, in einem freigegebenen Ordner auf dem Domain-Controller.

2. Speichern Sie die Schlüsseldatei im selben öffentlichen Verzeichnis auf dem Domain-Controller.

3. Erstellen Sie im selben öffentlichen Verzeichnis auf dem Domain-Controller die Datei install_props.json mit dem nachfolgend angeführten Inhalt, mit dem Sie Ihre Annahme des Lizenzvertrags und der Datenschutzrichtlinie bestätigen.

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

4. Erstellen Sie auf dem Domain-Controller eine neue Richtlinie für die Gruppe, zu der die geschützten Geräte gehören.

5. Legen Sie mit dem **Gruppenrichtlinienobjekteditor** ein neues Installationspaket im Knoten **Computer-Konfiguration** an. Geben Sie den Pfad zur msi-Datei für Kaspersky Embedded Systems Security (oder die Programmkonsole) im UNC-Format (Universal Naming Convention) ein.

6. Aktivieren Sie das Kontrollkästchen **Immer mit erhöhten Rechten installieren** für den Dienst Windows Installer, und zwar sowohl im Knoten **Computer-Konfiguration**, als auch im Knoten **Benutzer-Konfiguration** der ausgewählten Gruppe.

7. Übernehmen Sie die Änderungen mithilfe des Befehls `gpupdate /force`.

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

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

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

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

Deinstallation von Kaspersky Embedded Systems Security über Gruppenrichtlinien von Active Directory

Dump- und Protokolldateien werden bei der Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht. Sie können Dump- und Protokolldateien manuell aus dem Ordner löschen, der angegeben wurde bei dem Erstellen von Dump-Dateien und Protokolldateien anpassen.

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

Sie können das Programm nur mit den Standarddeinstallationseinstellungen deinstallieren.

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

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

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

1. Wählen Sie im Domänencontroller die Organisationseinheit aus, von deren geschützten Geräten Sie Kaspersky Embedded Systems Security oder die Programmkonsole deinstallieren möchten.

2. Wählen Sie eine Richtlinie aus, die für die Installation von Kaspersky Embedded Systems Security erstellt wurde, öffnen Sie im **Editor für Gruppenrichtlinien** im Knoten **Software-Installation** (**Computerkonfiguration** > **Software-Einstellungen** > **Software-Installation**) das Kontextmenü des Installationspakets für Kaspersky Embedded Systems Security (die Programmkonsole) und wählen Sie den Befehl **Alle Aufgaben** > **Löschen**.

3. Wählen Sie die Deinstallationsmethode **Sofortige Deinstallation der Software von Benutzern und Computern**.

4. Übernehmen Sie die Änderungen mithilfe des Befehls `gpupdate /force`.

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

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

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

EICAR-Testvirus

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

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

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

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

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

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

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

Präfixe in EICAR-Dateien

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

Echtzeitschutz für Dateien und Funktionen der Untersuchung auf Befehl testen

Nach der Installation von Kaspersky Embedded Systems Security können Sie bestätigen, dass Kaspersky Embedded Systems Security Objekte erkennt, die bösartigen Code enthalten. Um das zu prüfen, können Sie den EICAR-Testvirus verwenden.

So prüfen Sie die Aufgabe "Echtzeitschutz für Dateien":

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

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

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

3. Öffnen Sie die Programmkonsole auf dem geschützten Gerät.

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

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

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

Geräts.

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

- Die Datei eicar.com wird vom geschützten Gerät gelöscht.
- In der Programmkonsole wird dem Protokoll der Aufgabenausführung der Status *Kritisch* zugewiesen. Das Protokoll enthält eine neue Zeile mit Informationen zu einer Bedrohung in der Datei eicar.com. (Um das Aufgabenprotokoll anzuzeigen, erweitern Sie in der Struktur der Programmkonsole den **Echtzeit-Computerschutz**, wählen Sie die Aufgabe **Echtzeitschutz für Dateien** und klicken Sie im Ergebnisfenster des Knotens auf den Link **Protokoll der Aufgabenausführung öffnen** öffnen).
  - Auf dem Gerät, von dem aus Sie die Datei kopiert haben, wird die folgende Meldung des Windows Messenger Dienstes mit folgendem Inhalt angezeigt: `Kaspersky Security für Windows Server hat den Zugriff auf <Pfad der Datei eicar.com auf dem Gerät>\eicar.com für den Computer <Netzwerkname des Geräts> um <Uhrzeit für Ereigniseintritt> gesperrt. Grund: Bedrohung erkannt. Virus: EICAR-Test-File. Name des Objektbenutzers: <Benutzername>. Computername: <Netzwerkname des Geräts, von dem die Datei kopiert wurde>`.

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

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

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

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

2. Öffnen Sie die Programmkonsole.
3. Führen Sie folgende Aktionen aus:
   a. Erweitern Sie in der Struktur der Programmkonsole den Knoten **Untersuchung auf Befehl**.
   b. Wählen Sie den untergeordneten Knoten **Untersuchung wichtiger Bereiche** aus.
   c. Öffnen Sie auf der Registerkarte **Untersuchungsbereich - Einstellungen** das Kontextmenü für den Knoten **Netzwerkumgebung** und wählen Sie **Netzwerkdatei hinzufügen**.
   d. Tragen Sie den Netzwerkpfad zur Datei eicar.com auf dem Remote-Gerät im UNC-Format (Universal Naming Convention) ein.
   e. Aktivieren Sie das Kontrollkästchen, um den hinzugefügten Netzwerkpfad in den Untersuchungsbereich aufzunehmen.
   f. Starten Sie die Aufgabe Untersuchung wichtiger Bereiche.

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

- Die Datei eicar.com wird von der Festplatte des Geräts gelöscht.

- In der Programmkonsole wird dem Protokoll der Aufgabenausführung der Status *Kritisch* zugewiesen. Das Protokoll der Aufgabe zur Untersuchung wichtiger Bereiche enthält eine neue Zeile mit Informationen zu einer Bedrohung in der Datei eicar.com. (Um das Aufgabenprotokoll anzuzeigen, erweitern Sie in der Struktur der Programmkonsole den untergeordneten Knoten **Untersuchung auf Befehl**, wählen Sie die Aufgabe zur Untersuchung wichtiger Bereiche und klicken Sie im Ergebnisfenster des Knotens auf den Link **Protokoll der Aufgabenausführung öffnen** öffnen).

Programmoberfläche

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

- Lokale Programmkonsole.
- Kaspersky Security Center-Verwaltungskonsole.
- Kaspersky Security Center Web-Konsole.
- Kaspersky Security Center Cloud-Konsole.

Kaspersky Security Center-Verwaltungskonsole

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

Das Programm kann über Kaspersky Security Center mithilfe des Verwaltungs-Plug-ins von Kaspersky Security für Windows Server verwaltet werden. Ausführliche Informationen über die Benutzeroberfläche von Kaspersky Security Center finden Sie in der *Hilfe von Kaspersky Security Center*.

Kaspersky Security Center Web-Konsole und Cloud-Konsole

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

Kaspersky Security Center Cloud-Konsole (im Folgenden auch als "Cloud-Konsole" bezeichnet) ist eine Cloud-basierte Lösung zum Schutz und zur Verwaltung eines Unternehmensnetzwerks. Ausführliche Informationen über die Cloud-Konsole von Kaspersky Security Center finden Sie in der *Hilfe zur Kaspersky Security Center Cloud-Konsole*.

Mit der Web-Konsole und der Cloud-Konsole können Sie Folgendes tun:

- Den Status des Sicherheitssystems Ihres Unternehmens überwachen.
- Kaspersky-Programme auf Geräten in Ihrem Netzwerk installieren.
- Installierte Programme verwalten.
- Berichte über den Status des Sicherheitssystems anzeigen.

Lizenzverwaltung für das Programm

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

Über den Endbenutzer-Lizenzvertrag

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

Lesen Sie den Endbenutzer-Lizenzvertrag sorgfältig, bevor Sie erste Schritte mit dem Programm ausführen.

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

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

Sie akzeptieren den Endbenutzer-Lizenzvertrag, indem Sie sich während der Installation des Programms mit seinen Bedingungen einverstanden erklären. Falls Sie den Bedingungen des Endbenutzer-Lizenzvertrags nicht zustimmen, müssen Sie die Programminstallation abbrechen und dürfen das Programm nicht verwenden.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, welches auf Basis eines Endbenutzer-Lizenzvertrags überlassen wird.

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

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

Der Umfang dieses Dienstes und der Zeitraum der Programmnutzung sind von dem Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Sie können das Programm auf zwei Arten aktivieren:

- Unter Verwendung einer Schlüsseldatei, die Ihnen die Nutzung des Programms unter einer kommerziellen Lizenz gewährt.
- Unter Verwendung eines Aktivierungscodes, um eine kommerzielle Lizenz zu kaufen.

Die *kommerzielle Lizenz* ist eine kostenpflichtige Lizenz, die beim Kauf des Programms zur Verfügung gestellt wird.

Sie können entweder die Kaspersky Embedded Systems Security Standardlizenz oder die erweiterte Lizenz der Kaspersky Embedded Systems Security Compliance Edition erwerben. Letztere enthält drei zusätzliche Komponenten für die System-Diagnose: Überwachung der Dateiintegrität, Überwachung des Registrierungszugriffs und Protokollanalyse.

Wenn eine kommerzielle Lizenz abläuft, kann das Programm zwar noch ausgeführt werden, aber folgende Funktionen stehen dann nicht mehr zur Verfügung:

- Integration mit Kaspersky Security Network
- Aktualisieren der Datenbanken von Kaspersky Embedded Systems Security

Wenn die Testlizenz abläuft, wird das Programm weiterhin ausgeführt und die Aufgaben zur **Untersuchung auf Befehl** und zum **Echtzeitschutz für Dateien** bleiben verfügbar. Jedoch sind alle weiteren Aufgaben, sowie das Aktualisieren der Datenbanken von Kaspersky Embedded Systems Security sind nicht mehr verfügbar. Dasselbe passiert, wenn Sie die Lizenz entfernen oder wenn Ihre Lizenz der Deny-Liste hinzugefügt wird.

Um alle Funktionen von Kaspersky Embedded Systems Security weiterhin nutzen zu können, müssen Sie die Lizenz verlängern.

Es wird empfohlen, die Lizenz vor ihrem Ablaufdatum zu verlängern, um die maximale Sicherheit Ihrer Geräte zu gewährleisten.

Stellen Sie sicher, dass das Ablaufdatum des Reserveschlüssels zeitlich hinter dem des aktiven Schlüssels angesiedelt ist.

Über das Lizenzzertifikat

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

Ein Lizenzzertifikat enthält die folgenden Informationen über die aktive Lizenz:

- Bestellnummer
- Informationen über den Benutzer, dem diese Lizenz gewährt wurde
- Informationen über das Programm, das mit dieser Lizenz aktiviert werden kann
- Maximale Anzahl von Lizenzeinheiten (z. B. Geräte, auf denen das Programm unter dieser Lizenz verwendet werden kann)
- Datum für den Beginn der Lizenzgültigkeit
- Gültigkeitsdauer der Lizenz bzw. Laufzeit der Lizenz
- Lizenztyp

Über den Schlüssel

Der *Schlüssel* ist eine Abfolge von Bits, mit deren Hilfe Sie das Programm aktivieren und anschließend gemäß den Bedingungen des Endbenutzer-Lizenzvertrags verwenden können. Der Schlüssel wird von den Kaspersky-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.

Kaspersky kann aufgrund von Verstößen gegen des Lizenzvertrags einen Schlüssel zur Deny-Liste hinzufügen. Wenn ein Schlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um das Programm zu nutzen.

Es gibt einen aktiven Schlüssel und einen Reserveschlüssel.

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

Reserveschlüssel – Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist. Der Reserveschlüssel wird automatisch aktiviert, wenn die Lizenz abläuft, die zum aktiven Schlüssel gehört. Ein Reserveschlüssel kann nur hinzugefügt werden, wenn ein aktiver Schlüssel vorhanden ist.

Über die Schlüsseldatei

Bei der *Schlüsseldatei* handelt es sich um eine Datei mit der Erweiterung .key, die Ihnen von Kaspersky zur Verfügung gestellt wird. Schlüsseldateien dienen dazu, das Programm durch Hinzufügen eines Lizenzschlüssels zu aktivieren.

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

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

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

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

- Wenden Sie sich an den Verkäufer der Lizenz.
- Rufen Sie die Schlüsseldatei mithilfe Ihres verfügbaren Aktivierungscodes über die Website von Kaspersky ab.

Über den Aktivierungscode

Bei einem *Aktivierungscode* handelt es sich um eine eindeutige Folge aus 20 Buchstaben und Ziffern. Sie müssen einen Aktivierungscode eingeben, um einen Schlüssel zur Aktivierung von Kaspersky Embedded Systems Security hinzuzufügen. Der Aktivierungscode wird an die E-Mail-Adresse geschickt, die Sie beim Kauf von Kaspersky Embedded Systems Security oder der Anforderung einer Testversion von Kaspersky Embedded Systems Security angegeben haben.

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

Bei Verlust des Aktivierungscodes nach der Installation des Programms kann dieser wiederherstellt werden. Ein Aktivierungscode kann beispielsweise für die Registrierung eines Kaspersky CompanyAccount erforderlich sein. Um Ihren Aktivierungscode wiederherzustellen, wenden Sie sich bitte an den Partner von Kaspersky Lab, von dem Sie die Lizenz erworben haben.

Über die Bereitstellung von Daten

Im Endbenutzer-Lizenzvertrag für Kaspersky Embedded Systems Security 3, insbesondere im Abschnitt "Bedingungen für die Datenverarbeitung", sind die Bedingungen, die Haftung und das Verfahren für die Übermittlung und Verarbeitung der in diesem Handbuch angegebenen Daten festgelegt. Bevor Sie den Endbenutzer-Lizenzvertrag akzeptieren, lesen Sie die Bedingungen sowie alle Dokumente, die mit dem Endbenutzer-Lizenzvertrag verknüpft sind, sorgfältig.

Die Daten, die Kaspersky von Ihnen erhält, wenn Sie die Anwendung verwenden, sind geschützt und werden gemäß der Datenschutzrichtlinie verarbeitet, die Sie unter www.kaspersky.com/Products-and-Services-Privacy-Policy abrufen können.

Die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie stehen während der Installation von Kaspersky Embedded Systems Security im Lieferumfang und nach der Installation über das Menü **Start** (**Alle Programme** > **Kaspersky Embedded Systems Security** > **Endbenutzer-Lizenzvertrag und Datenschutzrichtlinie**) zur Verfügung.

Bei der Deinstallation von Kaspersky Embedded Systems Security werden alle Daten gelöscht, die von Kaspersky Embedded Systems Security auf dem geschützten Gerät gespeichert wurden.

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

- Um den Mechanismus für den Erhalt von Updates zu unterstützen - Informationen über das installierte Programm und seine Aktivierung: Identifikator des zu installierenden Programms und dessen Vollversion, einschließlich Versionsnummer, Typ und Lizenz-ID, Installations-Identifikator, ID der Update-Aufgabe.

- Um die Möglichkeit zu nutzen, zu Wissensdatenbankartikeln zu navigieren, wenn Programmfehler auftreten (Redirector-Service) – Informationen über das Programm und den Verknüpfungstyp: Name, Gebietsschema und vollständige Versionsnummer des Programms, Typ des Umleitungslinks und Fehler-ID.

- Zur Verwaltung von Bestätigungen für die Datenverarbeitung - Informationen über den Status der Annahme von Endbenutzer-Lizenzverträgen und anderer Dokumente, welche die Bedingungen für die Datenübermittlung festlegen: ID und Version des Lizenzvertrags oder eines anderen Dokuments, als Teil dessen die Bedingungen für die Datenverarbeitung akzeptiert oder abgelehnt werden; ein Attribut, das die Handlung des Benutzers (Bestätigung oder Rückruf der Akzeptanz der Bedingungen) kennzeichnet; Datum und Uhrzeit der Statusänderungen der Annahme der Bedingungen für die Datenverarbeitung.

Lokale Datenverarbeitung

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

Die Tabelle unten enthält Informationen zur lokalen Verarbeitung und Speicherung von Daten in Berichten durch Kaspersky Embedded Systems Security.

Verarbeitung und Speicherung von Daten in Berichten

Funktionsbereich	Registrierung von Ereignissen
Nutzungsart	Kaspersky Embedded Systems Security speichert Daten lokal und sendet diese Daten an den Administrationsserver. Die Datenbank des Administrationsservers

	speichert Informationen zu Programmereignissen, die bei verwalteten geschützten Geräten auftreten.
Speicher	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<product version>\Reports • %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx • Datenbank des Administrationsservers
Sicherheitsmaßnahmen	Zugriffskontroll-Liste.
Aufbewahrungsdauer	Kaspersky Embedded Systems Security speichert die Daten, bis Kaspersky Embedded Systems Security deinstalliert wird. Bei der Deinstallation von Kaspersky Embedded Systems Security werden alle Daten gelöscht, die von Kaspersky Embedded Systems Security auf dem geschützten Gerät gespeichert wurden.
Ziel	Bereitstellen der Hauptfunktionen.

Kaspersky Embedded Systems Security löscht keine Ereignisse aus dem Windows-Ereignisprotokoll, auch nicht während der Deinstallation von Kaspersky Embedded Systems Security.

Für die Bereitstellung der Ereignisregistrierungsfunktion verarbeitet Kaspersky Embedded Systems Security lokal die folgenden Daten:

- Namen, Prüfsummen (MD5, SHA-256) und Attribute der verarbeiteten Dateien sowie die vollständigen Pfade auf den untersuchten Medien zu diesen Dateien.
- Aktionen an den von Kaspersky Embedded Systems Security untersuchten Dateien.
- Aktionen durch den Benutzer an den untersuchten Dateien auf dem geschützten Computer.
- Informationen zu Konten von Benutzern, die Aktionen am geschützten Netzwerk bzw. Gerät vornehmen.
- Werte des Geräteinstanzpfads für Geräte, die den Regeln für die Gerätekontrolle hinzugefügt wurden.
- Informationen zu Prozessen und Skripten, die auf dem System ausgeführt werden: Prüfsummen (MD5, SHA-256) und vollständige Pfade zu ausführbaren Dateien, Informationen zu digitalen Zertifikaten.
- Windows Firewall-Einstellungen.
- Windows-Ereignisprotokolleinträge.
- Namen der Konten von Benutzern, die Aktionen an untersuchten Dateien auf dem geschützten Computer ausführen.
- Exemplarklasse der gestarteten ausführbaren Dateien und die Typen, Namen, Prüfsummen und Attribute dieser Dateien.
- Informationen zur Netzwerkaktivität:
  - Die IP-Adressen der blockierten externen Geräte.
  - Verarbeitete IP-Adressen.

- Informationen zum Status des Windows USN-Protokolls.

Die folgende Tabelle enthält Informationen zu Dienstdaten die von Kaspersky Embedded Systems Security verarbeitet wurden. Die Dienstdaten umfassen: Programmparameter, Quarantäne- und Backup-Dateien, Informationen in den Dienstdatenbanken des Programms, Lizenzdaten.

Die Tabelle unten enthält Informationen zur lokalen Verarbeitung und Speicherung von benutzerdefinierten Parameterdaten durch Kaspersky Embedded Systems Security.

Verarbeitung und Speicherung von benutzerdefinierten Parameterdaten

Funktionsbereich	Alle Funktionen von Kaspersky Embedded Systems Security
Nutzungsart	Kaspersky Embedded Systems Security speichert Daten lokal und sendet diese Daten an den Administrationsserver. Die Daten sind in der Datenbank des Administrationsservers gespeichert. Die vom Programm lokal verarbeiteten Daten werden nicht automatisch an Kaspersky oder sonstige Dritthersteller-Systeme gesendet.
Speicher	• %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Embedded Systems Security\<product version>\ • Datenbank des Administrationsservers
Sicherheitsmaßnahmen	Zugriffskontroll-Liste.
Verarbeitungszeitraum	Kaspersky Embedded Systems Security speichert die Daten, bis Kaspersky Embedded Systems Security deinstalliert wird. Bei der Deinstallation von Kaspersky Embedded Systems Security werden alle Daten gelöscht, die von Kaspersky Embedded Systems Security auf dem geschützten Gerät gespeichert wurden. Kaspersky Embedded Systems Security löscht keine Daten zu Parametern, die in die Konfigurationsdatei exportiert wurden. Kaspersky Embedded Systems Security löscht keine Quarantäne- oder Backup-Objekte, wenn die Kontrollkästchen **Quarantäne-Objekte exportieren** und **Backup-Objekte exportieren** im Installationsassistenten aktiviert wurden.
Ziel	Bereitstellen der Hauptfunktionen.

Für bestimmte Zwecke verarbeitet Kaspersky Embedded Systems Security die folgenden Daten lokal:

- Quarantäne- oder Backup-Objekte.
- Informationen zu Benutzerkonten (Benutzername und Kennwort), anhand deren Kaspersky Embedded Systems Security Aufgaben ausführt.
- Kennwort für Kaspersky Embedded Systems Security.
- IP-Adressen und IDs von blockierten Anmeldesitzungen.
- Einstellungen für Windows Firewall und Windows Firewall-Regeln.
- Prüfsummen (MD5, SHA-256) und Pfade zu ausführbaren Dateien, die den Regeln für Aufgaben der Kontrolle des Programmstarts hinzugefügt wurden.
- Werte des Geräteinstanzpfads für Geräte, die den Regeln für die Gerätekontrolle hinzugefügt wurden.

- Informationen zu Dateien und Ordnern in den Aufgabenbereichen für Kaspersky Embedded Systems Security.
- IP-Adressen im oder außerhalb des Schutzbereichs.
- Informationen zu Ereignissen im Windows-Ereignisprotokoll.
- Informationen zu Erkenntnissen, die mit der iSwift- oder iChecker-Technologie entdeckt wurden.
- Prüfsummen (MD5, SHA-256), vollständige Pfade und Masken, die in Ausnahmeeinstellungen definiert wurden.
- Informationen zu Prozessen, die der vertrauenswürdigen Zone hinzugefügt wurden.
- Informationen zu hinzugefügten Lizenzschlüsseln.
- Informationen zu digitalen Zertifikaten.
- Nicht entpackte Dateien aus einem Archiv oder andere zusammengesetzte Objekte während der Untersuchung.

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

Mit Kaspersky Security für Windows Server können Sie die Sicherheitsstufe für lokal verarbeitete Daten konfigurieren (Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Security für Windows Server, Ereignisregistrierung. Protokolle für Kaspersky Security für Windows Server): 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 die Daten protokolliert werden, ändern.

Die vom Programm lokal verarbeiteten Daten werden nicht automatisch an Kaspersky oder sonstige Drittherstellersysteme gesendet.

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

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

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

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

Lokale Datenverarbeitung mithilfe von Hilfskomponenten des Programms

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

- Die Programmkonsole. Diese Komponente ist im Paket "Administrations-Tools" von Kaspersky Embedded Systems Security enthalten und wird von einem Snap-in für die Microsoft Management Console dargestellt.
- Das Verwaltungs-Plug-in Diese Komponente bietet eine vollständige Integration in Kaspersky Security Center.

Bei der Ausführung der in diesem Handbuch beschriebenen Hauptfunktionen des Programms wird von den Hilfskomponenten des Programms ein Satz von Daten auf dem geschützten Gerät verarbeitet und gespeichert, d. h. dort, wo die Daten installiert sind, auch wenn die Hilfskomponenten nachträglich zu Kaspersky Embedded Systems Security installiert werden.

Von den Programmkomponenten werden die folgenden Daten lokal verarbeitet und gespeichert:

- Programmkonsole: der Name des geschützten Geräts mit installiertem Kaspersky Embedded Systems Security (IP-Adresse oder Domain-Name), mit dem sich die Programmkonsole das letzte Mal ferngesteuert verbunden hat; im Microsoft Management Console-Snap-in konfigurierte Anzeigeparameter; Daten zum letzten Ordner, in dem der Benutzer über die Programmkonsole Objekte ausgewählt hat (mithilfe des Systemdialogfelds, das durch Klicken auf die Schaltfläche **Durchsuchen** geöffnet wurde). Die Protokolldateien der Programmkonsole können auch die folgenden Daten enthalten: den Namen des geschützten Geräts mit installiertem Programm Kaspersky Embedded Systems Security, zu dem die Remote-Verbindung hergestellt wurde, sowie den Namen des Benutzerkontos, unter dem die Remote-Verbindung hergestellt wurde.

- Von Kaspersky Embedded Systems Security verarbeitete Daten können vom Verwaltungs-Plug-in verarbeitet und temporär gespeichert werden. Dazu zählen z. B. konfigurierte Parameter der Programmaufgaben und -komponenten, Parameter der Kaspersky Security Center-Richtlinien sowie Daten, die über Netzwerklisten versendet werden.

Die Tabelle unten enthält Informationen zu von Kaspersky Embedded Systems Security lokal verarbeiteten und gespeicherten Daten in Dump- und Protokolldateien.

Kaspersky Embedded Systems Security verarbeitet und speichert lokal die folgenden Dump- und Protokolldateien:

- Informationen zu Aktionen auf dem geschützten Gerät durch Kaspersky Embedded Systems Security.

- Informationen zu Objekten, die von Kaspersky Embedded Systems Security verarbeitet wurden.

- Informationen zu Aktivitäten auf dem geschützten Gerät, die von Kaspersky Embedded Systems Security verarbeitet wurden.

- Informationen zu Fehlern, die während der Ausführung von Kaspersky Embedded Systems Security aufgetreten sind.

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

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

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

Daten in Protokoll- und Dump-Dateien

Kaspersky Embedded Systems Security kann gemäß den Einstellungen Debug-Informationen in Protokolldateien für den technischen Support schreiben, während Kaspersky Embedded Systems Security ausgeführt wird.

Dump-Dateien für Kaspersky Embedded Systems Security werden vom Betriebssystem bei Programmabstürzen erstellt und beim nächsten Absturz überschrieben.

Protokoll- und Dump-Dateien können persönliche Daten des Benutzers oder vertrauliche Daten Ihres Unternehmens enthalten.

Verwenden Sie Kaspersky Embedded Systems Security nicht auf Geräten, für die eine Datenübertragung durch die Richtlinien Ihres Unternehmens verboten ist.

Kaspersky Embedded Systems Security zeichnet standardmäßig keine Debug-Informationen auf.

Protokoll- und Dump-Dateien werden nicht automatisch weiter als bis auf den Host übertragen, auf dem sie generiert wurden. Der Inhalt von Protokolldateien kann mit Standardanzeigeprogrammen für Textdateien angezeigt werden. Protokoll- und Dump-Dateien werden unbegrenzt archiviert und bei Deinstallation von Kaspersky Embedded Systems Security nicht gelöscht.

Debug-Informationen können für den technischen Support von Nutzen sein.

Es werden keine speziellen Verfahren bereitgestellt, um den Zugriff auf Protokoll- und Dump-Dateien einzuschränken. Der Administrator kann das Programm so anpassen, dass Daten in einen geschützten Ordner geschrieben werden.

Der Pfad zum Protokoll- und Dump-Dateiordner wird nicht standardmäßig konfiguriert. Der Administrator muss den Pfad angeben, damit der Protokoll- und Dump-Ordner verwendet werden kann.

Daten in Protokoll- und Dump-Dateien können Folgendes enthalten:

- Von Kaspersky Embedded Systems Security auf dem Host durchgeführte Aktionen.
- Informationen zu Objekten, die von Kaspersky Endpoint Agent verarbeitet wurden.
- Fehler bei der Ausführung von Kaspersky Endpoint Agent.

Aktivieren des Programms mit einer Schlüsseldatei

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

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

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

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

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

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
2. Betätigen Sie im Ergebnisfenster des Knotens **Lizenzverwaltung** den Link **Schlüssel hinzufügen**.
3. Klicken Sie im folgenden Fenster auf **Durchsuchen**.
4. Wählen Sie eine Schlüsseldatei mit der Dateiendung .key aus.

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

5. Klicken Sie auf **OK**.

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

Aktivieren des Programms mit einem Aktivierungscode

Um das Programm mit einem Aktivierungscode zu aktivieren, muss das geschützte Gerät mit dem Internet verbunden sein.

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

Bei der Aktivierung des Programms mit dieser Methode sendet Kaspersky Embedded Systems Security Daten an den Aktivierungsserver, um den eingegebenen Code zu überprüfen:

- Ist die Überprüfung des Aktivierungscodes erfolgreich, wird das Programm aktiviert.
- Schlägt die Überprüfung des Aktivierungscodes fehl, wird eine entsprechende Benachrichtigung angezeigt. In diesem Fall müssen Sie sich an den Softwarehändler wenden, von dem Sie Ihre Lizenz für Kaspersky Embedded Systems Security erworben haben.
- Wenn die für den Aktivierungscode zulässige Anzahl Aktivierungen überschritten wird, wird eine entsprechende Benachrichtigung angezeigt. Die Programmaktivierungsprozedur wird unterbrochen und Sie werden aufgefordert, den Technischen Support von Kaspersky zu kontaktieren.

Sie können Kaspersky Embedded Systems Security mit einem Aktivierungscode über die Programmkonsole aktivieren oder durch Erstellen der Gruppenaufgabe namens "Programm aktivieren" über das Verwaltungs-Plug-in oder über das Web-Plug-in.

So aktivieren Sie Kaspersky Embedded Systems Security mit einem Aktivierungscode in der Programmkonsole:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
2. Klicken Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** auf den Link **Aktivierungscode hinzufügen**.
3. Geben Sie im folgenden Fenster im Feld **Aktivierungscode** den Aktivierungscode ein.
   - Wenn Sie den Aktivierungscode als Reserveschlüssel verwenden möchten, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.
   - Wenn Sie die Lizenzinformationen einsehen möchten, klicken Sie auf die Schaltfläche **Lizenzinformationen anzeigen**. Diese werden daraufhin im Gruppenfeld **Lizenzinformationen** angezeigt.
4. Klicken Sie auf **OK**.

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

Anzeigen von Informationen über die aktive Lizenz

Informationen zur Lizenzverwaltung anzeigen

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

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

Anzeigen von Informationen über die aktive Lizenz

Um Informationen über die aktive Lizenz anzuzeigen,

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

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

Allgemeine Lizenzinformationen im Knoten Lizenzverwaltung

Feld	Beschreibung
Aktivierungscode	Der Aktivierungscode. Dieses Feld wird ausgefüllt, wenn Sie das Programm mithilfe eines Aktivierungscodes aktivieren.
Aktivierungsstatus	Informationen über den Aktivierungsstatus des Programms. Die Spalte **Aktivierungsstatus** des Detailbereichs des Knotens **Lizenzverwaltung** kann die folgenden Statusvarianten haben: • **Übernommen** – wenn Sie das Programm mithilfe eines Aktivierungscodes oder einer Schlüsseldatei aktiviert haben. • **Aktivierung** – wenn Sie einen Aktivierungscode für die Aktivierung des Programms verwendet haben und der Aktivierungsprozess noch nicht abgeschlossen ist. Der Status ändert sich zu **Übernommen**, sobald die Aktivierung

	des Programms abgeschlossen ist und die Inhalte des Detailbereichs des Knotens aktualisiert wurden. • **Fehler beim Aktivieren** – wenn das Programm nicht aktiviert werden konnte. Die Ursache für das Fehlschlagen der Aktivierung finden Sie im Protokoll der Aufgabenausführung.
Schlüssel	Der Schlüssel, der zur Aktivierung des Programms verwendet wurde.
Lizenztyp	Lizenztyp: kommerziell oder Probe
Gültig bis	Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Status des Aktivierungscodes oder Schlüssels	Status des Aktivierungscodes oder des Schlüssels: *Aktiv* oder *Reserveschlüssel*.

Um detaillierte Informationen über die aktuelle Lizenz anzuzeigen,

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

Im Fenster **Schlüsseleigenschaften** 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 oder dem Partner angezeigt, bei dem Sie Kaspersky Embedded Systems Security gekauft haben (siehe Tabelle unten).

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

Feld	Beschreibung
Registerkarte Allgemein	
Schlüssel	Der Schlüssel, der zur Aktivierung des Programms verwendet wurde.
Schlüssel hinzugefügt am	Datum, an dem der Schlüssel zum Programm hinzugefügt wurde.
Lizenztyp	Lizenztyp: kommerziell oder Probe
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 *Unbegrenzt* angezeigt. Wenn Kaspersky Embedded Systems Security das Ablaufdatum der Lizenz nicht ermitteln kann, ist der Wert *Unbekannt*.
Programm	Name des Programms, das mit der Schlüsseldatei oder dem Aktivierungscode aktiviert wurde.
Nutzungsbeschränkung für Schlüssel	Beschränkungen für die Nutzung des Schlüssels (falls vorhanden).
Verfügbarkeit des Technischen Supports	Informationen darüber, ob Kaspersky oder einer seiner Partner dem Kunden technischen Support gemäß den Lizenzbedingungen leistet.
Registerkarte Erweitert	
Lizenzinformationen	Aktueller Lizenzschlüssel.
Support-Informationen	Kontaktinformationen von Kaspersky oder seinem Partner, der für den technischen Support verantwortlich ist. Dieses Feld kann leer sein, wenn kein technischer Support geleistet wird.

Informationen zum Benutzer	Informationen zum Eigentümer der Lizenz: ein Kundenname und der Name des Unternehmens, für das die Lizenz erworben wurde.

Funktionsbeschränkungen bei Ablauf der Lizenz

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

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

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

Verlängern der Lizenz

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

Sie können die Lizenz schon vor dem Ablaufdatum verlängern, indem Sie einen Reserveschlüssel hinzufügen. So vermeiden Sie, dass das Gerät nach Ablauf der Laufzeit der aktuellen Lizenz bis zur Aktivierung des Programms mit der neuen Lizenz ungeschützt ist.

So verlängern Sie eine Lizenz:

1. Besorgen Sie sich einen neuen Aktivierungscode oder eine Schlüsseldatei für das Programm.
2. 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 einer Schlüsseldatei verlängern möchten:
     a. Klicken Sie auf den Link **Schlüssel hinzufügen**.
     b. Klicken Sie im folgenden Fenster auf **Durchsuchen**.
     c. Wählen Sie eine neue Schlüsseldatei mit der Dateiendung .key aus.
     d. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.
   - Wenn Sie die Lizenz mithilfe eines Aktivierungscodes verlängern möchten:

a. Klicken Sie auf den Link **Aktivierungscode hinzufügen**.

b. Geben Sie den erworbenen Aktivierungscode im erscheinenden Fenster ein.

c. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.

Für die Übernahme des Aktivierungscodes ist eine Internetverbindung erforderlich.

4. Klicken Sie auf **OK**.

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

Löschen des Schlüssels

Sie können den hinzugefügten Schlüssel entfernen.

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

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

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

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Lizenzverwaltung**.
2. Wählen Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** in der Tabelle mit Informationen über die hinzugefügten Schlüssel den Schlüssel aus, den Sie entfernen möchten.
3. Wählen Sie im Kontextmenü der Zeile mit den Informationen über den ausgewählten Schlüssel den Punkt **Löschen** aus.
4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um das Löschen des Schlüssels zu bestätigen.

Der ausgewählte Schlüssel wird gelöscht.

Arbeiten mit dem Verwaltungs-Plug-in

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

Verwaltung von Kaspersky Embedded Systems Security über Kaspersky Security Center

Über das Verwaltungs-Plug-in für Kaspersky Security für Windows Server können Sie mehrere geschützte Geräte zentral verwalten, auf denen Kaspersky Security für Windows Server installiert und die in einer Administrationsgruppe enthalten ist. Kaspersky Security Center kann jedes geschützte Gerät in der Administrationsgruppe auch separat konfigurieren.

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

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

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

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

  Mithilfe von Richtlinien können Sie allgemeine Programmeinstellungen, Einstellungen für Aufgaben zum Echtzeit-Computerschutz, Einstellungen für Aufgaben zur Überwachung der Desktop-Aktivitäten und Einstellungen zum Start von lokalen Systemaufgaben nach Zeitplan anpassen.

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

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

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

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

Kaspersky Security Center erlaubt die Anpassung der Programmeinstellungen und erweiterten Optionen, sowie auch die Arbeit mit Protokollen und Benachrichtigungen. Sie können diese Einstellungen für Gruppen von geschützten Geräten und für ein einzelnes geschütztes Gerät anpassen.

Programmeinstellungen verwalten

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

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Öffnen der allgemeinen Einstellungen über die Richtlinie

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

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Programmeinstellungen** aus.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt der Einstellung, die Sie konfigurieren möchten.

Öffnen der allgemeinen Einstellungen im Eigenschaftenfenster des Programms

Um das Eigenschaftenfenster von Kaspersky Embedded Systems Security für ein einzelnes geschütztes Gerät zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Name des geschützten Geräts>** zu öffnen:

   - Doppelklicken Sie auf den Namen des geschützten Geräts.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Geräts aus.

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.

5. Wählen Sie im Abschnitt **Programme** die Option **Kaspersky Embedded Systems Security 3.1** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Einstellungen für Kaspersky Embedded Systems Security 3.1** wird geöffnet.

7. Wählen Sie den Abschnitt **Programmeinstellungen** aus.

Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center

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

Skalierbarkeit, Schnittstelle und Untersuchungseinstellungen im Kaspersky Security Center anpassen

Um Skalierbarkeit, Schnittstelle und Untersuchungseinstellungen anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:

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

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

4. Klicken Sie im Abschnitt **Programmeinstellungen** im Unterabschnitt **Skalierbarkeit, Oberfläche und Untersuchungseinstellungen** auf **Einstellungen**.

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

   - Passen Sie im Abschnitt **Skalierbarkeitseinstellungen** die Einstellungen an, durch die die Anzahl der von Kaspersky Embedded Systems Security verwendeten Arbeitsprozesse festgelegt wird:

     - Skalierbarkeitseinstellungen automatisch ermitteln
     - Anzahl der Arbeitsprozesse manuell angeben
       - Maximale Anzahl aktiver Prozesse
       - Anzahl der Prozesse für den Echtzeitschutz
       - Anzahl der Prozesse für im Hintergrund ausgeführte Untersuchungen auf Befehl

   - Passen Sie im Abschnitt **Interaktion mit dem Benutzer** die Anzeige des Programmsymbols im Infobereich der Taskleiste an: Deaktivieren oder aktivieren Sie dazu das Kontrollkästchen **Symbol im Infobereich der Taskleiste anzeigen**.

6. Passen Sie auf der Registerkarte **Untersuchungseinstellungen** folgende Einstellungen an:

   - Dateiattribute nach der Untersuchung wiederherstellen
   - CPU-Auslastung für die Untersuchung auf Bedrohungen begrenzen
     - Obergrenze (Prozent)
   - Ordner für während der Untersuchung erstellte temporäre Dateien

7. Wählen Sie auf der Registerkarte **Hierarchischer Speicher** die Option für den Zugriff auf den hierarchischen Speicher.

8. Klicken Sie auf **OK**.

Die vorgenommenen Programmeinstellungen werden gespeichert.

Sicherheitseinstellungen in Kaspersky Security Center anpassen

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

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

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

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

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

5. Konfigurieren Sie im Fenster **Sicherheitseinstellungen** die folgenden Einstellungen:

   - In dem Bereich **Einstellungen für den Kennwortschutz** aktivieren oder deaktivieren Sie die Einstellung **Programmprozesse vor externen Bedrohungen schützen**.
   - Legen Sie im Abschnitt **Einstellungen für den Kennwortschutz** das Kennwort für den Schutz des Zugriffs auf die Funktionen von Kaspersky Embedded Systems Security fest.
   - Passen Sie im Abschnitt **Selbstschutz** die Wiederherstellungseinstellungen für die Aufgaben von Kaspersky Embedded Systems Security bei Störungen oder einer fehlerhaften Beendigung des Programms an.
     - **Wiederherstellen von Aufgaben ausführen**
     - **Einstellungen für Zuverlässigkeit**
   - Legen Sie im Abschnitt **Maximale Anzahl zum Wiederherstellen der Aufgaben zur Untersuchung auf Befehl** die von Kaspersky Embedded Systems Security beim Wechsel auf eine USV-Quelle erzeugte Belastungsbeschränkung auf den geschützten Geräten fest:
     - **Aufgaben zur Untersuchung nach Zeitplan nicht starten**
     - **Laufende Untersuchungsaufgaben anhalten**
   - Legen Sie im Abschnitt **Einstellungen für den Kennwortschutz** das Kennwort für den Schutz des Zugriffs auf die Funktionen von Kaspersky Embedded Systems Security fest.

6. Klicken Sie auf **OK**.

Die konfigurierten Sicherheitseinstellungen werden gespeichert.

Verbindungseinstellungen über Kaspersky Security Center anpassen

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

Zum Einrichten der Verbindungseinstellungen gehen Sie wie folgt vor:

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

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

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

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

- Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

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

   Das Fenster **Verbindungseinstellungen** wird geöffnet.

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

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

     - Keinen Proxyserver verwenden.
     - Angegebenen Proxyserver verwenden.
     - IP-Adresse oder symbolischer Name des Proxyservers und Portnummer.
     - Für lokale Adressen keinen Proxyserver verwenden.

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

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

       - **Keine Authentifizierung 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 Benutzernamens und Kennworts über das von Microsoft entwickelten NTLM-Protokoll zur Netzwerkauthentifizierung.
       - **Benutzername und Kennwort verwenden** – Authentifizierung mithilfe des Benutzernamens und Kennworts.

     - Geben Sie bei Bedarf den Benutzernamen und das Kennwort an.

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

6. Klicken Sie auf **OK**.

Die vorgenommenen Verbindungseinstellungen werden gespeichert.

Zeitplan für den Start von lokalen Systemaufgaben anpassen

Mithilfe von Richtlinien können Sie den Start von lokalen Systemaufgaben zur Untersuchung auf Befehl und zum Update nach einem lokal auf jedem geschützten Gerät 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 geschützten Gerät gemäß Zeitplan ausgeführt. Sie können lokale Systemaufgaben manuell starten.

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

Standardmäßig ist das Starten einer lokalen Systemaufgabe 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 Gruppenupdates oder ausgeführte Untersuchungen auf Befehl verwenden, erlauben Sie die Ausführung lokaler Systemaufgaben in der Richtlinie. Kaspersky Embedded Systems Security führt alle Programmdatenbank- und Modulupdates aus und startet alle Untersuchungen des lokalen Systems auf Befehl anhand des standardmäßig festgelegten Zeitplans.

Mithilfe von Richtlinien können Sie den Start folgender lokaler Systemaufgaben nach Zeitplan erlauben oder verbieten:

- Aufgaben zur Untersuchung auf Befehl: Untersuchung wichtiger Bereiche, Untersuchung von Quarantäne-Objekten, Untersuchung beim Hochfahren des Betriebssystems, Integritätsprüfung für Programme, Überwachung der Baseline-Integrität.

- Aufgaben zum Update: Update der Programm-Datenbanken, Update der Programm-Module, Update-Verteilung.

Wenn Sie ein geschütztes Gerät aus der Administrationsgruppe ausschließen, wird der Zeitplan der lokalen Systemaufgaben automatisch aktiviert.

So erlauben oder verbieten Sie den Start der lokalen Systemaufgaben von Kaspersky Embedded Systems Security nach Zeitplan in einer Richtlinie:

1. 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. Auf der Registerkarte **Richtlinie** im Kontextmenü der Richtlinie, für die Sie den Start von lokalen Systemaufgaben für Kaspersky Embedded Systems Security auf der Gruppe der geschützten Geräte planen möchten, wählen Sie **Eigenschaften**.

3. Öffnen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Programmeinstellungen**. Klicken Sie im Abschnitt **Start von lokalen Systemaufgaben** auf die Schaltfläche **Einstellungen** und führen eine der folgenden Aktionen aus:

   - Aktivieren Sie die Kontrollkästchen **Aufgaben zur Untersuchung auf Befehl** und **Aufgaben zum Update und zur Update-Verteilung**, um den Start der angeführten Aufgaben nach Zeitplan zu erlauben.

   - Deaktivieren Sie die Kontrollkästchen **Aufgaben zur Untersuchung auf Befehl** und **Aufgaben zum Update und zur Update-Verteilung**, um den Start der angeführten Aufgaben nach Zeitplan zu verbieten.

Das Aktivieren oder Deaktivieren der Kontrollkästchen beeinflusst nicht die Starteinstellungen der lokalen benutzerdefinierten Aufgaben des angegebenen Typs.

4. Vergewissern Sie sich, dass die Richtlinie, die Sie anpassen, aktiv ist und für die ausgewählte Gruppe von geschützten Geräten übernommen wurde.

5. Klicken Sie auf **OK**.

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

Quarantäne- und Backup-Einstellungen in Kaspersky Security Center anpassen

Um die Backup-Einstellungen in Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:

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

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

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **Zusätzlich** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Speicher**.

5. Passen Sie im Fenster **Speichereinstellungen** 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 Geräts 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.

   - So legen Sie den Grenzwert für freien Speicher für den Backup fest:

     - Definieren Sie den Wert der Einstellung **Maximale Größe des Backups (MB)**.

     - Aktivieren Sie das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz (MB)**.

     - Angabe des Mindestwerts in Megabytes für den freien Speicher im Backup-Ordner.

- Führen Sie einen der folgenden Schritte aus, um einen Ordner für wiederhergestellte Objekte anzugeben:
    - Wählen Sie im Abschnitt **Einstellungen für die Wiederherstellung von Objekten** den entsprechenden Ordner auf einem lokalen Laufwerk des geschützten Geräts aus.
    - Geben Sie den Namen des Ordners und den vollständigen Pfad dazu in das Feld **Ordner für die Wiederherstellung von Objekten** ein.

6. Passen Sie im Fenster **Speichereinstellungen** auf der Registerkarte **Quarantäne** die folgenden Quarantäne-Einstellungen an:
    - Wenn Sie den Quarantäneordner ändern möchten, geben Sie im Eingabefeld **Quarantäneordner** den vollständigen Ordnerpfad auf einem lokalen Laufwerk des geschützten Geräts an.
    - Wenn Sie die maximale Größe der **Quarantäne** festlegen möchten, aktivieren Sie das Kontrollkästchen Maximale Größe der Quarantäne (MB) und tragen Sie im Eingabefeld den Wert dieses Parameters in MB ein.
    - Wenn Sie die minimale Größe für den freien Speicherplatz in der Quarantäne festlegen möchten, aktivieren Sie die Kontrollkästchen **Maximale Größe der Quarantäne (MB)** und **Grenzwert für verfügbaren Speicherplatz (MB)** und tragen Sie im Eingabefeld den Wert dieses Parameters in MB ein.
    - Wenn Sie den Ordner ändern möchten, in dem Objekte aus der Quarantäne wiederhergestellt werden, geben Sie im Feld **Ordner für die Wiederherstellung von Objekten** den vollständigen Pfad zum Ordner auf einem lokalen Laufwerk des geschützten Geräts an.
7. Klicken Sie auf **OK**.

Die vorgenommenen Quarantäne- und Backup-Einstellungen werden gespeichert.

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt bietet Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Embedded Systems Security auf mehreren geschützten Geräten.

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

Eine Richtlinie übernimmt die Einstellungen, Funktionen und angegebenen Aufgaben von Kaspersky Embedded Systems Security auf allen geschützten Geräten einer Administrationsgruppe.

Sie können mehrere Richtlinien für eine Administrationsgruppe erstellen und sie temporär übernehmen. Die in der Gruppe aktuell gültige Richtlinie hat in der Verwaltungskonsole den Status *aktiv*.

Informationen über den Geltungsbereich einer Richtlinie werden im Systemaudit-Protokoll von Kaspersky Embedded Systems Security protokolliert. Diese Informationen stehen in der Programmkonsole unter dem Knoten **Systemaudit-Protokoll** zur Verfügung.

In Kaspersky Security Center existiert eine einzige Methode zur Übernahme von Richtlinien auf geschützten Geräten: *Änderung von Einstellungen verbieten*. Nach der Übernahme der Richtlinie übernimmt Kaspersky Embedded Systems Security die Werte von Einstellungen auf den geschützten Geräten, neben denen Sie in den Richtlinieneigenschaften das Zeichen gesetzt haben. In diesem Fall verwendet Kaspersky Embedded Systems Security nicht die Werte der Einstellungen, die vor Anwendung der Richtlinie wirksam waren. Einstellungswerte der aktiven Richtlinie, für die in den Richtlinieneigenschaften das Zeichen gesetzt ist, werden von Kaspersky Embedded Systems Security nicht übernommen.

Ist eine Richtlinie aktiv, so werden die Werte der Einstellungen, die in der Richtlinie mit dem Symbol markiert sind, in der Programmkonsole angezeigt, können jedoch nicht bearbeitet werden. Die Werte der restlichen Einstellungen (die in der Richtlinie mit dem Symbol markiert sind) können in der Programmkonsole bearbeitet werden.

Die in der aktiven Richtlinie festgelegten und mit dem Symbol markierten Einstellungen blockieren auch die Bearbeitung der Einstellungen in Kaspersky Security Center für ein einzelnes geschütztes Gerät im Fenster **Eigenschaften: <Name des geschützten Geräts>**.

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

Wenn die Richtlinie die Einstellungen für eine Aufgabe zum Echtzeit-Computerschutz definiert und diese Aufgabe derzeit ausgeführt wird, 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. Die Einstellungen für Aufgaben zum Echtzeit-Computerschutz können mit den Dialogfeldern des Assistenten konfiguriert werden.

2. Anpassung der Richtlinieneinstellungen. Im Fenster **Eigenschaften: <Name der Richtlinie>** der erstellten Richtlinie können Sie Folgendes anpassen: Einstellungen für Aufgaben zum Echtzeit-Computerschutz, allgemeine Einstellungen für Kaspersky Embedded Systems Security, Einstellungen für Quarantäne und Backup-Einstellungen, Genauigkeitsstufe für Protokolle der Aufgabenausführung sowie Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Embedded Systems Security.

So erstellen Sie eine Richtlinie für eine Gruppe von geschützten Geräten, auf denen Kaspersky Embedded Systems Security installiert ist:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie anschließend die Administrationsgruppe aus, für deren geschützte Geräte Sie eine Richtlinie anlegen möchten.

2. Öffnen Sie im Detailbereich der ausgewählten Administrationsgruppe die Registerkarte **Richtlinien** und klicken Sie auf den Link **Richtlinie erstellen**, um den Richtlinien-Assistenten zu öffnen und eine Richtlinie zu erstellen.

   Das Fenster **Assistent für neue Richtlinie** wird geöffnet.

3. Wählen Sie im Fenster **Wählen Sie die Gruppe aus, für die Sie eine Richtlinie erstellen möchten** Kaspersky Embedded Systems Security aus und klicken Sie auf **Weiter**.

4. Geben Sie einen Gruppenrichtliniennamen in das Feld **Name** ein.

   Die Namen von Richtlinien dürfen keines der folgenden Symbole enthalten: `" * < : > ? \ | .`

5. Gehen Sie wie folgt vor, um eine Richtlinienkonfiguration einer früheren Programmversion zu verwenden:

   a. Aktivieren Sie das Kontrollkästchen **Einstellungen der Richtlinie für frühere Programmversionen verwenden**.

b. Klicken Sie auf die Schaltfläche **Auswählen**.

c. Wählen Sie die Richtlinie aus, die Sie übernehmen möchten.

d. Klicken Sie auf **Weiter**.

6. Wählen Sie im Fenster **Vorgangsart auswählen** eine der folgenden Optionen aus:

   - **Erstellen**, um eine neue Richtlinie mit den Standardeinstellungen zu erstellen.
   - **Richtlinie importieren, die mit einer vorherigen Version von Kaspersky Embedded Systems Security erstellt wurde** erstellt wurde, um die importierte Richtlinie als Vorlage zu verwenden.
   - Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie eine Konfigurationsdatei mit einer vorhandenen Richtlinie aus.

7. Passen Sie im Fenster **Echtzeit-Computerschutz** bei Bedarf die Einstellungen der Aufgaben Echtzeitschutz für Dateien, Verwendung von KSN, Exploit-Prävention und Skript-Untersuchung Ihren Bedürfnissen entsprechend an. Erlauben oder verbieten Sie die Übernahme der konfigurierten Aufgaben der Richtlinie in den Netzwerken der geschützten Geräte:

   - Klicken Sie auf , um die Konfiguration der Einstellungen einer Aufgabe auf den geschützten Geräten 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 geschützten Geräten des Netzwerks zu verbieten und die Übernahme der in der Richtlinie konfigurierten Aufgabeneinstellungen zu erlauben.

   In neu erstellten Richtlinien gelten für die Parameter der Aufgaben zum Echtzeit-Computerschutz die Standardeinstellungen.

   - Wenn Sie die standardmäßig festgelegten Einstellungen der Aufgabe "Echtzeitschutz für Dateien" ändern möchten, klicken Sie im Unterabschnitt **Einstellungen** auf **Echtzeitschutz für Dateien**. Passen Sie im erscheinenden Fenster die Aufgabeneinstellungen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.
   - Wenn Sie die Standardeinstellungen der Aufgabe Verwendung von KSN ändern möchten, klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Verwendung von KSN**. Passen Sie im erscheinenden Fenster die Aufgabeneinstellungen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.

     Um die Aufgabe zur Verwendung von KSN zu starten, müssen Sie die KSN-Erklärung im Fenster **KSN-Datenverarbeitung** akzeptieren.

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

8. Wählen Sie im Fenster **Gruppenrichtlinie für das 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, dann wird diese deaktiviert und die eine neue Richtlinie übernommen.
   - **Inaktive Richtlinie**, wenn Sie nicht möchten, dass die Richtlinie sofort angewendet wird. Sie können diese Richtlinie später aktivieren.

- Aktivieren Sie das Kontrollkästchen **Richtlinieneigenschaften sofort nach ihrer Erstellung öffnen**, um den **Assistenten für neue Richtlinien** automatisch zu schließen und die neu erstellte Richtlinie nach Klicken auf die Schaltfläche **Weiter** zu konfigurieren.

9. Klicken Sie auf **Fertig**.

Die erstellte Richtlinie wird in der Richtlinienliste auf der Registerkarte **Richtlinien** der ausgewählten Administrationsgruppe angezeigt. Im Fenster **Eigenschaften: <Name der Richtlinie>** können Sie andere Einstellungen, Aufgaben und Funktionen von Kaspersky Embedded Systems Security anpassen.

Abschnitte mit Richtlinieneinstellungen für Kaspersky Embedded Systems Security

Allgemein

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

- Richtlinienstatus festlegen.
- Vererbungseinstellungen von übergeordneten und untergeordneten Richtlinien konfigurieren.

Ereignisbenachrichtigung

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

- *Kritische Ereignisse*
- *Funktionsfehler*
- *Warnung*
- *Informatives Ereignis*
  Über die Schaltfläche **Eigenschaften** können Sie die folgenden Einstellungen für die ausgewählten Ereignisse konfigurieren:
- Geben Sie den Speicherort und die Speicherdauer für Informationen über protokollierte Ereignisse an.
- Geben Sie für protokollierte Ereignisse die Methode für die Benachrichtigung an.

Programmeinstellungen

Einstellungen des Abschnitts "Programmeinstellungen"

Abschnitt	Einstellungen
Skalierbarkeit, Oberfläche und Untersuchungseinstellungen	Im Unterabschnitt **Skalierbarkeit, Oberfläche und Untersuchungseinstellungen** 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 und Zuverlässigkeit	Im Unterabschnitt **Sicherheit und Zuverlässigkeit** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Einstellungen der Aufgabenausführung anpassen. • Aktionen des Programms beim Wechsel des geschützten Geräts in den USV-Akkubetrieb angeben. • Kennwortschutz der Programmfunktionen aktivieren und deaktivieren.
Verbindungen	Im Unterabschnitt **Verbindungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Proxyserver-Einstellungen für die Verbindung mit den Update-Servern, den Aktivierungsservern und KSN konfigurieren: • Festlegung der Proxyserver-Einstellungen. • Geben Sie die Einstellungen für die Authentifizierung auf dem Proxyserver an.
Start von lokalen Systemaufgaben	Im Unterabschnitt **Start von lokalen Systemaufgaben** können Sie über die Schaltfläche **Einstellungen** den Start der folgenden lokalen Systemaufgaben nach einem auf den geschützten Geräten festgelegten Zeitplan erlauben oder verbieten: • Aufgabe zur Untersuchung auf Befehl • Update-Aufgaben und Aufgabe zur Update-Verteilung

Zusätzlich

Einstellungen des Abschnitts "Zusätzlich"

Abschnitt	Einstellungen
Vertrauenswürdige Zone	Im Unterabschnitt **Vertrauenswürdige Zone** können Sie über die Schaltfläche **Einstellungen** die folgenden Parameter für die Verwendung der vertrauenswürdigen Zone konfigurieren: • Erstellung einer Liste der Ausnahmen von der vertrauenswürdigen Zone. • Aktivieren oder deaktivieren der Untersuchung von Backup-Operationen. • Erstellen Sie eine Liste der vertrauenswürdigen Prozesse.
Untersuchung von Wechseldatenträgern	Im Unterabschnitt **Untersuchung von Wechseldatenträgern** können Sie über die Schaltfläche **Einstellungen** die Untersuchungseinstellungen für Wechseldatenträger anpassen.
Benutzerrechte für die Programmverwaltung	Im Unterabschnitt **Benutzerrechte für die Programmverwaltung** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Embedded Systems Security anpassen.
Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service	Im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Security Service anpassen.

Speicher	Im Unterabschnitt **Speicher** können Sie über die Schaltfläche **Einstellungen** folgende Einstellungen für Quarantäne, Backup und blockierte Hosts anpassen: • Angabe des Ordnerpfads, in dem Sie die Quarantäne- oder Backup-Objekte ablegen möchten. • Anpassung der maximalen Größe des Backups und der Quarantäne sowie Festlegung des Grenzwerts für verfügbaren Speicherplatz • Angabe des Ordnerpfads, in dem Sie die wiederhergestellten Quarantäne- oder Backup-Objekte ablegen möchten. • Passen Sie an, wie lange Hosts blockiert werden.

Echtzeit-Computerschutz

Einstellungen des Abschnitts "Echtzeit-Computerschutz"

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

Überwachung der Desktop-Aktivitäten

Einstellungen des Abschnitts "Überwachung der Desktop-Aktivitäten"

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

Netzwerküberwachung

Einstellungen des Abschnitts "Netzwerküberwachung"

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

System-Diagnose

Einstellungen des Abschnitts "System-Diagnose"

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

Protokolle und Benachrichtigungen

Abschnitt	Einstellungen
Protokolle der Aufgabenausführung	Im Unterabschnitt **Protokolle der Aufgabenausführung** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Prioritätsstufe protokollierter Ereignisse für die ausgewählten Programmkomponenten angeben. • Speicherdauer für Protokolle der Aufgabenausführung festlegen. • Konfiguration der SIEM-Integration in Kaspersky Security Center.
Ereignisbenachrichtigungen	Im Unterabschnitt **Ereignisbenachrichtigungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Legen Sie Einstellungen für die Benutzerbenachrichtigung für die Ereignisse *Objekt gefunden*, *Nicht vertrauenswürdiges externes Gerät erkannt und eingeschränkt* und *Host wurde der Liste der nicht vertrauenswürdigen Hosts hinzugefügt* fest. • Benachrichtigung des Administrators über ein beliebiges ausgewähltes Ereignis aus der Liste der Ereignisse im Abschnitt **Benachrichtigungen anpassen**.
Interaktion mit Administrationsserver	Im Abschnitt **Interaktion mit Administrationsserver** können Sie über die Schaltfläche **Einstellungen** die Typen der Objekte auswählen, über die Kaspersky Embedded Systems Security Informationen an den Administrationsserver übergeben soll.

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.

Anpassen einer Richtlinie

In dem Fenster **Eigenschaften: <Richtlinienname>** einer vorhandenen Richtlinie können Sie Folgendes konfigurieren:

- Allgemeine Einstellungen von Kaspersky Embedded Systems Security.
- Einstellungen für Quarantäne und Backup.
- Einstellungen für vertrauenswürdige Zone, Echtzeit-Computerschutz und Überwachung der Desktop-Aktivitäten.
- Genauigkeitsstufe für Protokolle der Aufgabenausführung.
- Benachrichtigungen der Benutzer und des Administrators über Ereignisse in Kaspersky Embedded Systems Security.
- Zugriffsrechte für die Programmverwaltung und Kaspersky Security Service.

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

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

2. Erweitern Sie die Administrationsgruppe, für die Sie die zugehörigen Richtlinieneinstellungen anpassen möchten und öffnen Sie die Registerkarte **Richtlinien** im Detailbereich.

3. Wählen Sie die Richtlinie, die Sie anpassen möchten und öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>** auf eine der folgenden Arten:

   - Wählen Sie im Kontextmenü der Richtlinie die Option **Eigenschaften** aus.
   - Klicken Sie im rechten Ergebnisbereich der ausgewählten Richtlinie auf den Link **Richtlinie anpassen**.
   - Doppelklicken Sie auf die ausgewählte Richtlinie.

4. Aktivieren oder deaktivieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Richtlinienstatus** die Richtlinie. Wählen Sie dazu eine der folgenden Varianten:

   - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie auf allen geschützten Geräten übernommen wird, die zur ausgewählten Administrationsgruppe gehören.
   - **Inaktive Richtlinie**, wenn Sie die Richtlinie später auf allen geschützten Geräten der ausgewählten Administrationsgruppe aktivieren möchten.

   Die Einstellung **Out-Of-Office Richtlinie** ist bei der Verwendung von Kaspersky Embedded Systems Security nicht verfügbar.

5. In den Abschnitten **Konfiguration von Ereignissen**, **Programmeinstellungen**, **Zusätzlich**, **Protokolle und Benachrichtigungen** und **Revisionsverlauf** können Sie die allgemeinen Einstellungen der Programmausführung ändern (siehe Tabelle unten).

6. Konfigurieren Sie in den Abschnitten **Echtzeit-Computerschutz**, **Überwachung der Desktop-Aktivitäten**, **Netzwerküberwachung** und **System-Diagnose** die Einstellungen für die Ausführung der Aufgaben des Programms sowie die Einstellungen für deren Start (siehe Tabelle unten).

   Sie können die Ausführung einer beliebigen Aufgabe auf allen geschützten Geräten, die zu einer Administrationsgruppe gehören, mithilfe einer Richtlinie von Kaspersky Security Center aktivieren und deaktivieren.

   Sie können die Übernahme der in der Richtlinie festgelegten Einstellungen auf allen geschützten Geräten des Netzwerks für jede einzelne Programmkomponente festlegen.

7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden in der Richtlinie übernommen.

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Embedded Systems Security, ihre Erstellung, die Konfiguration ihrer Ausführung sowie über den Start/die Beendigung von Aufgaben.

Über die Erstellung von Aufgaben in Kaspersky Security Center

Sie können Gruppenaufgaben für Administrationsgruppen und für Zusammenstellungen von geschützten Geräten erstellen. Sie können die folgenden Typen von Aufgaben über Kaspersky Security Center erstellen:

- Programm aktivieren
- Update-Verteilung
- Update der Programm-Datenbanken
- Update der Programm-Module
- Rollback des Datenbanken-Updates
- Untersuchung auf Befehl
- Integritätsprüfung für Programme
- Überwachung der Baseline-Integrität
- Erstellen von Regeln für die Kontrolle des Programmstarts
- Erstellen von Regeln für die Gerätekontrolle

Sie können lokale Aufgaben und Gruppenaufgaben auf folgende Art und Weise erstellen:

- Für ein geschütztes Gerät: Im Fenster **Eigenschaften: <Name des geschützten Geräts>** im Abschnitt **Aufgaben**.
- Für eine Administrationsgruppe: Im Ergebnisfenster des Knotens der ausgewählten Gruppe von geschützten Geräten auf der Registerkarte **Aufgaben**.
- Für eine Auswahl an geschützten Geräten: Im Ergebnisfenster des Knotens **Geräteauswahl**.

Mithilfe von Richtlinien können Sie Zeitpläne für lokale Systemaufgaben zum Update und zur Untersuchung auf Befehl auf allen geschützten Geräten in derselben Administrationsgruppe deaktivieren.

Allgemeine Informationen über die Aufgaben in Kaspersky Security Center sind im *Hilfesystem von Kaspersky Security Center* zu finden.

Aufgabe mithilfe von Kaspersky Security Center erstellen

Gehen Sie folgendermaßen vor, um eine neue Aufgabe in der Verwaltungskonsole von Kaspersky Security Center zu erstellen:

1. Starten Sie den Assistenten für neue Aufgaben nach einer der folgenden Methoden:

- Für das Erstellen einer lokalen Aufgabe:

  a. In der Verwaltungskonsole klappen Sie den Knoten **Verwaltete Geräte** auf und gehen auf die Gruppe, zu der das geschützte Gerät gehört.

  b. Öffnen Sie im Ergebnisfenster der Registerkarte **Geräte** das Kontextmenü des geschützten Geräts und wählen Sie den Punkt **Eigenschaften**.

  c. Klicken Sie im nächsten Fenster auf die Schaltfläche **Hinzufügen** im Abschnitt **Aufgaben**.

- Für das Erstellen einer Gruppenaufgabe:

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

  b. Wählen Sie die Administrationsgruppe aus, für die Sie eine Aufgabe erstellen möchten.

  c. Öffnen Sie im Ergebnisfenster die Registerkarte **Aufgaben** und wählen Sie **Aufgabe erstellen**.

- Um eine Aufgabe für eine benutzerdefinierte Auswahl von geschützten Geräten zu erstellen, gehen Sie wie folgt vor:

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

  b. Wählen Sie die Administrationsgruppe aus, in der die geschützten Geräte enthalten sind.

  c. Wählen Sie ein geschütztes Gerät oder eine benutzerdefinierte Zusammenstellung von geschützten Geräten aus.

  d. Wählen Sie aus der Dropdownliste **Aktion ausführen** die Option **Aufgabe erstellen** aus.

  Darauf öffnet sich der Assistent für neue Aufgaben.

2. Wählen Sie im Fenster **Aufgabentyp** unter der Überschrift **Kaspersky Embedded Systems Security 3.1** den Typ der zu erstellenden Aufgabe aus.

3. Wenn Sie einen anderen Aufgabentyp als Rollback des Datenbanken-Updates, Integritätsprüfung für Programme oder Programmaktivierung ausgewählt haben, wird das Fenster **Einstellungen** geöffnet. Die Einstellungen können abhängig vom Aufgabentyp unterschiedlich sein:

   - Aufgabe zur Untersuchung auf Befehl erstellen.

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

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

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

     c. Im Fenster **Verbindungseinstellungen**:

     Geben Sie den Modus des FTP-Servers für die Verbindung mit dem geschützten Gerät 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 Geräte 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** 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 geschützten Geräts erforderlich sein. Damit Kaspersky Embedded Systems Security das geschützte Gerät nach Abschluss der Aufgabe automatisch neu startet, aktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**.

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

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

- Um die Aufgabe zur Update-Verteilung zu erstellen, geben Sie im Fenster **Einstellungen für die Update-Verteilung** die Zusammensetzung der Updates und den Zielordner an.

- Um die Aufgabe zur Aktivierung des Programms zu erstellen, gehen Sie wie folgt vor:

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

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

- Erstellen Sie die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts"

- Erstellen Sie die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle.

4. Passen Sie den Aufgabenzeitplan an.

   Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen.

5. Klicken Sie auf **OK**.

6. Wenn die Aufgabe für eine Zusammenstellung von geschützten Geräten erstellt wird, wählen Sie das Netzwerk (oder die Gruppe) der geschützten Geräte aus, an denen die Aufgabe ausgeführt werden soll.

7. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, womit Sie die Aufgabe ausführen möchten.

8. Geben Sie im Fenster **Aufgabenname festlegen** einen Aufgabennamen an (maximal 100 Zeichen), wobei folgende Zeichen unzulässig sind: " * < > ? \ | : .

   Wir empfehlen, dass Sie den Aufgabentyp zum Namen der Aufgabe hinzufügen (beispielsweise "Untersuchung von freigegebenen Ordnern auf Befehl").

9. Im Fenster **Erstellung der Aufgabe fertig stellen**:

a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten ausführen**, wenn die Aufgabe sofort nach ihrer Erstellung gestartet werden soll.

b. Klicken Sie auf **Fertig**.

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

Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen

Um lokale Aufgaben oder allgemeine Programmeinstellungen für ein einzelnes geschütztes Gerät 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 das geschützte Gerät gehört.

2. Wählen Sie im Ergebnisfenster die Registerkarte **Geräte** aus.

3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Name des geschützten Geräts>** zu öffnen:

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

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.

4. Um lokale Aufgabeneinstellungen anzupassen, gehen Sie wie folgt vor:

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

   b. Wählen Sie in der Aufgabenliste die lokale Aufgabe aus, deren Einstellungen Sie anpassen möchten:

      - Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben.
      - Wählen Sie den Aufgabennamen aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
      - Wählen Sie den Punkt **Eigenschaften** im Kontextmenü der ausgewählten Aufgabe.

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

5. Um Programmeinstellungen anzupassen, gehen Sie wie folgt vor:

   a. Wechseln Sie zum Abschnitt **Programme**.

   b. Wählen Sie in der Liste der installierten Programme das Programm aus, das Sie anpassen möchten:

      - Doppelklicken Sie in der Liste der installierten Programme auf den Programmnamen.
      - Wählen Sie den Programmnamen in der Liste der installierten Programme aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
      - Öffnen Sie in der Liste der installierten Programme das Kontextmenü für den Programmnamen und wählen Sie den Punkt **Eigenschaften**.

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

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

Gruppenaufgaben in Kaspersky Security Center anpassen

Bei der Verwaltung von Kaspersky Embedded Systems Security über die Kaspersky Security Center Cloud Console können Sie keine benutzerdefinierten HTTP- und FTP-Server oder Netzwerkordner manuell hinzufügen.

Gehen Sie wie folgt vor, um eine Gruppenaufgabe für mehrere geschützte Geräte zu konfigurieren:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und klicken Sie auf den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

   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:
     - Legen Sie im Abschnitt **Untersuchungsbereich** einen Untersuchungsbereich fest.
     - Konfigurieren Sie im Abschnitt **Einstellungen** die Integration in andere Programmkomponenten sowie die Aufgabenpriorität.
   - Um eine Update-Aufgabe zu konfigurieren, passen Sie die gewünschten Aufgabenparameter Ihren Bedürfnissen an:

- Passen Sie im Abschnitt **Einstellungen** die Einstellungen für die Update-Quelle an und optimieren Sie das Laufwerk-Subsystem.
- Klicken Sie auf die Schaltfläche **Verbindungseinstellungen**, um die Einstellungen für die Verbindung mit Update-Quellen anzupassen.

- Um die Einstellungen der Aufgabe zum Update der Programm-Module zu konfigurieren, gehen Sie wie folgt vor:
  - Wechseln Sie zum Abschnitt **Einstellungen für das Update der Programm-Module**.
  - Wählen Sie eine auszuführende Aktion aus: Kopieren und installieren Sie wichtige Updates von Programm-Modulen oder nur danach suchen.
- 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.
- So konfigurieren Sie die Aufgabe zur Aktivierung des Programms:
  - 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 Aktivierungscode oder eine Schlüsseldatei zur Verlängerung der Lizenz hinzufügen möchten.
- Um die automatische Generation von Erlaubnisregeln für die Gerätekontrolle zu konfigurieren, geben Sie im Bereich **Einstellungen** die Einstellungen ein, die verwendet werden, um die Liste der Erlaubnisregeln zu erstellen.

6. Passen Sie den Aufgabenzeitplan im Abschnitt **Zeitplan** an. Sie können alle Aufgabentypen außer Rollback des Datenbanken-Updates planen.
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
8. Geben Sie bei Bedarf im Abschnitt **Ausnahmen vom Gültigkeitsbereich** der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
9. Klicken Sie im Fenster **Eigenschaften <Aufgabenname>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Anpassbare Einstellungen für Gruppenaufgaben sind in der nachfolgenden Tabelle zusammengefasst.

Einstellungen für Gruppenaufgaben in Kaspersky Embedded Systems Security

Aufgabentyp in Kaspersky Embedded Systems Security	Abschnitt im Eigenschaftenfenster: <Aufgabenname>	Aufgabeneinstellungen
Erstellen von Regeln für die Kontrolle des Programmstarts	**Einstellungen**	Beim Anpassen der Einstellungen der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" können Sie auswählen, wie Erlaubnisregeln erstellt werden:

		• Erlaubnisregeln auf Grundlage gestarteter Programme erstellen • Erlaubnisregeln für Programme aus folgenden Ordnern erstellen
	Einstellungen	Sie können Aktionen festlegen, die bei der Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen: • **Digitales Zertifikat verwenden** • **Header und Fingerabdruck des digitalen Zertifikats verwenden** • **Falls kein Zertifikat vorhanden, Folgendes verwenden** • **SHA256-Hash verwenden** • **Regeln für Benutzer oder Benutzergruppe erstellen** Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.
	Zeitplan	Sie können Einstellungen anpassen, um eine Aufgabe zu planen.
Erstellen von Regeln für die Gerätekontrolle	**Einstellungen**	• Wählen Sie den Betriebsmodus aus: Berücksichtigen Sie Systemdaten auf allen jemals angeschlossenen externen Geräte oder berücksichtigen Sie nur derzeit angeschlossene externe Geräte. • Passen Sie die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln an, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.
	Zeitplan	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Programm aktivieren	**Aktivierungsparameter**	Um das Programm zu aktivieren oder die Lizenz zu verlängern, können Sie eine Schlüsseldatei hinzufügen.
	Zeitplan	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Update-Verteilung	**Update-Quelle**	Sie können den Administrationsserver von Kaspersky Security Center oder die Kaspersky-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-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.
	Fenster **Verbindungseinstellungen**	Im Fenster **Verbindungseinstellungen**, das aus dem Abschnitt **Update-Quelle** verlinkt ist, können Sie festlegen, ob ein Proxyserver verwendet werden soll, um eine Verbindung zu den Kaspersky-Update-Servern oder anderen Servern herzustellen.
	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 Pfad zu dem Ordner an, in dem Kaspersky Embedded Systems Security die kopierten Updates speichern soll.
	Zeitplan	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Update der Programm-Datenbanken	**Einstellungen**	Im Gruppenfeld **Update-Quelle** können Sie den Administrationsserver von Kaspersky Security Center oder die Kaspersky-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-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind. Im Abschnitt Optimierung der Nutzung des Festplatten-Subsystems können Sie die Funktion zur Verringerung der Auslastung des Festplatten-Subsystems anpassen: • **Belastung des Festplatten-Subsystems verringern** • **Für die Optimierung genutztes Arbeitsspeichervolumen (MB)**
	Fenster **Verbindungseinstellungen**	Im Fenster **Verbindungseinstellungen**, das aus dem Abschnitt **Update-Quelle** verlinkt ist, können Sie festlegen, ob ein Proxyserver verwendet werden soll, um eine Verbindung zu den Kaspersky-Update-Servern oder anderen Servern herzustellen.
	Zeitplan	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Update der Programm-Module	**Update-Quelle**	Sie können den Administrationsserver von Kaspersky Security Center oder die Kaspersky-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-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 ein Proxyserver verwendet werden soll, um eine Verbindung zu den Kaspersky-Update-Servern oder anderen Servern herzustellen.
	Einstellungen für das Update der Programm-Module	Sie können die Aktionen angeben, die Kaspersky Embedded Systems Security bei Vorliegen kritischer Updates der Programm-Module und bei Vorliegen von Informationen über verfügbare planmäßige Updates ausführen soll, sowie auch das Verhalten von Kaspersky Embedded Systems Security nach Abschluss der Installation kritischer Updates anpassen.
	Zeitplan	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Untersuchung auf Befehl anpassen	**Untersuchungsbereich**	Sie können einen Untersuchungsbereich für die Aufgabe zur Untersuchung auf Befehl festlegen sowie zur Einstellung der Sicherheitsstufe wechseln.
	Fenster **Untersuchung auf Befehl anpassen**	Im Fenster **Untersuchung auf Befehl anpassen**, das aus dem Abschnitt **Untersuchungsbereich** verlinkt ist, können Sie eine der vorbestimmten Sicherheitsstufen auswählen oder eine 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 für die Aufgabe zur Untersuchung auf Befehl angeben: Aufgabe im Hintergrundmodus ausführen (niedrige Priorität) oder Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten.
	Zeitplan	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Integritätsprüfung für Programme	**Zeitplan**	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.
Überwachung der Baseline-Integrität	**Zeitplan**	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Für ein Rollback des Datenbanken-Updates können Sie nur die Standardaufgabeneinstellungen anpassen, die von Kaspersky Security Center in den Blöcken **Benachrichtigung** und **Ausnahmen vom Gültigkeitsbereich der Aufgabe** kontrolliert werden.

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

Aufgabe Programm aktivieren

So konfigurieren Sie eine Aufgabe zur Aktivierung des Programms:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und klicken Sie auf den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

   Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
5. Geben Sie im Abschnitt **Aktivierungsparameter** die Schlüsseldatei an, mit der Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.
6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird.
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 Abschnitten finden Sie im *Hilfesystem von Kaspersky Security Center*.
9. Klicken Sie im Fenster **Eigenschaften <Aufgabenname>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Update-Aufgaben

So konfigurieren Sie die Aufgaben "Update-Verteilung", "Update der Programm-Datenbanken" oder "Update der Programm-Module":

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und klicken Sie auf den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

   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. Gehen Sie im Abschnitt **Update-Quelle** wie folgt vor:
   a. Wählen Sie die Update-Quelle aus:
      - Kaspersky Security Center-Administrationsserver.
      - Kaspersky-Update-Server.
      - Andere HTTP-, FTP-Server oder Netzwerkressourcen.

      Um einen freigegebenen SMB-Ordner als Update-Quelle zu verwenden, müssen Sie ein Benutzerkonto für den Aufgabenstart festlegen.

      Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.
   b. Klicken Sie auf **Verbindungseinstellungen**.
   c. Stellen Sie im Fenster **Verbindungseinstellungen**, das sich öffnet, die Verwendung von Proxy-Servern für das Verbinden mit Kaspersky-Update-Servern und anderen Servern ein.

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

> Der Abschnitt zur **Optimierung der Nutzung des Festplatten-Subsystems** ist nur für die Aufgabe zum Update der Programm-Datenbanken verfügbar.

- **Belastung des Festplatten-Subsystems verringern**
- **Für die Optimierung genutztes Arbeitsspeichervolumen (MB)**

6. Geben Sie für die Aufgabe zum Update der Programm-Module im Abschnitt **Einstellungen für das Update der Programm-Module** an, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn wichtige Aktualisierungen von Softwaremodulen verfügbar sind oder Informationen zu geplanten Aktualisierungen verfügbar sind.

   Sie können auch angeben, welche Aktionen Kaspersky Embedded Systems Security ausführen soll, wenn kritische Updates installiert werden.

   > Der Abschnitt **Einstellungen für das Update der Programm-Module** ist nur für die Aufgabe zum Update der Programm-Module verfügbar.

7. Geben Sie für die Aufgabe zur Update-Verteilung im Abschnitt **Einstellungen für die Update-Verteilung** den Satz von Updates und den Zielordner an.

   > Der Abschnitt **Einstellungen für die Update-Verteilung** ist nur für die Aufgabe zur Update-Verteilung verfügbar.

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 die Aufgabe ausgeführt wird.

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

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

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Für ein Rollback des Datenbanken-Updates können Sie nur die 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 Abschnitten finden Sie im *Hilfesystem von Kaspersky Security Center*.

Integritätsprüfung für Programme

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

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und klicken Sie auf den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

   Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
5. Wählen Sie im Abschnitt **Geräte** die Geräte aus, für die Sie die Aufgabe zur Integritätsprüfung für Programme anpassen möchten.
6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird.
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 Abschnitten finden Sie im *Hilfesystem von Kaspersky Security Center*.
9. Klicken Sie im Fenster **Eigenschaften <Aufgabenname>** auf **OK**.

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Anpassen der Einstellungen für die Fehlerdiagnose in Kaspersky Security Center

Wenn beim Betrieb von Kaspersky Embedded Systems Security ein Problem auftritt (z. B. wenn das Programm abstürzt), können Sie es diagnostizieren. Zu diesem Zweck können Sie die Erstellung von Protokoll-Dateien und einer Dump-Datei für den Prozess von Kaspersky Embedded Systems Security aktivieren und diese Dateien zur Analyse an den Technischen Support von Kaspersky senden.

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

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsberechtigungen konfigurieren und nur bestimmten Benutzern den Zugriff auf Protokolle, Trace- und Dump-Dateien erlauben.

Um die Einstellungen für die Fehlerdiagnose in Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center das Fenster **Programmeinstellungen**.
2. Öffnen Sie den Abschnitt **Crash-Diagnose**.
3. Wenn Sie Debug-Informationen in eine Datei schreiben möchten, aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern**.
4. Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.
5. Passen Sie die Genauigkeitsstufe für die Debug-Informationen an.
6. Geben Sie die maximale Größe der Protokolldateien an.
7. Geben Sie die maximale Größe der Dateien für ein Protokoll an.

   Kaspersky Embedded Systems Security erstellt für jede zu debuggende Komponente so viele Protokolldateien, bis die maximale Anzahl erreicht ist.

8. 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).

Subsystemcodes in Kaspersky Embedded Systems Security

Code des Subsystems	Name des Subsystems
*	Alle Komponenten.
gui	Subsystem der Benutzeroberfläche, Snap-In von Kaspersky Embedded Systems Security in der Microsoft Management Console.
ak_conn	Subsystem zur Integration des Administrationsagenten von Kaspersky Security Center.
bl	Steuerungsprozess, implementiert Steuerungsaufgaben von Kaspersky Embedded Systems Security
wp	Arbeitsprozess, der die Aufgaben zum Antiviren-Schutz realisiert
blgate	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security
ods	Subsystem für Untersuchung auf Befehl
oas	Subsystem für den Echtzeitschutz für Dateien
qb	Subsystem für Quarantäne und Backup-Speicher

scandll	Hilfsmodul für die Untersuchung auf Viren.
core	Subsystem für die Antiviren-Basisfunktionalität
avscan	Subsystem für die Antiviren-Bearbeitung
avserv	Subsystem zur Steuerung des Antiviren-Kerns
prague	Subsystem für die Basisfunktionalität
updater	Subsystem für das Datenbanken-Update und das Update der Programm-Module
snmp	Subsystem für Unterstützung des SNMP-Berichts
perfcount	Subsystem für Leistungsindikatoren

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

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

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

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

Die festgelegten Programmeinstellungen werden auf dem geschützten Gerät übernommen.

Arbeit mit dem Aufgabenzeitplan

Sie können Zeitpläne für die Aufgaben von Kaspersky Embedded Systems Security festlegen.

Aufgaben planen

In der Programmkonsole können Sie lokale Systemaufgaben und benutzerdefinierte Aufgaben planen. Gruppenaufgaben können nicht über die Programmkonsole geplant werden.

So planen Sie Gruppenaufgaben mithilfe des Verwaltungs-Plug-in:

1. Öffnen Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Wählen Sie die Gruppe aus, zu der das geschützte Gerät gehört.
3. Wählen Sie im Ergebnisfenster die Registerkarte **Aufgaben** aus.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:

   - Doppelklicken Sie auf den Namen der Aufgabe.
   - Öffnen Sie das Kontextmenü für den Namen der Aufgabe und wählen Sie den Punkt "Eigenschaften".

5. Wählen Sie den Abschnitt **Zeitplan** aus.

6. Aktivieren Sie im Block **Zeitplan-Einstellungen** das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.

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

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

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

      - **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 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 die Startzeit, das Datum und die Häufigkeit der Aufgabe festgelegt haben, wird die geschätzte Zeit für den nächsten Start angezeigt.

      Gehen Sie zur Registerkarte **Zeitplan** und öffnen Sie das Fenster **Aufgabeneinstellungen**. Im oberen Bereich des Fensters wird im Feld **Nächster Start**, die geschätzte Startzeit angezeigt. Jedes Mal, wenn Sie das Fenster öffnen, wird diese geschätzte Startzeit aktualisiert und angezeigt.

      Im Feld **Nächster Start** wird der Wert **Durch Richtlinie verboten** angezeigt, wenn die Richtlinieneinstellungen von Kaspersky Security Center den Start geplanter lokaler Systemaufgaben verhindern.

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

- Im Abschnitt **Einstellungen für das Anhalten der Aufgabe**:

  a. Aktivieren Sie das Kontrollkästchen **Dauer** und geben Sie in den Feldern auf der rechten Seite die maximale Anzahl der Stunden und Minuten für die Ausführung der Aufgabe ein.

  b. Aktivieren Sie das Kontrollkästchen **Anhalten von** und geben Sie in den Feldern auf der rechten Seite den Start- und Endwert eines Zeitintervalls für 24 Stunden ein, in dem die Ausführung der Aufgabe angehalten wird.

- Im Abschnitt **Erweiterte Einstellungen**:

  a. Aktivieren Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.

  b. Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.

  c. Aktivieren Sie das Kontrollkästchen **Aufgabenstart zufällig wählen innerhalb von** und geben Sie einen Wert in Minuten ein.

9. Klicken Sie auf **OK**.

10. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen für den Aufgabenstart zu speichern.

Wenn Sie Programmeinstellungen für eine einzelne Aufgabe mithilfe von Kaspersky Security Center konfigurieren möchten, siehe Abschnitt "Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen".

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 den Zeitplan für den Aufgabenstart zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

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

2. Wählen Sie die Gruppe aus, zu der das geschützte Gerät gehört.

3. Wählen Sie im Ergebnisfenster die Registerkarte **Aufgaben** aus.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:

   - Doppelklicken Sie auf den Namen der Aufgabe.

   - Öffnen Sie das Kontextmenü für den Namen der Aufgabe und wählen Sie den Punkt "Eigenschaften".

5. Wählen Sie den Abschnitt **Zeitplan** aus.

6. Führen Sie einen der folgenden Schritte aus:

- Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**, wenn Sie den Aufgabenstart nach Zeitplan aktivieren möchten
- Deaktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**, 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.

7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Übernehmen**.

Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden gespeichert.

Berichte in Kaspersky Security Center

Die Berichte von Kaspersky Security Center enthalten Informationen zum Status der verwalteten Geräte. Die Berichte basieren auf Informationen, die auf dem Administrationsserver gespeichert sind.

Ab Kaspersky Security Center 11 sind folgende Berichtstypen für Kaspersky Embedded Systems Security verfügbar:

- Bericht über den Status der Programmkomponenten
- Bericht über verbotene Programme
- Bericht über verbotene Programme im Testmodus

Detaillierte Informationen zu allen Berichten in Kaspersky Security Center und deren Konfiguration finden Sie in der *Hilfe zu Kaspersky Security Center*.

Bericht über den Status der Programmkomponenten von Kaspersky Embedded Systems Security

Sie können den Schutzstatus aller Netzwerkgeräte überwachen und eine strukturierte Übersicht der Komponentenauswahl auf jedem Gerät anzeigen lassen.

Der Bericht zeigt für jede Komponente eine der folgenden Statusvarianten an: *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, wird in Kaspersky Security Center der Status N/A (Nicht verfügbar) zugewiesen.

Sie können eine Komponentenauswahl erstellen und den Filter verwenden, um Netzwerkgeräte mit einer festgelegten Auswahl an Komponenten samt Status anzuzeigen.

Nähere Informationen zur Erstellung und Verwendung einer Auswahl finden Sie in der *Hilfe zu Kaspersky Security Center*.

Um den aktuellen Status der Komponenten in den Programmeinstellungen zu überprüfen, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der 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**.
3. Wählen Sie den Abschnitt **Komponenten**.
4. Eine Tabelle mit Statusvarianten wird Ihnen angezeigt.

Um einen Standardbericht für Kaspersky Security Center anzusehen, gehen Sie wie folgt vor:

1. Wählen Sie in der Programmkonsolenstruktur den Knoten **Administrationsserver <Name des Administrationsservers>**.
2. Öffnen Sie die Registerkarte **Protokolle**.
3. Doppelklicken Sie auf das Listenelement **Bericht über den Status der Programmkomponenten**.

   Ein Bericht wird erstellt.
4. Sehen Sie sich die folgenden Berichtsdetails an:
   - Schaubild.
   - Übersichtstabelle mit Komponenten und der Gesamtanzahl der Netzwerkgeräte, auf denen jede Komponente installiert ist, sowie die Gruppen, zu denen sie gehören.
   - Detaillierte Tabelle mit dem Status, der Version, dem Gerät und der Gruppe der Komponente.

Berichte über verbotene Programme im Modus "Aktiv" und "Statistik"

Basierend auf den Ergebnissen der Aufgabe zur Kontrolle des Programmstarts können zwei Arten von Berichten erstellt werden: ein Bericht über verbotene Programme (wenn die Aufgabe im 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 Geräten im Netzwerk. Jeder Bericht wird für alle Administrationsgruppen erstellt und sammelt die Daten aller Kaspersky-Programme, die auf den geschützten Geräten installiert sind.

Um einen Bericht über verbotene Programme im Modus "Nur Statistik" anzuzeigen, gehen Sie wie folgt vor:

1. Starten Sie die Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik.
2. Wählen Sie in der Programmkonsolenstruktur den Knoten **Administrationsserver <Name des Administrationsservers>**.
3. Öffnen Sie die Registerkarte **Protokolle**.
4. Doppelklicken Sie auf das Element **Bericht über verbotene Programme im Testmodus**.

Ein Bericht wird erstellt.

5. Sehen Sie sich die folgenden Berichtsdetails an:

   - Ein Schaubild mit den Top-10-Programmen, deren Start am häufigsten blockiert wurde.
   - Eine Übersichtstabelle mit den Fällen, in denen ein Programm blockiert wurde, mit Angabe des Namens der ausführbaren Datei, der Ursache, der Uhrzeit der Blockierung und der Anzahl der Geräte, auf denen sie stattgefunden hat.
   - Eine ausführliche Tabelle welche die Daten zum Gerät, dem Dateipfad und die Kriterien für das Blockieren angibt.

Um einen Bericht über verbotene Programme im Modus "Aktiv" anzuzeigen, gehen Sie wie folgt vor:

1. Starten Sie die Aufgabe zur Kontrolle des Programmstarts im Modus "Aktiv".
2. Wählen Sie in der Programmkonsolenstruktur den Knoten **Administrationsserver <Name des Administrationsservers>**.
3. Öffnen Sie die Registerkarte **Protokolle**.
4. Doppelklicken Sie auf das Element **Bericht über verbotene Programme**.

   Ein Bericht wird erstellt.

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

Verwendung der Konsole für Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zur Konsole für Kaspersky Embedded Systems Security und zur Verwaltung des Programms über die Programmkonsole, die auf dem geschützten Gerät oder auf einem anderen Gerät installiert ist.

Über die Konsole für Kaspersky Embedded Systems Security

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

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

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

Sie können die Programmkonsole und Kaspersky Embedded Systems Security auf verschiedenen geschützten Geräten installieren, die verschiedenen Domänen zugewiesen sind. In diesem Fall kann es Einschränkungen beim Senden von Informationen von dem Programm an die Programmkonsole geben. Beispielsweise wird nach dem Start einer Aufgabe in der Programmkonsole der Status dieser Aufgabe in der Programmkonsole möglicherweise nicht mehr aktualisiert.

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

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

In der 64-Bit-Version von Microsoft Windows können Sie das Snap-in von Kaspersky Embedded Systems Security nur in der 32-Bit-Version der Microsoft Management Console hinzufügen. Zum Hinzufügen des Kaspersky Embedded Systems Security-Snap-Ins, öffnen Sie die Microsoft Management Console über die Befehlszeile, indem Sie den folgenden Befehl ausführen: mmc.exe /32.

Mehrere Kaspersky Embedded Systems Security-Snap-Ins können einer Microsoft Management Console, die im Autorenmodus geöffnet ist, hinzugefügt werden. Sie können dann den Schutz mehrerer Geräte verwalten, auf denen Kaspersky Embedded Systems installiert ist.

Benutzeroberfläche der Konsole für Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zu den wichtigsten Elementen der Programmoberfläche.

Fenster "Konsole für Kaspersky Embedded Systems Security"

Die Konsole für Kaspersky Embedded Systems Security wird in der Struktur der Microsoft Management Console als Knoten angezeigt.

Nachdem eine Verbindung mit dem Programm Kaspersky Embedded Systems Security, das auf einem anderen geschützten Gerät installiert ist, hergestellt wurde, werden der Name des geschützten Geräts, auf dem das Programm installiert ist, sowie der Name des Benutzerkontos, mit dessen Rechten die Verbindung hergestellt wurde, zur Bezeichnung des Knotens hinzugefügt: **Kaspersky Embedded Systems Security <Name des geschützten Geräts> als <Benutzerkonto-Name>**. Wenn die Verbindung zu Kaspersky Embedded Systems Security, das auf demselben geschützten Gerät wie die Programmkonsole installiert ist, hergestellt wird, ändert sich der Knotenname in **Kaspersky Embedded Systems Security**.

Die Programmkonsolenstruktur

Die Struktur der Programmkonsole enthält den Hauptknoten **Kaspersky Embedded Systems Security** und die untergeordneten Knoten für die funktionellen Programmkomponenten.

Der Knoten **Kaspersky Embedded Systems Security** enthält die folgenden untergeordneten Knoten:

- **Echtzeit-Computerschutz**: Verwaltung von Aufgaben zum Echtzeit-Computerschutz und von KSN-Diensten. Im Knoten **Echtzeit-Computerschutz** können die folgenden Aufgaben angepasst werden:
  - **Echtzeitschutz für Dateien**
  - **Verwendung von KSN**
  - **Exploit-Prävention**
- **Computer-Kontrolle**: kontrolliert den Start der auf dem geschützten Gerät installierten Programme und der Verbindungen zu externen Geräten. Im Knoten **Computer-Kontrolle** können die folgenden Aufgaben verwaltet werden:
  - **Kontrolle des Programmstarts**
  - **Gerätekontrolle**
  - **Firewall-Verwaltung**
- **Automatisches Erstellen von Regeln**: passt die automatische Erstellung von Gruppen- und Systemregeln für die Aufgaben "Kontrolle des Programmstarts" und "Gerätekontrolle" an.
  - **Erstellen von Regeln für die Kontrolle des Programmstarts**
  - **Erstellen von Regeln für die Gerätekontrolle**
  - Gruppenaufgaben für die Erstellung von Regeln **<Namen der Aufgaben>** (sofern vorhanden).

    Gruppenaufgaben werden mithilfe von Kaspersky Security Center erstellt. Gruppenaufgaben können nicht über die Programmkonsole verwaltet werden.
- **System-Diagnose**: Anpassen der Steuerung von Dateioperationen und der Einstellungen für die Analyse des Windows-Ereignisprotokolls.
  - **Überwachung der Datei-Integrität**
  - **Protokollanalyse**

- **Untersuchung auf Befehl**: Verwalten der Aufgabe zur Virensuche. Jede Aufgabe hat ihr eigenes Steuerelement:
  - **Untersuchung beim Hochfahren des Betriebssystems**
  - **Untersuchung wichtiger Bereiche**
  - **Untersuchung von Quarantäne-Objekten**
  - **Integritätsprüfung für Programme**
  - Benutzerdefinierte Aufgaben **<Namen der Aufgaben>** (sofern vorhanden)

  Im Knoten werden Systemaufgaben, bei der Installation erstellte Programme, benutzerdefinierte Aufgaben sowie Gruppenaufgaben zur Untersuchung auf Befehl angezeigt, die mithilfe von Kaspersky Security Center erstellt und an das geschützte Gerät übertragen wurden.
- **Update**: Verwaltet Datenbanken-Updates und Updates der Module für Kaspersky Embedded Systems Security und kopiert das Update in einen Ordner als lokale Update-Quelle. Der Knoten enthält untergeordnete Knoten für die Steuerung jeder Update-Aufgabe und für die Aufgabe **Rollback des Programm-Datenbanken-Updates**:
  - **Update der Programm-Datenbanken**
  - **Update der Programm-Module**
  - **Update-Verteilung**
  - **Rollback des Programm-Datenbanken-Updates**

  Im Knoten werden alle benutzerdefinierten Aufgaben und Gruppenaufgaben zum Update angezeigt, die mithilfe von Kaspersky Security Center erstellt und an das geschützte Gerät übertragen wurden.
- **Speicher**: Verwaltung von Quarantäne- und Backup-Einstellungen.
  - **Quarantäne**
  - **Backup**
- **Protokolle und Benachrichtigungen**: Verwaltet die lokalen Protokolle der Aufgabenausführung, das Sicherheitsprotokoll und das Systemaudit-Protokoll von Kaspersky Embedded Systems Security.
  - **Sicherheitsprotokoll**
  - **Systemaudit-Protokoll**
  - **Protokolle der Aufgabenausführung**
- **Lizenzverwaltung**: Schlüssel und Aktivierungscodes für Kaspersky Embedded Systems Security hinzufügen oder löschen, Informationen über Lizenzen anzeigen.

Ergebnisfenster

Im Ergebnisfenster werden Informationen über den ausgewählten Knoten angezeigt. Wenn der Knoten **Kaspersky Embedded Systems Security** ausgewählt ist, werden im Detailbereich Informationen über den aktuellen Schutzstatus des Geräts und Informationen über Kaspersky Embedded Systems Security, den Schutzstatus seiner funktionellen Komponenten und das Ablaufdatum der Lizenz angezeigt.

Kontextmenü des Knotens "Kaspersky Embedded Systems Security"

Mithilfe der Befehle im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** können Sie folgende Aktionen ausführen:

- **Verbindung mit anderem Computer herstellen**. Verbindung mit anderem Gerät herstellen, um Kaspersky Embedded Systems Security zu verwalten, das darauf installiert ist. Hierfür können Sie auch den Link in der rechten unteren Ecke im Ergebnisbereich des Knotens **Kaspersky Embedded Systems Security** verwenden.
- **Dienst starten** / **Dienst beenden**. Programm oder eine ausgewählte Aufgabe starten oder beenden. Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden. Dies kann auch über das Kontextmenü der Aufgaben des Programms erfolgen.
- **Untersuchung von Wechseldatenträgern anpassen.** Die Untersuchung von Wechseldatenträgern anpassen, die über den USB-Anschluss an das geschützte Gerät angeschlossen werden.
- **Einstellungen der vertrauenswürdigen Zone anpassen.** Einstellungen der vertrauenswürdigen Zone aufrufen und anpassen.
- **Benutzerrechte für die Programmverwaltung ändern**. Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security aufrufen und anpassen.
- **Benutzerrechte für die Verwaltung von Kaspersky Security Service ändern**. Benutzerrechte für die Verwaltung von Kaspersky Security Service anzeigen und anpassen.
- **Einstellungen exportieren**. Programmeinstellungen in einer Konfigurationsdatei im XML-Format speichern. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Einstellungen importieren**. Programmeinstellungen aus Konfigurationsdatei im XML-Format importieren. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Angaben zum Programm und zu verfügbaren Modul-Updates.** Siehe Informationen über Kaspersky Embedded Systems Security sowie über aktuelle verfügbare Updates der Programm-Module.
- **Aktualisieren**. Fensterinhalte der Programmkonsole aktualisieren. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.
- **Eigenschaften**. Einstellungen von Kaspersky Embedded Systems Security oder einer ausgewählten Aufgabe anzeigen und anpassen. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.

  Hierfür können Sie auch den Link **Eigenschaften des Programms** im Ergebnisbereich des Knotens **Kaspersky Embedded Systems Security** oder die Schaltfläche in der Symbolleiste verwenden.

- **Hilfe**. Informationen hierzu finden Sie in der Hilfe zu Kaspersky Embedded Systems Security. Dies kann auch über das Kontextmenü der Aufgabe des Programms erfolgen.

Symbolleiste und Kontextmenü der Aufgaben von Kaspersky Embedded Systems Security

Sie können die Aufgaben für Kaspersky Embedded Systems Security mithilfe der Punkte des Kontextmenüs für jede Aufgabe in der Programmkonsolenstruktur verwalten.

Mithilfe der Punkte im Kontextmenü der ausgewählten Aufgabe können Sie folgende Aktionen ausführen:

- **Starten/Beenden**. Die Ausführung einer Aufgabe starten oder beenden. Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden.
- **Fortsetzen / Anhalten**. Ausführung der Aufgabe anhalten/fortsetzen. Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden. Diese Aktion ist nur für Aufgaben zum Echtzeit-Computerschutz und zur Untersuchung auf Befehl verfügbar.
- **Aufgabe hinzufügen**. Neue benutzerdefinierte Aufgabe erstellen. Diese Aktion ist nur für Untersuchungen auf Befehl verfügbar.
- **Protokoll öffnen**. Protokoll der Aufgabenausführung anzeigen und verwalten. Diese Operation ist für alle Aufgaben verfügbar.
- **Aufgabe löschen**. Benutzerdefinierte Aufgabe löschen. Diese Aktion ist nur für Untersuchungen auf Befehl verfügbar.
- **Vorlagen für Einstellungen**. Vorlagen verwalten. Diese Aktion ist nur für Aufgaben zum Echtzeitschutz für Dateien und zur Untersuchung auf Befehl verfügbar.

Taskleistensymbol im Infobereich

Jedes Mal, wenn Kaspersky Embedded Systems Security nach dem Neustart des geschützten Geräts automatisch gestartet wird, erscheint im Infobereich das Taskleistensymbol . Es wird standardmäßig angezeigt, wenn Sie bei der Installation des Programms die Komponente Taskleistensymbol installiert haben.

Das Aussehen des Taskleistensymbols zeigt den aktuellen Schutzstatus des Geräts an. Es gibt zwei Arten von Status:

	Aktiv (farbiges Symbol) – mindestens eine der folgenden Aufgaben wird derzeit ausgeführt: Echtzeitschutz für Dateien oder Kontrolle des Programmstarts
	Inaktiv (graues Symbol) – keine der folgenden Aufgaben wird ausgeführt: Echtzeitschutz für Dateien und Kontrolle des Programmstarts

Sie können das Kontextmenü des Taskleistensymbols mit der rechten Maustaste öffnen.

Das Kontextmenü enthält mehrere Befehle zur Anzeige der Programmfenster (s. Tabelle unten).

Befehle im Kontextmenü des Taskleistensymbols

Befehl	Beschreibung
Programmkonsole öffnen	Öffnet die Konsole für Kaspersky Embedded Systems Security (falls installiert).
Kompaktes Diagnosefenster öffnen	Öffnet das kompakte Diagnosefenster.
Über das Programm	Öffnet das Fenster **Über das Programm** mit Informationen zu Kaspersky Embedded Systems Security.

	Wenn Sie als Benutzer von Kaspersky Embedded Systems Security registriert sind, enthält das Fenster **Über das Programm** Informationen über die installierten kritischen Updates.
Ausblenden	Blendet das Taskleistensymbol im Infobereich der Taskleiste aus.

Sie können das ausgeblendete Taskleistensymbol jederzeit wieder einblenden.

Um das Taskleistensymbol wieder einzublenden,

wählen Sie im **Startmenü** von Microsoft Windows **Alle Programme** > **Kaspersky Embedded Systems Security** > **Systemfachsymbol** aus.

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

In den allgemeinen Einstellungen von Kaspersky Embedded Systems Security können Sie festlegen, ob das Taskleistensymbol angezeigt werden soll oder nicht, wenn das Programm nach dem Neustart des geschützten Geräts automatisch gestartet wird.

Kaspersky Embedded Systems Security über die Programmkonsole auf einem anderen Gerät verwalten

Sie können Kaspersky Embedded Systems Security über eine auf einem Remote-Gerät installierte Programmkonsole verwalten.

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, damit die Programmverwaltung mithilfe der Konsole für Kaspersky Embedded Systems Security auf einem Remote-Gerät verfügbar ist:

- Die Benutzer der Programmkonsole auf einem Remote-Gerät sind der Gruppe der ESS-Administratoren auf dem geschützten Gerät zugeordnet.
- Wenn auf dem geschützten Gerät die Windows-Firewall aktiviert ist, sind Netzwerkverbindungen für den Prozess des Kaspersky Security Management Service kavfsgt.exe erlaubt.
- Während der Installation von Kaspersky Embedded Systems Security wird im Fenster des Installationsassistenten das Kontrollkästchen **Remote-Zugriff erlauben** aktiviert.

Wenn Kaspersky Embedded Systems Security auf dem Remote-Gerät kennwortgeschützt ist, geben Sie ein Kennwort ein, um Zugriff auf die Programmverwaltung über die Programmkonsole zu erhalten.

Allgemeine Programmeinstellungen über die Programmkonsole konfigurieren

Die allgemeinen Einstellungen und die Einstellungen für die Crash-Diagnose von Kaspersky Embedded Systems Security legen die allgemeinen Bedingungen für den Einsatz des Programms fest. Diese Einstellungen ermöglichen Folgendes: Regelung der Anzahl der aktiven Prozesse, die von Kaspersky Embedded Systems Security verwendet werden; Wiederherstellung der Aufgaben von Kaspersky Embedded Systems Security nach deren Absturz aktivieren; Führen eines Protokolls; Anlegen von Dump-Dateien für Prozesse von Kaspersky Embedded Systems Security bei deren Absturz; andere allgemeine Einstellungen.

Die Programmeinstellungen sind in der Programmkonsole nicht verfügbar, wenn die aktive Richtlinie von Kaspersky Security Center Änderungen der festgelegten Einstellungen blockiert.

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

1. Wählen Sie in der Struktur der Programmkonsole den Knoten **Kaspersky Embedded Systems Security** aus und führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Eigenschaften des Programms**.
   - Wählen Sie im Kontextmenü des Knotens **Eigenschaften** aus.

   Das Fenster **Programmeinstellungen** wird geöffnet.

2. Legen Sie im nächsten Fenster die allgemeinen Einstellungen von Kaspersky Embedded Systems Security gemäß Ihren Anforderungen fest:

   - Auf der Registerkarte **Skalierbarkeit und Oberfläche** können Sie folgende Einstellungen anpassen:
     - Im Abschnitt **Skalierbarkeitseinstellungen**:
       - Maximale Anzahl der Arbeitsprozesse, die von Kaspersky Embedded Systems Security gestartet werden können
       - Anzahl der Prozesse für den Echtzeitschutz
       - Anzahl der aktiven Prozesse für im Hintergrund laufende Aufgaben zur Untersuchung auf Befehl
   - Wählen Sie im Abschnitt **Interaktion mit dem Benutzer** aus, ob das Taskleistensymbol nach jedem Start des Programms in der Taskleiste angezeigt werden soll.
   - Auf der Registerkarte **Sicherheit und Zuverlässigkeit** können Sie folgende Einstellungen anpassen:
     - Im Bereich **Einstellungen für den Kennwortschutz** konfigurieren Sie den Schutz von Programmprozessen.
     - Passen Sie im Abschnitt **Einstellungen für den Kennwortschutz** die Einstellungen für den Kennwortschutz der Programmfunktionen an.
     - Geben Sie im Abschnitt **Selbstschutz** die Anzahl der Versuche zur Wiederherstellung von Aufgaben zur Untersuchung auf Befehl bei einem Absturz an.
   - Legen Sie im Abschnitt **Maximale Anzahl zum Wiederherstellen der Aufgaben zur Untersuchung auf Befehl** die Aktionen fest, die Kaspersky Embedded Systems Security nach dem Wechsel in den USV-Akkubetrieb ausführen soll.
   - Auf der Registerkarte **Untersuchungseinstellungen**:
     - **Dateiattribute nach der Untersuchung wiederherstellen**
     - **CPU-Auslastung für die Untersuchung auf Bedrohungen begrenzen**
       - **Obergrenze (Prozent)**
     - **Ordner für während der Untersuchung erstellte temporäre Dateien**

- Auf der Registerkarte **Verbindungseinstellungen**:
  - Geben Sie im Abschnitt **Proxyserver-Einstellungen** die Einstellungen für den Proxyserver an.
  - Geben Sie im Abschnitt **Einstellungen für die Authentifizierung auf dem Proxyserver** den Authentifizierungstyp und die notwendigen Daten für die Authentifizierung auf dem Proxyserver an.
  - Geben Sie im Abschnitt **Lizenzverwaltung** an, ob Kaspersky Security Center als Proxyserver für die Programmaktivierung verwendet wird.
- Auf der Registerkarte **Crash-Diagnose**:
  - Wenn Sie Debug-Informationen in eine Datei schreiben möchten, aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern**.
    - Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.
    - Passen Sie die Genauigkeitsstufe für die Debug-Informationen an.
    - Geben Sie die maximale Größe der Protokolldateien an.
    - Geben Sie die maximale Größe der Dateien für ein Protokoll an. Kaspersky Embedded Systems Security erstellt für jede zu debuggende Komponente so viele Protokolldateien, bis die maximale Anzahl erreicht ist.
    - Geben Sie die Komponenten für das Debuggen an.
  - Wenn Sie eine Dump-Datei erstellen möchten, aktivieren Sie das Kontrollkästchen **Bei Absturz Dump-Datei erstellen**.

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

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

    Die Informationen in den Dump-Dateien des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsberechtigungen konfigurieren und nur bestimmten Benutzern den Zugriff auf Protokolle, Trace- und Dump-Dateien erlauben.

3. Klicken Sie auf **OK**.

Die Einstellungen von Kaspersky Embedded Systems Security werden gespeichert.

Aufgaben von Kaspersky Embedded Systems Security verwalten

Dieser Abschnitt enthält Informationen zum Erstellen, Konfigurieren, Starten und Beenden der Aufgaben von Kaspersky Embedded Systems Security.

Aufgabenkategorien von Kaspersky Embedded Systems Security

Die Funktionen Echtzeit-Computerschutz, Computer-Kontrolle, Untersuchung auf Befehl und Update in Kaspersky Embedded Systems Security sind in Form von Aufgaben implementiert.

Aufgaben lassen sich über das Kontextmenü des Aufgabennamens in der Struktur der Programmkonsole, der Symbolleiste und der Symbolleiste für den Schnellzugriff verwalten. Informationen über den Aufgabenstatus werden im Ergebnisfenster angezeigt. Operationen, die sich auf die Verwaltung von Aufgaben beziehen, werden im Systemaudit-Protokoll protokolliert.

Es gibt zwei Typen von Aufgaben in Kaspersky Embedded Systems Security: *lokal* und *Gruppe*.

Lokale Aufgaben

Lokale Aufgaben können nur auf dem geschützten Gerät ausgeführt werden, für das sie erstellt wurden. Je nach Startmethode existieren folgende Typen lokaler Aufgaben:

- **Lokale Systemaufgaben**. Diese Aufgaben werden während der Installation von Kaspersky Embedded Systems Security automatisch erstellt. Sie können die Einstellungen aller lokaler Systemaufgaben ändern. Eine Ausnahme bilden die Aufgaben "Untersuchung von Quarantäne-Objekten" und "Rollback des Datenbanken-Updates". Sie können die lokalen Systemaufgaben nicht umbenennen oder löschen. Lokale Systemaufgaben und benutzerdefinierte Aufgaben zur Untersuchung auf Befehl können gleichzeitig gestartet werden.

- **Lokale benutzerdefinierte Aufgaben**. In der Programmkonsole können Sie Aufgaben zur Untersuchung auf Befehl erstellen. In Kaspersky Security Center können Sie Aufgaben für die Untersuchung auf Befehl, für das Update der Programm-Datenbanken, für das Rollback des Datenbanken-Updates und für die Update-Verteilung erstellen. Sie können benutzerdefinierte Aufgaben umbenennen, anpassen und löschen. Es können gleichzeitig mehrere benutzerdefinierte Aufgaben gestartet werden.

Gruppenaufgaben

Gruppenaufgaben und Aufgaben für Zusammenstellungen von geschützten Geräten können über Kaspersky Security Center verwaltet werden. Alle Gruppenaufgaben sind benutzerdefinierte Aufgaben. Gruppenaufgaben werden ebenso in der Programmkonsole angezeigt. In der Programmkonsole können Sie nur den Status von Gruppenaufgaben sehen. Sie können die Programmkonsole nicht zum Verwalten oder Konfigurieren von Gruppenaufgaben verwenden.

Manuelles Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe

Sie können nur die Aufgaben Echtzeit-Computerschutz und Untersuchung auf Befehl anhalten und fortsetzen. Keine anderen Aufgaben können manuell angehalten oder fortgesetzt werden.

So können Sie eine Aufgabe starten, anhalten, fortsetzen oder beenden:

1. Öffnen Sie in der Programmkonsole das Kontextmenü der Aufgabe.

2. Wählen Sie einen der folgenden Punkte aus: **Starten**, **Anhalten**, **Fortsetzen** oder **Beenden**.

Die Operation wird ausgeführt und im Systemaudit-Protokoll erfasst.

Wenn Sie eine Aufgabe zur Untersuchung auf Befehl fortsetzen, setzt Kaspersky Embedded Systems Security die Untersuchung von dem Objekt fort, an dem die Untersuchung angehalten wurde.

Arbeit mit dem Aufgabenzeitplan

Sie können Zeitpläne für die Aufgaben von Kaspersky Embedded Systems Security festlegen.

Einstellungen für den Aufgabenzeitplan anpassen

In der Programmkonsole können Sie planen, wann lokale System- und benutzerdefinierte Aufgaben gestartet werden sollen. Sie können jedoch nicht planen, wann Gruppenaufgaben gestartet werden sollen.

So planen Sie eine Aufgabe:

1. Öffnen Sie das Kontextmenü der Aufgabe, die Sie planen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Zeitplan** das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.
4. Führen Sie die folgenden Schritte aus, um Zeitplan-Einstellungen festzulegen:

   a. Wählen Sie im Dropdown-Menü **Startintervall** eines der Folgenden aus:

   - **Alle n Stunden**: Um die Aufgabe in stündlichen Abständen auszuführen, geben Sie die Anzahl der Stunden im Feld **Alle** <Anzahl> **Stunden** ein.
   - **Alle n Tage**: Um die Aufgabe in täglichen Intervallen auszuführen; geben Sie die Anzahl der Tage im Feld **Alle** <Anzahl> **Tage** ein.
   - **Wöchentlich**: Um die Aufgabe in wöchentlichen Intervallen auszuführen; geben Sie die Anzahl der Wochen im Feld **Alle** <Anzahl> **Wochen am** ein. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (standardmäßig werden Aufgaben montags gestartet).
   - **Bei Programmstart**: Um die Aufgabe bei jedem Start von Kaspersky Embedded Systems Security auszuführen.
   - **Nach dem Update der Programm-Datenbanken**: Um die Aufgabe nach jedem Update der Programm-Datenbanken auszuführen.

   b. Geben Sie im Feld **Startzeit** den Zeitpunkt an, zu dem die Aufgabe zum ersten Mal gestartet werden soll.

   c. Geben Sie im Feld **Beginnen am** das Datum an, zu dem die Aufgabe zum ersten Mal gestartet werden soll.

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 geschätzte Zeitpunkt des nächsten Aufgabenstarts angezeigt. Die geschätzte Zeit, die bis zum nächsten Aufgabenstart verbleibt, wird jedes Mal angezeigt, wenn Sie das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Zeitplan** öffnen.

Im Feld **Nächster Start** wird der Wert **Durch Richtlinie verboten** angezeigt, wenn die Einstellungen der geltenden Richtlinie von Kaspersky Security Center den Start einer geplanten lokalen Systemaufgabe verhindern.

5. Verwenden Sie die Registerkarte **Erweitert**, um die folgenden Zeitplan-Einstellungen festzulegen:

   - Im Abschnitt **Einstellungen für das Anhalten der Aufgabe**:

     a. Wählen Sie das Kontrollkästchen **Dauer**. Geben Sie in die Felder rechts die maximale Aufgabendauer in Stunden und Minuten ein.

     b. Wählen Sie das Kontrollkästchen **Anhalten von**. Geben Sie in die Felder rechts ein, wann die Aufgabe angehalten und fortgesetzt werden soll (unter 24 Stunden).

   - Im Abschnitt **Erweiterte Einstellungen**:

     a. Wählen Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und geben das Enddatum des Aufgabenzeitplans an.

     b. Wählen Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, um übersprungene Aufgaben zu starten.

     c. Aktivieren Sie das Kontrollkästchen **Aufgabenstart zufällig wählen innerhalb von** und geben Sie einen Wert in Minuten ein.

6. Klicken Sie auf **OK**.

Die Zeitplan-Einstellungen werden gespeichert.

Start nach Zeitplan aktivieren und deaktivieren

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

So aktivieren oder deaktivieren Sie den Zeitplan für den Aufgabenstart:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für die geplante Aufgabe.

2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Zeitplan** eine der folgenden Aktionen:

   - Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen** um den Zeitplan für den Aufgabenstart zu aktivieren.

- Deaktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**, um den Zeitplan für den Aufgabenstart zu deaktivieren.

  Die Einstellungen für den Aufgabenzeitplan werden nicht gelöscht, sondern beim nächsten Aktivieren eines Zeitplans für den Aufgabenstart angewendet.

4. Klicken Sie auf **OK**.

Die Zeitplan-Einstellungen werden gespeichert.

Verwendung von Benutzerkonten für den Aufgabenstart

Sie können Aufgaben starten, indem Sie das Systemkonto verwenden oder ein anderes Benutzerkonto angeben.

Über die Verwendung eines Benutzerkontos für den Aufgabenstart

Sie können das Konto angeben, um die folgenden Aufgaben von Kaspersky Embedded Systems Security auszuführen:

- Erstellen von Regeln für die Kontrolle des Programmstarts
- Erstellen von Regeln für die Gerätekontrolle
- Untersuchung auf Befehl
- Update

Die angegebenen Aufgaben werden standardmäßig mit den Rechten des Systemkontos ausgeführt.

In folgenden Fällen sollten Sie ein anderes Benutzerkonto mit ausreichenden Zugriffsrechten angeben:

- Aufgabe **Update**: Wenn Sie als Update-Quelle einen freigegebenen Ordner auf einem anderen Netzwerkgerät angegeben haben.
- Aufgabe **Update**: Wenn für Zugriff auf die Update-Quelle ein Proxyserver mit integrierter NTLM-Authentifizierung von Microsoft Windows verwendet wird.
- Aufgaben **zur Untersuchung auf Befehl**: Wenn das Systemkonto nicht über die Zugriffsrechte für die untersuchenden Objekte verfügt (z. B. Zugriff auf Dateien in den freigegebenen Ordnern des geschützten Geräts).
- Aufgabe **Erstellen von Regeln für die Kontrolle des Programmstarts**: Wenn die erstellten Regeln in eine Konfigurationsdatei exportiert werden, die sich an einem Speicherort befindet, auf den das Systemkonto keinen Zugriff hat (z. B. in einem der freigegebenen Ordner auf dem geschützten Gerät).

Sie können die Aufgaben zum Update, zur Untersuchung auf Befehl und zur automatischen Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts mit den Rechten des Systemkontos starten. Kaspersky Embedded Systems Security führt diese Aufgaben aus und greift auf die freigegebenen Ordner auf einem anderen Netzwerk-Gerät zu, wenn dieses Gerät in derselben Domäne wie das geschützte Gerät registriert ist. In diesem Fall muss das Systemkonto über die Zugriffsrechte für diese Ordner verfügen. Kaspersky Embedded Systems Security greift dann mit den Rechten des Kontos **<Domänenname \ Gerätename>** auf das Gerät zu.

Benutzerkonto für den Aufgabenstart festlegen

So legen Sie ein Konto für den Aufgabenstart fest:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü von der Aufgabe, die Sie starten möchten, indem Sie ein bestimmtes Benutzerkonto verwenden.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
3. Führen Sie im folgenden Fenster auf der Registerkarte **Mit folgenden Rechten starten** die folgenden Schritte aus:

   a. Wählen Sie den Punkt **Benutzername** aus.

   b. Geben Sie den Namen und das Kennwort des Benutzers an, dessen Benutzerkonto Sie verwenden möchten.

   Der von Ihnen ausgewählte Benutzer muss auf dem geschützten Gerät oder in der gleichen Domäne wie dieses geschützte Gerät angemeldet sein.

   c. Bestätigen Sie das Kennwort.
4. Klicken Sie auf **OK**.

Die Änderung der Einstellungen wird gespeichert.

Import und Export von Einstellungen

In diesem Abschnitt wird erläutert, wie Sie die Einstellungen von Kaspersky Embedded Systems Security exportieren. Außerdem erfahren Sie, wie Sie bestimmte Softwareeinstellungen in eine XML-Konfigurationsdatei exportieren und diese Einstellungen aus einer Konfigurationsdatei zurück in das Programm importieren.

Über den Import und Export von Einstellungen

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

Wenn Sie alle Einstellungen von Kaspersky Embedded Systems Security exportieren, dann werden die allgemeinen Programmeinstellungen und die Einstellungen der folgenden Komponenten und Funktionen von Kaspersky Embedded Systems Security in eine Datei geschrieben:

- Echtzeitschutz für Dateien
- Verwendung von KSN
- Gerätekontrolle
- Kontrolle des Programmstarts
- Erstellen von Regeln für die Gerätekontrolle
- Erstellen von Regeln für die Kontrolle des Programmstarts
- Benutzerdefinierte Aufgaben zur Untersuchung auf Befehl
- Überwachung der Datei-Integrität
- Protokollanalyse
- Datenbanken-Update und Update der Programm-Module für Kaspersky Embedded Systems Security
- Quarantäne
- Backup
- Berichte
- Benachrichtigungen an den Administrator und die Benutzer
- Vertrauenswürdige Zone
- Exploit-Prävention
- Kennwortschutz

Ferner können Sie die allgemeinen Einstellungen von Kaspersky Embedded Systems Security und die Berechtigungen des Benutzerkontos in der Datei speichern.

Die Einstellungen von Gruppenaufgaben können nicht exportiert werden.

Kaspersky Embedded Systems Security exportiert alle Kennwörter, die vom Programm verwendet werden, beispielsweise die Anmeldeeinstellungen von Konten für den Start von Aufgaben oder für die Verbindungsaufnahme mit Proxyservern. Exportierte Kennwörter werden in der Konfigurationsdatei verschlüsselt gespeichert. Sie können Kennwörter mithilfe von Kaspersky Embedded Systems Security nur dann importieren, wenn dieses Programm auf demselben geschützten Gerät installiert ist und weder neu installiert noch aktualisiert wurde.

Sie können keine gespeicherten Kennwörter mithilfe von Kaspersky Embedded Systems Security importieren, wenn das Programm auf einem anderen geschützten Gerät installiert ist. Nach dem Import von Einstellungen auf ein anderes geschütztes Gerät müssen alle Kennwörter manuell angegeben werden.

Wenn zum Zeitpunkt des Exports von Einstellungen eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert das Programm die aus der Richtlinie übernommenen Werte.

Einstellungen aus einer Konfigurationsdatei, die nur Einstellungen für bestimmte Komponenten von Kaspersky Embedded Systems Security enthält (z. B. aus einer Datei, die in Kaspersky Embedded Systems Security erstellt wurde, als nicht alle Komponenten installiert waren), können importiert werden. Nach dem Import der Einstellungen werden in Kaspersky Embedded Systems Security nur jene Einstellungen geändert, die in der Konfigurationsdatei vorhanden waren. Alle anderen Einstellungen bleiben unverändert.

Gesperrte Einstellungen der aktiven Richtlinie von Kaspersky Security Center werden beim Import von Einstellungen nicht verändert.

Einstellungen exportieren

So exportieren Sie Einstellungen in eine Konfigurationsdatei:

1. Führen Sie in der Struktur der Programmkonsole eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** die Option **Einstellungen exportieren**, um alle Einstellungen von Kaspersky Embedded Systems Security zu exportieren.
   - Wählen Sie im Kontextmenü des Namens der Aufgabe den Punkt **Einstellungen exportieren** aus, um die Einstellungen einer einzelnen Komponente des Programms zu exportieren.
   - Zum Exportieren der Einstellungen der vertrauenswürdigen Zone gehen Sie wie folgt vor:

     a. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.

     b. Wählen Sie den Punkt **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

     Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

     c. Klicken Sie auf die Schaltfläche **Export**.

     Der Assistent für den Export von Einstellungen wird geöffnet.

2. Folgen Sie den Anweisungen in den Fenstern des **Export-Assistent für Programmeinstellungen**: Geben Sie den Namen und Pfad für die Konfigurationsdatei an, in der die Einstellungen gespeichert werden sollen.

   Sie können Umgebungsvariablen des Systems verwenden, wenn Sie den Pfad angeben, jedoch keine benutzerdefinierten Umgebungsvariablen.

   Wenn zum Zeitpunkt des Exports von Einstellungen eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert Kaspersky Embedded Systems Security die Einstellungen aus der Richtlinie.

3. Klicken Sie im Fenster **Export der Programmeinstellungen abgeschlossen** auf die Schaltfläche **Schließen**.

Der Assistent für den Export von Einstellungen wird geschlossen und speichert die Exporteinstellungen.

Einstellungen importieren

So importieren Sie Einstellungen aus einer gespeicherten Konfigurationsdatei:

1. Führen Sie in der Struktur der Programmkonsole eine der folgenden Aktionen aus:

   - Wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** die Option **Einstellungen importieren**, um alle Einstellungen von Kaspersky Embedded Systems Security zu importieren.

   - Wählen Sie im Kontextmenü des Namens der Aufgabe den Punkt **Einstellungen importieren** aus, um die Einstellungen einer einzelnen funktionalen Komponente zu importieren.

   - Zum Importieren der Einstellungen der vertrauenswürdigen Zone gehen Sie wie folgt vor:

     a. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.

     b. Wählen Sie den Punkt **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

     Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

     c. Klicken Sie auf die Schaltfläche **Import**.

     Der Assistent für den Import von Einstellungen wird geöffnet.

2. Folgen Sie den Anweisungen im **Import-Assistent für Programmeinstellungen**: Geben Sie die Konfigurationsdatei mit den Einstellungen, die importiert werden sollen, an.

   Nachdem Sie allgemeine Einstellungen für Kaspersky Embedded Systems Security oder dessen funktionale Komponenten auf dem geschützten Gerät importiert haben, können Sie die vorherigen Einstellungen nicht wiederherstellen.

3. Klicken Sie im Fenster **Import der Programmeinstellungen abgeschlossen** auf die Schaltfläche **Schließen**.

   Der Assistent für den Import von Einstellungen wird geschlossen und speichert die importierten Einstellungen.

4. Klicken Sie in der Symbolleiste der Programmkonsole auf die Schaltfläche **Aktualisieren**.

Das Fenster der Programmkonsole zeigt die importierten Einstellungen an.

Kaspersky Embedded Systems Security importiert keine Kennwörter (Konto-Anmeldedaten für den Aufgabenstart oder für die Proxyserver-Verbindung) aus einer Datei, die auf einem anderen geschützten Gerät angelegt oder auf dem gleichen geschützten Gerät gespeichert wurde, nachdem Kaspersky Embedded Systems Security auf diesem neu installiert oder aktualisiert wurde. Die Kennwörter müssen nach dem Abschluss des Imports manuell eingegeben werden.

Verwendung von Vorlagen für Sicherheitseinstellungen

Dieser Abschnitt enthält Informationen über die Arbeit mit Vorlagen für Sicherheitseinstellungen in den Schutz- und Untersuchungsaufgaben von Kaspersky Embedded Systems Security.

Über Vorlagen für Sicherheitseinstellungen

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

Sie können Vorlagen für die Angabe der Sicherheitseinstellungen für die folgenden Aufgaben von Kaspersky Embedded Systems Security verwenden:

- Echtzeitschutz für Dateien
- Untersuchung beim Hochfahren des Betriebssystems
- Untersuchung wichtiger Bereiche
- Benutzerdefinierte Aufgaben zur Untersuchung auf Befehl

Die Sicherheitseinstellungen aus einer Vorlage, die für einen übergeordneten Knoten in der Struktur der Dateiressourcen des geschützten Geräts übernommen wird, werden für alle untergeordneten Knoten übernommen. In folgenden Fällen wird die Vorlage des übergeordneten Knotens nicht für die untergeordneten Knoten übernommen:

- Wenn Sie die Sicherheitseinstellungen der untergeordneten Knoten gesondert angegeben haben.
- Wenn es sich bei den untergeordneten Knoten um virtuelle Knoten handelt. In diesem Fall müssen Sie die Vorlage für jeden virtuellen Knoten gesondert anwenden.

Vorlage für Sicherheitseinstellungen erstellen

Gehen Sie wie folgt vor, um die Sicherheitseinstellungen des Knotens manuell in einer Vorlage zu speichern:

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, für deren Sicherheitseinstellungen Sie eine Vorlage erstellen möchten.
2. Klicken Sie im Ergebnisbereich der ausgewählten Aufgabe auf den Link **Schutzbereich anpassen** oder **Untersuchungsbereich anpassen**.
3. Wählen Sie in der Struktur bzw. Liste der freigegebenen Netzwerkordner des geschützten Geräts die Vorlage, die Sie anzeigen möchten.
4. Klicken Sie auf der Registerkarte **Sicherheitsstufe** auf die Schaltfläche **Als Vorlage speichern**.

   Das Fenster **Eigenschaften der Vorlage** wird geöffnet.
5. Geben Sie im Feld **Vorlagenname** den Namen der Vorlage ein.
6. Geben Sie im Feld **Beschreibung** zusätzliche Informationen zu der Vorlage ein.
7. Klicken Sie auf **OK**.

Die Vorlage für Sicherheitseinstellungen wird gespeichert.

Sicherheitseinstellungen in einer Vorlage aufrufen

So rufen Sie die Sicherheitseinstellungen in einer von Ihnen erstellten Vorlage auf:

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe mit der Vorlage für Sicherheitseinstellungen aus, die angezeigt werden soll.
2. Wählen Sie im Kontextmenü der ausgewählten Aufgabe den Punkt **Vorlagen für Einstellungen** aus.

   Das Fenster **Vorlagen** wird geöffnet.
3. Wählen Sie in der Vorlagenliste die Vorlage aus, die angezeigt werden soll.
4. Klicken Sie auf die Schaltfläche **Anzeigen**.

Das Fenster **<Vorlagenname>** wird geöffnet. Auf der Registerkarte **Allgemein** werden der Vorlagenname und zusätzliche Informationen zur Vorlage angezeigt. Auf der Registerkarte **Einstellungen** werden die in der Vorlage gespeicherten Sicherheitseinstellungen aufgelistet.

Vorlage für Sicherheitseinstellungen anwenden

Gehen Sie wie folgt vor, um die Sicherheitseinstellungen aus der Vorlage auf einen ausgewählten Knoten zu übernehmen:

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, auf die Sie eine Vorlage für Einstellungen der Sicherheit anwenden möchten.
2. Klicken Sie im Ergebnisbereich der ausgewählten Aufgabe auf den Link **Schutzbereich anpassen** oder **Untersuchungsbereich anpassen**.
3. Öffnen Sie in der Struktur oder Liste der freigegebenen Netzwerkordner des geschützten Geräts das Kontextmenü des Knotens bzw. Elements, auf den bzw. dass Sie die Vorlage anwenden möchten.
4. Wählen Sie **Vorlage übernehmen → <Name der Vorlage>** aus.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Dadurch wird die Vorlage für Sicherheitseinstellungen auf den ausgewählten Knoten in der Struktur der Dateiressourcen des geschützten Geräts angewendet. Der Wert auf der Registerkarte **Sicherheitsstufe** für den ausgewählten Knoten ändert sich in **Benutzerdefiniert**.

Wenn die Sicherheitseinstellungen einer Vorlage für einen übergeordneten Knoten in der Struktur der Dateiressourcen des geschützten Geräts übernommen werden, dann werden diese Einstellungen auch für alle untergeordneten Knoten übernommen.

Sie können den Schutz- oder Untersuchungsbereich von untergeordneten Knoten in der Struktur der Dateiressourcen des geschützten Geräts separat konfigurieren. In diesem Fall werden die Sicherheitseinstellungen der Vorlage, die auf den übergeordneten Knoten angewendet wird, nicht automatisch auf die untergeordneten Knoten angewendet.

So übernehmen Sie die Sicherheitseinstellungen aus der Vorlage für alle ausgewählten Knoten:

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe aus, deren Vorlage für Einstellungen der Sicherheit Sie übernehmen möchten.

2. Klicken Sie im Ergebnisbereich der ausgewählten Aufgabe auf den Link **Schutzbereich anpassen** oder **Untersuchungsbereich anpassen**.

3. Wählen Sie in der Struktur oder Liste der freigegebenen Netzwerkordner des geschützten Geräts den übergeordneten Knoten aus, um die Vorlage für diesen Knoten und alle untergeordneten Knoten zu übernehmen.

4. Wählen Sie im Kontextmenü **Vorlage übernehmen** → **<Name der Vorlage>** aus.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Vorlage für Sicherheitseinstellungen wird für den übergeordneten und alle untergeordneten Knoten in der Struktur der Dateiressourcen des geschützten Geräts übernommen. Der Wert auf der Registerkarte **Sicherheitsstufe** für den ausgewählten Knoten ändert sich in **Benutzerdefiniert**.

Vorlage für Sicherheitseinstellungen löschen

Vorlage für Sicherheitseinstellungen löschen:

1. Wählen Sie in der Struktur der Programmkonsole die Aufgabe mit der Vorlage für Sicherheitseinstellungen aus, die Sie löschen möchten.

2. Wählen Sie im Kontextmenü der ausgewählten Aufgabe den Punkt **Vorlagen für Einstellungen** aus.

   Das Fenster **Vorlagen** wird geöffnet.

   Im Ergebnisfenster des übergeordneten Knotens **Untersuchung auf Befehl** können Sie die Vorlage für Einstellungen für benutzerdefinierte Aufgaben zur Untersuchung auf Befehl anzeigen.

3. Wählen Sie in der Vorlagenliste die zu löschende Vorlage aus.

4. Klicken Sie auf die Schaltfläche **Löschen**.

   Ein Fenster zur Bestätigung des Löschvorgangs wird geöffnet.

5. Klicken Sie im folgenden Fenster auf **Ja**.

Die gewählte Vorlage wird gelöscht.

Sie können die Vorlage für Sicherheitseinstellungen anwenden, um Knoten in der Struktur der Dateiressourcen des geschützten Geräts zu schützen oder zu scannen. In diesem Fall bleiben die Sicherheitseinstellungen für solche Knoten nach dem Löschen der Vorlage unverändert.

Schutzstatus und Informationen zu Kaspersky Embedded Systems Security anzeigen

Um Informationen über den Geräteschutzstatus von Kaspersky Embedded Systems Security anzuzeigen,

wählen Sie in der Programmkonsolenstruktur den Knoten **Kaspersky Embedded Systems Security** aus.

Standardmäßig werden die Informationen im Ergebnisbereich der Programmkonsole automatisch aktualisiert:

- alle 10 Sekunden bei lokaler Verbindung
- alle 15 Sekunden bei Remote-Verbindung

Sie können die Informationen auch manuell aktualisieren.

*Und die Informationen im Knoten **Kaspersky Embedded Systems Security** manuell zu aktualisieren,*

wählen Sie im Kontextmenü des Knotens **Kaspersky Embedded Systems Security** den Befehl **Aktualisieren**.

Im Ergebnisbereich der Programmkonsole werden die folgenden Programminformationen angezeigt:

- Status der Verwendung von Kaspersky Security Network.
- Schutzstatus des geschützten Geräts.
- Daten über das Datenbanken-Update und das Update der Programm-Module.
- Aktuelle Diagnoseinformationen.
- Daten zu den Steuerungsaufgaben des geschützten Geräts.
- Lizenzinformationen.
- Status der Integration in Kaspersky Security Center: Details des Servers, auf dem Kaspersky Security Center installiert und mit dem das Programm verknüpft ist; Daten über die Kontrolle der Programmaufgaben durch die aktive Richtlinie.

Für die Darstellung des Schutzstatus werden verschiedene Farben verwendet:

- *Grün*. Aufgabe wird gemäß den vorgenommenen Einstellungen ausgeführt. Der Schutz ist aktiv.
- *Gelb*. Aufgabe ist angehalten, beendet oder nicht gestartet. Es besteht ein potentielles Sicherheitsrisiko. Die Aufgabe sollte konfiguriert und gestartet werden.
- *Rot*. Aufgabe ist fehlgeschlagen oder bei der Aufgabenausführung wurde eine Sicherheitsbedrohung erkannt. Es empfiehlt sich, die Aufgabe zu starten oder Maßnahmen zur Beseitigung der erkannten Sicherheitsbedrohung zu ergreifen.

Ein Teil der Informationen in diesem Block (beispielsweise Aufgabennamen oder Anzahl erkannter Bedrohungen) wird in Form von Links dargestellt, über die Sie zum Knoten der entsprechenden Aufgabe wechseln oder das Protokoll der Aufgabenausführung öffnen können.

Der Abschnitt **Verwendung von Kaspersky Security Network** zeigt den aktuellen Status der Aufgabe, z. B. *Läuft*, *Beendet* oder *Noch nicht ausgeführt*. Der Indikator kann folgende Werte annehmen:

- Die Farbe Grün gibt an, dass die Aufgabe zur Verwendung von KSN ausgeführt wird und dass Anfragen zum Status von URLs an KSN gesendet werden.
- Die Farbe Gelb gibt an, dass eine der Erklärungen akzeptiert wurde, die Aufgabe aber nicht ausgeführt wird oder dass die Aufgabe ausgeführt wird, aber keine Dateianfragen an KSN gesendet werden.

Computerschutz

Im Abschnitt **Computerschutz** (siehe Tabelle unten) werden Informationen über den aktuellen Schutzstatus des Geräts angezeigt.

Informationen über den Schutzstatus des Geräts

Abschnitt "Schutz"	Informationen
Statusanzeige für den Geräteschutz	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der im Abschnitt ausführbaren Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Standard-Darstellung, die anzeigt, dass die Komponente „Echtzeitschutz für Dateien“ installiert ist und die Aufgabe ausgeführt wird. • Gelb – die Komponente „Echtzeitschutz für Dateien“ wurde nicht installiert und die Aufgabe zur Untersuchung wichtiger Bereiche wurde seit langer Zeit nicht ausgeführt. • Rot – die Aufgabe zum Echtzeitschutz für Dateien wird nicht ausgeführt.
Echtzeitschutz für Dateien	**Aufgabenstatus** – aktueller Status der Aufgabe, z. B. *Läuft* oder *Beendet*. **Gefunden** – Anzahl der Objekte, die von Kaspersky Embedded Systems Security gefunden wurden. Findet Kaspersky Embedded Systems Security beispielsweise in fünf Dateien ein und dasselbe schädliche Programm, dann wird der Wert in diesem Feld um den Wert eins erhöht. Ist die Anzahl der gefundenen schädliche Programme größer als 0, so wird der Wert rot dargestellt.
Untersuchung wichtiger Bereiche	**Letzte Untersuchung am** – Datum und Uhrzeit der letzten Untersuchung wichtiger Bereiche des Computers auf Viren und andere Bedrohungen der Computersicherheit. *Noch nicht ausgeführt* – Ereignis, das auftritt, wenn die Aufgabe zur Untersuchung wichtiger Bereiche seit mindestens 30 Tagen nicht mehr ausgeführt wurde (Standard). Sie können den Grenzwert für die Auslösung dieses Ereignisses ändern.
Exploit-Prävention	**Status** – aktueller Status der Verfahren zur Exploit-Prävention, beispielsweise *Übernommen* oder *Nicht übernommen*. **Präventionsmodus** – einer von zwei verfügbaren Modi, der bei der Konfiguration des Schutzes des Prozess-Speichers ausgewählt wurde: **Bei Exploit beenden** oder **Nur Statistik**. **Geschützte Prozesse** – Gesamtanzahl der Prozesse, die zum Schutzbereich hinzugefügt wurden und gemäß dem gewählten Modus verarbeitet werden.
Objekte im Backup	*Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* – Ereignis, das auftritt, wenn sich der verfügbare Speicherplatz im Backup dem festgelegten Grenzwert nähert. Kaspersky Embedded Systems Security verschiebt Objekte weiterhin ins Backup. In diesem Fall wird der Wert im Feld **Belegter Speicherplatz** gelb dargestellt. *Maximale Größe des Backups wurde überschritten* – Ereignis, das auftritt, wenn die Größe des Backups den festgelegten Grenzwert erreicht. Kaspersky Embedded Systems Security verschiebt Objekte weiterhin ins Backup. In diesem Fall wird der Wert im Feld **Belegter Speicherplatz** rot dargestellt. **Objekte im Backup** – Anzahl der Objekte, die sich momentan im Backup befinden. **Belegter Speicherplatz** – Volumen des verwendeten Speicherplatzes im Backup.

Update

Im Abschnitt **Update** (siehe Tabelle unten) werden Informationen über die Aktualität der Antiviren-Datenbanken und Programm-Module angezeigt.

Informationen über den Zustand der Datenbanken und Module von Kaspersky Embedded Systems Security

Abschnitt "Update"	Informationen
Statusindikator für Datenbanken und Programm-Module	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der Programm-Datenbanken und Programm-Module. Der Indikator kann folgende Werte annehmen: • Grün – Standarddarstellung, die anzeigt, dass die Programm-Datenbanken aktuell sind und dass das letzte Update der Programm-Datenbanken erfolgreich abgeschlossen wurde. • Gelb – die Datenbanken sind veraltet, oder die letzte Aufgabe zum Datenbanken-Update ist fehlgeschlagen. • Rot – das Ereignis *Programm-Datenbanken sind stark veraltet* oder *Programm-Datenbanken sind beschädigt* ist eingetreten.
Update der Programm-Datenbanken und **Update der Programm-Module**	**Status der Programm-Datenbanken** – Bewertung des Status des Updates der Programm-Datenbanken. Die Einstellung kann folgende Werte annehmen: • **Programm-Datenbanken sind aktuell** – die Programm-Datenbanken wurden vor höchstens 7 Tagen aktualisiert (Standard). • **Programm-Datenbanken sind veraltet** – die Programm-Datenbanken wurden zuletzt vor 7–14 Tagen aktualisiert (Standard). • **Programm-Datenbanken sind stark veraltet** – die Programm-Datenbanken wurden zuletzt vor mehr als 14 Tagen aktualisiert (Standard). Sie können die Grenzwerte für die Auslösung der Ereignisse *Programm-Datenbanken sind aktuell* und *Programm-Datenbanken sind stark veraltet* ändern. **Veröffentlichungsdatum der Programm-Datenbanken** – Datum und Uhrzeit der Veröffentlichung des aktuellen Updates der Programm-Datenbanken. Datum und Uhrzeit werden in UTC angegeben. **Status der letzten gestarteten Aufgabe zum Update der Programm-Datenbanken** – Datum und Uhrzeit des letzten Datenbanken-Updates. Datum und Uhrzeit werden in der lokalen Zeit des geschützten Geräts angegeben. Das Feld ist rot, wenn das Ereignis *Fehlgeschlagen* eingetreten ist. **Verfügbare Updates der Programm-Module** – Anzahl der zum Download und zur Installation verfügbaren Updates für die Module von Kaspersky Embedded Systems Security. **Installierte Updates der Programm-Module** – Anzahl der installierten Updates für Module von Kaspersky Embedded Systems Security.

Kontrollkomponenten

Im Abschnitt **Kontrollkomponenten** (siehe Tabelle unten) werden Informationen über den Status der Aufgaben "Kontrolle des Programmstarts", "Gerätekontrolle" und "Firewall-Verwaltung" angezeigt.

Informationen über den Status der Gerätekontrolle

Abschnitt	Informationen

Kontrollkomponenten	
Statusindikator der Kontrolle geschützter Geräte	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der im Abschnitt ausführbaren Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Standarddarstellung, die anzeigt, dass die Komponente "Kontrolle des Programmstarts" installiert wurde und die Aufgabe im Modus **Aktiv** ausgeführt wird. • Gelb – Die Kontrolle des Programmstarts wird im Modus **Nur Statistik** ausgeführt. • Rot – Die Aufgabe zur Kontrolle des Programmstarts wird nicht ausgeführt oder ist fehlgeschlagen.
Kontrolle des Programmstarts	**Aufgabenstatus** – aktueller Status der Aufgabe, z. B. *Läuft* oder *Beendet*. **Ausführungsmodus** – einer der zwei verfügbaren Modi für die Aufgabe zur Kontrolle des Programmstarts: **Aktiv** oder **Nur Statistik**. **Blockierte Programmstarts** – Anzahl der versuchten Programmstarts, die durch Kaspersky Embedded Systems Security während der Ausführung der Aufgabe zur Kontrolle des Programmstarts blockiert wurden. Ist die Anzahl der blockierten Versuche des Programmstarts größer als 0, so ist das Feld rot. **Durchschnittl. Bearbeitungsdauer (ms)** – Zeit, die Kaspersky Embedded Systems Security für die Verarbeitung eines versuchten Programmstarts auf dem geschützten Gerät benötigte.
Gerätekontrolle	**Aufgabenstatus** – aktueller Status der Aufgabe, z. B. *Läuft* oder *Beendet*. **Ausführungsmodus** – einer der zwei verfügbaren Modi für die Aufgabe zur Gerätekontrolle: **Aktiv** oder **Nur Statistik**. **Blockierte Geräte** – Anzahl der Verbindungsversuche eines externen Geräts, die von Kaspersky Embedded Systems Security während der Aufgabe zur Gerätekontrolle blockiert wurden. Ist die Anzahl der blockierten externen Geräte größer als 0, ist der Feldwert rot.
Firewall-Verwaltung	**Aufgabenstatus** – aktueller Status der Aufgabe, z. B. *Läuft* oder *Beendet*. **Blockierte Verbindungsversuche** – Anzahl der Verbindungen mit dem geschützten Gerät, die gemäß den festgelegten Firewall-Regeln nicht erlaubt wurden.

Diagnose

Im Abschnitt **Diagnose** (s. Tabelle unten) werden Informationen über den Status der Aufgaben "Überwachung der Datei-Integrität" und "Protokollanalyse" angezeigt.

Informationen über den Status der System-Diagnose

Abschnitt "Diagnose"	Informationen
Statusindikator der Diagnose	Die Farbe der Leiste mit dem Namen des Abschnitts gibt Aufschluss über den Status der im Abschnitt ausführbaren Aufgaben. Der Indikator kann folgende Werte annehmen: • Grün – Standarddarstellung, die anzeigt, dass eine oder beide Komponenten der System-Diagnose installiert sind und dass Aufgaben ausgeführt werden.

	• Gelb – beide Komponenten sind installiert, aber eine der Aufgaben zur System-Diagnose läuft nicht; das Ereignis *Nicht gestartet* ist eingetreten. • Rot – eine der Aufgaben ist fehlgeschlagen.
Überwachung der Datei-Integrität	**Aufgabenstatus** – aktueller Status der Aufgabe, z. B. *Läuft* oder *Beendet*. **Verbotene Dateioperationen** – Anzahl der Veränderungen an Dateien, die sich im Überwachungsbereich befinden. Diese Änderungen deuten eventuell auf eine Verletzung der Sicherheit auf dem geschützten Gerät hin.
Protokollanalyse	**Aufgabenstatus** – aktueller Status der Aufgabe, z. B. *Läuft* oder *Beendet*. **Verstöße gegen die konfigurierten Regeln**– Anzahl der registrierten Verstöße laut Angaben des Windows-Ereignisprotokolls. Diese Zahl wird auf Grundlage der festgelegten Aufgabenregeln oder mithilfe der heuristischen Analyse ermittelt.

Informationen zur Lizenzverwaltung von Kaspersky Embedded Systems Security werden in der Zeile in der linken unteren Ecke des Detailbereichs des Knotens **Kaspersky Embedded Systems Security** angezeigt.

Sie können die Einstellungen von Kaspersky Embedded Systems Security anpassen, indem Sie auf den Link **Eigenschaften des Programms** klicken.

Sie können eine Verbindung zu einem anderem geschützten Gerät herstellen, indem Sie auf den Link **Verbindung mit anderem Computer herstellen** klicken.

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

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

Kaspersky Embedded Systems Security über die Web Console und Cloud Console verwalten

Über das Web-Plug-in für Kaspersky Security für Windows Server können Sie mehrere geschützte Geräte zentral verwalten, auf denen Kaspersky Security für Windows Server installiert und die in einer Administrationsgruppe enthalten ist. Kaspersky Security Center Web Console und Kaspersky Security Center Cloud Console ermöglichen außerdem die separate Konfiguration jedes geschützten Geräts in den Administrationsgruppen.

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

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

Sie können Kaspersky Embedded Systems Security auf folgende Arten über die Kaspersky Security Center Web Console verwalten:

- **Mithilfe der Richtlinien von Kaspersky Security Center**. Die Richtlinien von Kaspersky Security Center ermöglichen es, einheitliche Schutzeinstellungen für Gerätegruppen per Fernzugriff zu konfigurieren. Die in der aktiven Richtlinie festgelegten Aufgabeneinstellungen haben Priorität vor den Aufgabeneinstellungen, die lokal in der Programmkonsole oder per Remote-Zugriff im Fenster mit den Eigenschaften des Geräts in der Web-Konsole für Kaspersky Security Center konfiguriert wurden. Mithilfe von Richtlinien können Sie allgemeine Programmeinstellungen, Einstellungen für Aufgaben zum Echtzeit-Computerschutz, Einstellungen für Aufgaben zur Überwachung der Desktop-Aktivitäten und Einstellungen zum Start von lokalen Systemaufgaben nach Zeitplan anpassen.

- **Mit Hilfe der Gruppenaufgaben von Kaspersky Security Center**. Die Gruppenaufgaben von Kaspersky Security Center ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit einer begrenzten Ausführungsdauer für Gerätegruppen per Fernzugriff. Mithilfe von Gruppenaufgaben können Sie das Programm aktivieren sowie die Einstellungen der Aufgaben zur Untersuchung auf Befehl, der Update-Aufgaben und der Aufgaben zum Erstellen von Regeln für die Kontrolle des Programmstarts konfigurieren.

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

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

Die Web-Konsole für Kaspersky Security Center und die Cloud-Konsole für Kaspersky Security Center erlaubt Ihnen die Anpassung der Programmeinstellungen und erweiterten Optionen, sowie die Arbeit mit Protokollen und Benachrichtigungen. Sie können diese Einstellungen sowohl für Gruppen von geschützten Geräten als auch für ein einzelnes geschütztes Gerät anpassen.

Einschränkungen für Web Plug-in

Das Web-Plug-in für Kaspersky Embedded Systems Security hat folgende Einschränkungen im Vergleich zum Verwaltungs-Plug-in für Kaspersky Embedded Systems Security:

- Um Benutzer oder Gruppen hinzuzufügen, müssen Sie die Zeichenfolge des Sicherheitsdescriptors mithilfe der Security Descriptor Definition Language (SDDL) angeben.
- Vordefinierte Sicherheitsstufen können nicht für die Aufgabe "Echtzeitschutz für Dateien" geändert werden.
- Die Regeln für die Aufgabe "Kontrolle des Programmstarts" können nicht mit digitalen Zertifikaten oder Kaspersky Security Center-Ereignissen erstellt werden.
- Die Regeln für die Gerätekontrollaufgabe können nicht anhand von verbundenen Geräten oder Systemdaten generiert werden.

Programmeinstellungen verwalten

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

Allgemeine Programmeinstellungen im Web-Plug-in konfigurieren

Sie können die allgemeinen Einstellungen von Kaspersky Embedded Systems Security im Web-Plug-in für Gruppen von geschützten Geräten und für ein einzelnes geschütztes Gerät konfigurieren.

Skalierbarkeit und Schnittstelle und Untersuchungseinstellungen im Web-Plug-in anpassen

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

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Skalierbarkeit, Oberfläche und Untersuchungseinstellungen** auf **Einstellungen**.

6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Skalierbarkeitseinstellungen

Einstellung	Beschreibung
Skalierbarkeitseinstellungen automatisch ermitteln	Die Zahl der verwendeten Prozesse wird von Kaspersky Embedded Systems Security automatisch geregelt. Dieser Wert gilt als Standard.
Anzahl der Arbeitsprozesse manuell angeben	Die Zahl der aktiven Arbeitsprozesse wird von Kaspersky Embedded Systems Security gemäß den angegebenen Werten gesteuert.
Maximale Anzahl aktiver Prozesse	Die maximale Anzahl der von Kaspersky Embedded Systems Security verwendeten Prozesse. Das Eingabefeld ist verfügbar, wenn die Variante **Anzahl der Arbeitsprozesse manuell angeben** ausgewählt wurde.
Anzahl der Prozesse für den Echtzeitschutz	Maximale Anzahl der Prozesse, die von den Komponenten der Aufgaben zum Echtzeit-Computerschutz 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.
Symbol im Infobereich der Taskleiste anzeigen	Anzeige des Taskleistensymbols im Infobereich anpassen.
Dateiattribute nach der Untersuchung wiederherstellen	Wenn Kaspersky Embedded Systems Security die Aufgabe zur Untersuchung auf Befehl ausführt, wird für jede untersuchte Datei der Zeitpunkt des letzten Zugriffs aktualisiert. Nach Abschluss der Untersuchung setzt Kaspersky Embedded Systems Security für die Datei den Zeitpunkt des letzten Zugriffs auf den ursprünglichen Wert zurück. Dieses Verhalten kann die Arbeit von Backup-Systemen beeinflussen, indem Backup-Kopien von Dateien erzeugt werden, die nicht geändert wurden. Dies kann außerdem bei Anwendungen, die Dateiänderungen überwachen, zu Fehlalarmen führen. Diese Einstellung ist standardmäßig aktiviert.
CPU-Auslastung für die Untersuchung auf Bedrohungen begrenzen	Während auf einem geschützten Gerät eine Untersuchung auf Befehl durchgeführt wird, begrenzt Kaspersky Embedded Systems Security die CPU-Nutzung auf dem Gerät mit dem im Feld **Obergrenze (Prozent)** angegeben Wert. Das Aktivieren dieser Einstellung kann sich negativ auf die Leistung von Kaspersky Embedded Systems Security auswirken. Diese Einstellung ist standardmäßig deaktiviert.
Obergrenze (in Prozent)	Der maximal zulässige Wert für die CPU-Ausnutzung von Kaspersky Embedded Systems Security. Dieses Eingabefeld ist verfügbar, wenn die Option **CPU-Auslastung für die Untersuchung auf Bedrohungen begrenzen** gewählt ist.
Ordner für während der Untersuchung erstellte temporäre Dateien	Ein Ordner, der von Kaspersky Embedded Systems Security während der Untersuchung zum Entpacken von Archivdateien benötigt wird.

	Standardmäßig wird der Ordner C:\Windows\Temp verwendet.
Einstellungen des HSM-Systems	Wählen Sie die Option zum Zugriff auf den hierarchischen Speicher aus.

Anpassen der Sicherheitseinstellungen im Web-Plug-in

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

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Sicherheit und Zuverlässigkeit** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Parameter für Sicherheit

Einstellung	Beschreibung
Programmprozesse vor externen Bedrohungen schützen	Wenn das Kontrollkästchen **Programmprozesse vor externen Bedrohungen schützen** aktiviert ist, schützt das Programm seine Prozesse vor Code-Injektion oder dem Zugriff auf Prozessdaten. Wenn Sie die Einstellung aktivieren oder deaktivieren, müssen Sie die Programmdienste nicht neu starten, damit die Änderungen wirksam werden. Diese Option ist standardmäßig aktiviert.
Wiederherstellen von Aufgaben ausführen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Wiederherstellung der Aufgaben von Kaspersky Embedded Systems Security nach einer Störung bzw. einer fehlerhaften Beendigung des Programms. Ist das Kontrollkästchen aktiviert, stellt Kaspersky Embedded Systems Security die Aufgaben von Kaspersky Embedded Systems Security nach einer Störung oder einer fehlerhaften Beendigung automatisch wieder her. Ist das Kontrollkästchen deaktiviert, stellt Kaspersky Embedded Systems Security die Aufgaben von Kaspersky Embedded Systems Security nach einer Störung oder einer fehlerhaften Beendigung nicht wieder her. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Maximale Anzahl der Versuche, um die Aufgaben zur Untersuchung auf Befehl wiederherzustellen: 1–10	Die Anzahl versuchter Wiederherstellungen der Aufgaben zur Untersuchung auf Befehl nach einer Störung von Kaspersky Embedded Systems Security. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Wiederherstellen von Aufgaben ausführen** aktiviert ist.
Aufgaben zur Untersuchung nach Zeitplan nicht starten	Dieses Kontrollkästchen aktiviert/deaktiviert beim Wechsel des geschützten Geräts auf eine USV-Quelle das Starten der Aufgaben zur Untersuchung nach Zeitplan bis zur Wiederherstellung der Standardstromversorgung.

	Ist dieses Kontrollkästchen aktiviert, startet Kaspersky Embedded Systems Security beim Wechsel des geschützten Geräts auf eine USV-Quelle bis zur Wiederherstellung der Standardstromversorgung keine Aufgaben zur Untersuchung nach Zeitplan. Ist das Kontrollkästchen deaktiviert, startet Kaspersky Embedded Systems Security die Aufgaben zur Untersuchung nach Zeitplan unabhängig von der Stromversorgung. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Laufende Untersuchungsaufgaben anhalten	Dieses Kontrollkästchen aktiviert oder deaktiviert die Ausführung der gestarteten Untersuchungsaufgaben beim Wechsel des geschützten Geräts auf eine USV-Quelle. Ist dieses Kontrollkästchen aktiviert, hält Kaspersky Embedded Systems Security beim Wechsel des geschützten Geräts auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben an. Ist dieses Kontrollkästchen deaktiviert, setzt Kaspersky Embedded Systems Security beim Wechsel des geschützten Geräts auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben fort. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Kennwortschutz verwenden	Legen Sie ein Kennwort für den Schutz des Zugriffs auf die Funktionen von Kaspersky Embedded Systems Security fest.

Anpassen der Verbindungseinstellungen im Web-Plug-in

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

Zum Einrichten der Verbindungseinstellungen gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Skalierbarkeit, Oberfläche und Untersuchungseinstellungen** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Verbindungseinstellungen

Einstellung	Beschreibung
Keinen Proxyserver verwenden	Ist diese Einstellung ausgewählt, verwendet Kaspersky Embedded Systems Security keinen Proxyserver zur Verbindungsaufnahme mit den KSN-Diensten, sondern stellt die Verbindung direkt her.
Einstellungen des angegebenen Proxyservers verwenden	Ist diese Einstellung ausgewählt, verwendet Kaspersky Embedded Systems Security für die Verbindungsaufnahme mit KSN die manuell eingegebenen Proxyserver-Einstellungen.

Für lokale Adressen keinen Proxyserver verwenden	Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Nutzung eines Proxyservers für Anfragen an Geräte aus dem Netzwerk, zu dem auch das geschützte Gerät gehört, auf dem Kaspersky Embedded Systems Security installiert ist. Ist das Kontrollkästchen aktiviert, wird aus dem Netzwerk, zu dem das geschützte Gerät mit installiertem Kaspersky Embedded Systems Security gehört, direkt auf Geräte zugegriffen. Es wird kein Proxyserver verwendet. Wenn das Kontrollkästchen deaktiviert ist, wird für den Zugriff auf die lokalen Geräte ein Proxyserver verwendet. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Einstellungen für die Authentifizierung auf dem Proxyserver	Legen Sie die Authentifizierungseinstellungen fest.
Keine Authentifizierung verwenden	Es erfolgt keine Authentifizierung. Dieser Modus gilt als Standard.
NTLM-Authentifizierung verwenden	Die Authentifizierung erfolgt mithilfe des von Microsoft entwickelten NTLM-Protokolls zur Netzwerkauthentifizierung.
NTLM-Authentifizierung mit Benutzername und Kennwort verwenden	Die Authentifizierung erfolgt mithilfe des Benutzernamens und Kennworts über das von Microsoft entwickelte NTLM-Protokoll zur Netzwerkauthentifizierung.
Benutzername und Kennwort verwenden	Die Authentifizierung erfolgt mithilfe des Benutzernamens und Kennworts.

Zeitplan für den Start von lokalen Systemaufgaben anpassen

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

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

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

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

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

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

Mithilfe von Richtlinien können Sie den Start folgender lokaler Systemaufgaben nach Zeitplan erlauben oder verbieten:

- Aufgaben zur Untersuchung auf Befehl: Untersuchung wichtiger Bereiche, Untersuchung von Quarantäne-Objekten, Untersuchung beim Hochfahren des Betriebssystems, Integritätsprüfung für Programme, Überwachung der Baseline-Integrität.
- Aufgaben zum Update: Update der Programm-Datenbanken, Update der Programm-Module, Update-Verteilung.

Wenn Sie ein geschütztes Gerät aus der Administrationsgruppe ausschließen, wird der Zeitplan der lokalen Systemaufgaben automatisch aktiviert.

So erlauben oder verbieten Sie den Start der lokalen Systemaufgaben von Kaspersky Embedded Systems Security nach Zeitplan in einer Richtlinie:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Unterabschnitt **Start von lokalen Systemaufgaben** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen für Start von lokalen Systemaufgaben nach Zeitplan

Einstellung	Beschreibung
Start von Aufgaben zur Untersuchung auf Befehl zulassen	Aktivieren oder deaktivieren Sie das Kontrollkästchen, um den geplanten Start von Aufgaben zur Untersuchung auf Befehl zu erlauben oder zu verbieten.
Start von Aufgaben zum Update und zur Update-Verteilung zulassen	Aktivieren oder deaktivieren Sie das Kontrollkästchen, um den Start von Update-Aufgaben und der Aufgabe zur Update-Verteilung nach Zeitplan zu erlauben oder zu verbieten.

Quarantäne- und Backup-Einstellungen im Web-Plug-in konfigurieren

Allgemeine Quarantäne- und Backup-Einstellungen in Kaspersky Security Center konfigurieren:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.

4. Wählen Sie den Abschnitt **Zusätzlich**.

5. Klicken Sie im Unterabschnitt **Speicher** auf **Einstellungen**.

6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen für Quarantäne und Backup

Einstellung	Beschreibung
Backup-Ordner	Angabe des Backup-Ordners.
Maximale Größe des Backups (MB)	Angabe der maximalen Größe des Backups.
Grenzwert für verfügbaren Speicherplatz (MB)	Angabe des Mindestwerts für den freien Speicher im Backup-Ordner.
Ordner für die Wiederherstellung von Objekten	Angabe eines Ordners für wiederhergestellte Objekte.
Quarantäneordner	Angabe des Backup-Ordners.
Maximale Größe der Quarantäne (MB)	Angabe der maximalen Größe des Backups.
Grenzwert für verfügbaren Speicherplatz (MB)	Angabe des Mindestwerts für den freien Speicher im Backup-Ordner.
Ordner für die Wiederherstellung von Objekten	Angabe eines Ordners für wiederhergestellte Objekte.
Zeitraum für die Blockierung von Hosts	Geben die Anzahl der Tage, Stunden und Minuten an, nach deren Ablauf die blockierten Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt bietet Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Embedded Systems Security auf mehreren geschützten Geräten.

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

Eine Richtlinie übernimmt die in Kaspersky Embedded Systems Security angegebenen Einstellungen, Funktionen und Aufgaben auf allen geschützten Geräten einer Administrationsgruppe.

Sie können mehrere Richtlinien für eine Administrationsgruppe erstellen und sie temporär übernehmen. Die in der Gruppe aktuell gültige Richtlinie hat in der Verwaltungskonsole den Status *aktiv*.

Informationen über den Geltungsbereich einer Richtlinie werden im Systemaudit-Protokoll von Kaspersky Embedded Systems Security protokolliert. Diese Informationen stehen in der Programmkonsole unter dem Knoten **Systemaudit-Protokoll** zur Verfügung.

In Kaspersky Security Center existiert eine einzige Methode zur Übernahme von Richtlinien auf geschützten Geräten: *Änderung von Einstellungen verbieten*. Nachdem eine Richtlinie angewendet wurde, verwendet Kaspersky Embedded Systems Security die Einstellungen, für welche Sie das Zeichen in den Richtlinieneigenschaften auf geschützten Geräten ausgewählt haben. In diesem Fall werden die ausgewählten Einstellungen verwendet anstatt der Einstellungen, die vor dem Anwenden der Richtlinie wirksam waren. Einstellungen der aktiven Richtlinie, für die in den Richtlinieneigenschaften das Zeichen gesetzt ist, werden von Kaspersky Embedded Systems Security nicht übernommen.

Ist eine Richtlinie aktiv, so werden die Werte der Einstellungen, die in der Richtlinie mit dem Symbol markiert sind, in der Programmkonsole angezeigt, können jedoch nicht bearbeitet werden. Die Werte der restlichen Einstellungen (die in der Richtlinie mit dem Symbol markiert sind) können in der Programmkonsole bearbeitet werden.

Die in der aktiven Richtlinie festgelegten und mit dem Symbol markierten Einstellungen blockieren auch die Bearbeitung der Einstellungen in Kaspersky Security Center für ein einzelnes geschütztes Gerät im Fenster **Eigenschaften: <Name des geschützten Geräts>**.

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

Wenn die Richtlinie Einstellungen für eine der Aufgaben zum Echtzeit-Computerschutz definiert und diese Aufgabe derzeit ausgeführt wird, 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

So erstellen Sie eine Richtlinie:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Das Fenster **Neue Richtlinie** wird geöffnet.
4. Wählen Sie im Abschnitt **Programm auswählen** "Kaspersky Embedded Systems Security" aus klicken Sie auf **Weiter**.
5. Auf der Registerkarte **Allgemein** können Sie die folgenden Aktionen vornehmen:
   - Ändern des Richtliniennamens

     Die Namen von Richtlinien dürfen keines der folgenden Symbole enthalten: `" * < : > ? \ | .`
   - Auswählen des Richtlinienstatus:
     - **Aktiv**. Nach der nächsten Synchronisierung wird die Richtlinie auf dem Computer als aktive Richtlinie verwendet.
     - **Inaktiv**. Backup-Richtlinie. Eine inaktive Richtlinie kann bei Bedarf aktiviert werden.

- **Abwesenheit**. Die Richtlinie wird aktiviert, wenn sich ein Computer außerhalb des Unternehmensnetzwerks befindet.

- Konfigurieren der Vererbbarkeit von Einstellungen:

  - **Einstellungen der übergeordneten Richtlinie erben**. Wenn diese Umschaltfläche aktiviert ist, erbt eine Richtlinie die Werte der Einstellungen der ihr übergeordneten Richtlinie. Richtlinieneinstellungen werden nicht vererbt, wenn die übergeordnete Richtlinie mit dem markiert ist.

  - **Vererbung von Einstellungen für untergeordnete Richtlinien erzwingen**. Wenn diese Umschaltfläche aktiviert ist, werden die Werte der Einstellungen der Richtlinie an die ihr untergeordneten Richtlinien weitergegeben. In den Einstellungen der untergeordneten Richtlinie ist dann automatisch das Kontrollkästchen **Einstellungen der übergeordneten Richtlinie erben** aktiviert. Untergeordnete Richtlinien erben die Einstellungen der ihnen übergeordneten Richtlinien, es sei denn, die Einstellungen sind mit dem Symbol markiert. Die Einstellungen von untergeordneten Richtlinien können nicht bearbeitet werden, wenn die übergeordnete Richtlinie mit dem Symbol markiert ist.

6. Konfigurieren Sie die Einstellungen nach Bedarf auf der Registerkarte **Programmeinstellungen**.

7. Klicken Sie auf **Speichern**.

Die erstellte Richtlinie wird in der Richtlinienliste auf der Registerkarte **Richtlinien und Profile** der ausgewählten Administrationsgruppe angezeigt. Im Fenster **<Name der Richtlinie>** können Sie andere Einstellungen, Aufgaben und Funktionen von Kaspersky Embedded Systems Security anpassen.

Abschnitte mit Richtlinieneinstellungen für Kaspersky Embedded Systems Security

Allgemein

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

- Richtlinienstatus festlegen.

- Vererbungseinstellungen von übergeordneten und untergeordneten Richtlinien konfigurieren.

Konfiguration von Ereignissen

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

- *Kritische Ereignisse*

- *Funktionsfehler*

- *Warnung*

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

- Geben Sie den Speicherort und die Speicherdauer für Informationen über protokollierte Ereignisse an.

- Geben Sie für protokollierte Ereignisse die Methode für die Benachrichtigung an.

Programmeinstellungen

Einstellungen des Abschnitts "Programmeinstellungen"

Abschnitt	Einstellungen
Skalierbarkeit, Oberfläche und Untersuchungseinstellungen	Im Unterabschnitt **Skalierbarkeit, Oberfläche und Untersuchungseinstellungen** 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 und Zuverlässigkeit	Im Unterabschnitt **Sicherheit und Zuverlässigkeit** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Einstellungen der Aufgabenausführung anpassen. • Aktionen des Programms beim Wechsel des geschützten Geräts in den USV-Akkubetrieb angeben. • Kennwortschutz der Programmfunktionen aktivieren und deaktivieren.
Verbindungen	Im Unterabschnitt **Verbindungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Proxyserver-Einstellungen für die Verbindung mit den Update-Servern, den Aktivierungsservern und KSN konfigurieren: • Festlegung der Proxyserver-Einstellungen. • Geben Sie die Einstellungen für die Authentifizierung auf dem Proxyserver an.
Start von lokalen Systemaufgaben	Im Unterabschnitt **Start von lokalen Systemaufgaben** können Sie über die Schaltfläche **Einstellungen** den Start der folgenden lokalen Systemaufgaben nach einem auf den geschützten Geräten festgelegten Zeitplan erlauben oder verbieten: • Aufgabe zur Untersuchung auf Befehl • Update-Aufgaben und Aufgabe zur Update-Verteilung

Zusätzlich

Einstellungen des Abschnitts "Zusätzlich"

Abschnitt	Einstellungen
Vertrauenswürdige Zone	Im Unterabschnitt **Vertrauenswürdige Zone** können Sie über die Schaltfläche **Einstellungen** die folgenden Parameter für die Verwendung der vertrauenswürdigen Zone konfigurieren: • Erstellung einer Liste der Ausnahmen von der vertrauenswürdigen Zone. • Aktivieren oder deaktivieren der Untersuchung von Backup-Operationen. • Erstellen Sie eine Liste der vertrauenswürdigen Prozesse.

Untersuchung von Wechseldatenträgern	Im Unterabschnitt **Untersuchung von Wechseldatenträgern** können Sie über die Schaltfläche **Einstellungen** die Untersuchungseinstellungen für Wechseldatenträger anpassen.
Benutzerrechte für die Programmverwaltung	Im Unterabschnitt **Benutzerrechte für die Programmverwaltung** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Embedded Systems Security anpassen.
Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service	Im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Security Service anpassen.
Speicher	Im Unterabschnitt **Speicher** können Sie über die Schaltfläche **Einstellungen** folgende Einstellungen für Quarantäne, Backup und blockierte Hosts anpassen: • Angabe des Ordnerpfads, in dem Sie die Quarantäne- oder Backup-Objekte ablegen möchten. • Anpassung der maximalen Größe des Backups und der Quarantäne sowie Festlegung des Grenzwerts für verfügbaren Speicherplatz • Angabe des Ordnerpfads, in dem Sie die wiederhergestellten Quarantäne- oder Backup-Objekte ablegen möchten. • Anpassen der Übermittlung von Informationen über im Backup und in der Quarantäne gespeicherte Objekte an den Administrationsserver • Passen Sie an, wie lange Hosts blockiert werden.

Echtzeitschutz für Computer

Einstellungen des Abschnitts "Echtzeitschutz für Server"

Abschnitt	Einstellungen
Echtzeitschutz für Dateien	Im Unterabschnitt **Echtzeitschutz für Dateien** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Schutzmodus angeben. • Verwendung der heuristischen Analyse anpassen. • Verwendung der vertrauenswürdigen Zone anpassen. • Schutzbereich angeben. • Sicherheitsstufe für den ausgewählten Schutzbereich festlegen: Sie können die vorinstallierte Sicherheitsstufe auswählen oder die Sicherheitseinstellungen manuell anpassen. • Einstellungen für den Aufgabenstart festlegen.
Verwendung von KSN	Im Unterabschnitt **Verwendung von KSN** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Aktionen für Objekte, die in KSN nicht vertrauenswürdig sind, angeben.

	• Datentransfer und Verwendung von Kaspersky Security Center als KSN Proxyserver konfigurieren.
Exploit-Prävention	Im Unterabschnitt **Exploit-Prävention** können Sie über die Schaltfläche **Einstellungen** die folgenden Parameter für die Aufgabenausführung konfigurieren: • Wählen Sie den Schutzmodus des Prozess-Arbeitsspeichers aus. • Geben Sie die Aktionen zur Verringerung des Exploit-Risikos an. • Ergänzen und bearbeiten Sie die Liste der geschützten Prozesse.

Überwachung der Desktop-Aktivitäten

Einstellungen des Abschnitts "Überwachung der Desktop-Aktivitäten"

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

Überwachung der Netzwerkaktivität

Einstellungen des Abschnitts "Netzwerküberwachung"

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

System-Diagnose

Einstellungen des Abschnitts "System-Diagnose"

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

Protokolle und Benachrichtigungen

Einstellungen des Abschnitts "Protokolle und Benachrichtigungen"

Abschnitt	Einstellungen
Protokolle der Aufgabenausführung	Im Unterabschnitt **Protokolle der Aufgabenausführung** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Prioritätsstufe protokollierter Ereignisse für die ausgewählten Programmkomponenten angeben. • Speicherdauer für Protokolle der Aufgabenausführung festlegen. • Konfiguration der SIEM-Integration in Kaspersky Security Center.
Ereignisbenachrichtigungen	Im Unterabschnitt **Ereignisbenachrichtigungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Legen Sie Einstellungen für die Benutzerbenachrichtigung für die Ereignisse *Objekt gefunden*, *Nicht vertrauenswürdiger Massenspeicher gefunden und eingeschränkt* und *Host als nicht vertrauenswürdig gelistet* fest. • Benachrichtigung des Administrators über ein beliebiges ausgewähltes Ereignis aus der Liste der Ereignisse im Abschnitt **Benachrichtigungen anpassen**.
Interaktion mit Administrationsserver	Im Unterabschnitt **Interaktion mit Administrationsserver** können Sie über die Schaltfläche **Einstellungen** die Typen der Objekte auswählen, über die Kaspersky Embedded Systems Security Informationen an den Administrationsserver übergeben soll.

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.

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Embedded Systems Security, ihre Erstellung, die Konfiguration ihrer Ausführung sowie über den Start/die Beendigung von Aufgaben.

Zur Erstellung von Aufgaben im Web-Plug-in

Sie können Gruppenaufgaben für Administrationsgruppen und für Zusammenstellungen von geschützten Geräten erstellen. Folgende Typen von Aufgaben können erstellt werden:

- Programm aktivieren
- Update-Verteilung
- Update der Programm-Datenbanken
- Update der Programm-Module
- Rollback des Datenbanken-Updates
- Untersuchung auf Befehl
- Integritätsprüfung für Programme
- Überwachung der Baseline-Integrität
- Erstellen von Regeln für die Kontrolle des Programmstarts
- Erstellen von Regeln für die Gerätekontrolle

Sie können lokale Aufgaben und Gruppenaufgaben auf folgende Art und Weise erstellen:

- Für ein geschütztes Gerät: Im Fenster **Eigenschaften: <Name des geschützten Geräts>** im Abschnitt **Aufgaben**.
- Für eine Administrationsgruppe: Im Ergebnisbereich des Knotens der ausgewählten Gruppe von geschützten Geräten auf der Registerkarte **Aufgaben**.
- Für eine Auswahl an geschützten Geräten: Im Ergebnisbereich des Knotens **Geräteauswahl**.

Mithilfe von Richtlinien können Sie Zeitpläne für lokale Systemaufgaben zum Update und zur Untersuchung auf Befehl auf allen geschützten Geräten in derselben Administrationsgruppe deaktivieren.

Allgemeine Informationen über den Aufgaben in Kaspersky Security Center sind im *Hilfesystem von Kaspersky Security Center* zu finden.

Eine Aufgabe im Web-Plug-in erstellen

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. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Verwaltete Geräte** aus.

b. Klicken Sie auf die Registerkarte **Gruppen**, um die Administrationsgruppe auszuwählen, zu der das geschützte Gerät gehört.

c. Klicken Sie auf den Namen des geschützten Geräts.

d. Wählen Sie im nächsten Fenster **<Name des Geräts>** den Abschnitt **Aufgaben** aus.

e. Klicken Sie auf **Hinzufügen**.

- Für das Erstellen einer Gruppenaufgabe:

  a. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Verwaltete Geräte** aus.

  b. Klicken Sie auf die Registerkarte **Gruppen**, um die Administrationsgruppe auszuwählen, für die Sie eine Aufgabe erstellen möchten.

  c. Klicken Sie auf **Hinzufügen**.

- Um eine Aufgabe für eine benutzerdefinierte Auswahl von geschützten Geräten zu erstellen, gehen Sie wie folgt vor:

  a. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Geräteauswahl** aus.

  b. Wählen Sie aus, wofür Sie eine Aufgabe erstellen möchten.

  c. Klicken Sie auf **Start**.

  d. Wählen Sie im Fenster **Auswahlergebnisse** die Geräte aus, für die Sie eine Aufgabe erstellen möchten.

  e. Klicken Sie auf **Neue Aufgabe**.

Darauf öffnet sich der Assistent für neue Aufgaben.

2. Wählen Sie in der Dropdown-Liste **Programm** die Option **Kaspersky Embedded Systems Security** aus.

3. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Typ der Aufgabe aus, die Sie erstellen möchten.

   Wenn Sie einen anderen Aufgabentyp als Rollback des Datenbanken-Updates, Integritätsprüfung für Programme oder Programmaktivierung ausgewählt haben, wird das Fenster "Einstellungen" geöffnet.

4. Je nach Typ der gewählten Aufgabe führen Sie eine der folgenden Aktionen aus:

   - Aufgabe zur Untersuchung auf Befehl erstellen.

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

     a. Wählen Sie im Abschnitt **Quelle für das Update der Programm-Datenbanken** eine Update-Quelle aus.

     b. Konfigurieren Sie im Fenster **Verbindungseinstellungen** die Proxyserver-Einstellungen.

   - Nachdem Sie eine Aufgabe zum Update der Programm-Module erstellt haben, passen Sie im Fenster **Update der Programm-Module** 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 geschützten Geräts erforderlich sein. Damit Kaspersky Embedded Systems Security das geschützte Gerät nach Abschluss der Aufgabe automatisch neu startet, aktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**.

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

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

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

a. Geben Sie im Fenster **Liste von Schlüsseln im Speicher von Kaspersky Security Center** die Schlüsseldatei an, die Sie zur Aktivierung des Programms verwenden möchten.

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

- Erstellen und konfigurieren Sie die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts".
- Erstellen und konfigurieren Sie die Aufgabe "Erstellen von Regeln für die Gerätekontrolle".

5. Klicken Sie auf **Weiter**.
6. Wenn die Aufgabe für eine Zusammenstellung von geschützten Geräten erstellt wird, wählen Sie das Netzwerk (oder die Gruppe) der geschützten Geräte aus, an denen die Aufgabe ausgeführt werden soll.
7. Klicken Sie auf **Weiter**.
8. Aktivieren Sie im Fenster **Erstellung der Aufgabe fertig stellen** das Kontrollkästchen **Aufgabendetails öffnen, wenn Erstellung abgeschlossen ist**, wenn Sie die Aufgabeneinstellungen konfigurieren möchten.
9. Klicken Sie auf **Fertig**.

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

Gruppenaufgaben im Web-Plug-in anpassen

Gehen Sie wie folgt vor, um eine Gruppenaufgabe für mehrere geschützte Geräte zu konfigurieren:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.
2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

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

3. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eines der Folgenden aus:

   - Wenn Sie eine Aufgabe zur Untersuchung auf Befehl konfigurieren:

     a. Legen Sie im Abschnitt **Untersuchungsbereich** einen Untersuchungsbereich fest.

     b. Konfigurieren Sie im Abschnitt **Einstellungen** die Integration in andere Programmkomponenten sowie die Aufgabenpriorität.

   - Um eine Update-Aufgabe zu konfigurieren, passen Sie die gewünschten Aufgabenparameter Ihren Bedürfnissen an:

     a. Passen Sie im Abschnitt **Update-Quellen** die Einstellungen für die Update-Quelle und die Proxyserver-Einstellungen an.

     b. Konfigurieren Sie im Abschnitt **Optimierung** die Optimierung des Festplattensubsystems.

   - Wenn Sie die Aufgabe "Update der Programm-Module" anpassen möchten, wählen Sie im Abschnitt **Erweiterte Einstellungen** 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 namens "Programm aktivieren" konfigurieren möchten, verwenden Sie die Schlüsseldatei, mit deren Hilfe Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie einen Aktivierungscode oder eine Schlüsseldatei zur Verlängerung der Lizenz hinzufügen möchten.

   - Um die automatische Generation von Erlaubnisregeln für die Gerätekontrolle zu konfigurieren, geben Sie die Einstellungen ein, die verwendet werden, um die Liste der Erlaubnisregeln zu erstellen.

4. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).

5. Geben Sie auf der Registerkarte **Einstellungen** im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

6. Klicken Sie auf **Speichern**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Aufgabe zum Aktivieren des Programms im Web-Plug-in anpassen

So konfigurieren Sie eine Aufgabe zur Aktivierung des Programms:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.

2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

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

3. Geben Sie im Abschnitt **Allgemein** die Schlüsseldatei an, mit der Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.

4. Passen Sie den Aufgabenzeitplan im Abschnitt **Zeitplan** an.

5. Klicken Sie im Fenster **<Aufgabenname>** auf **OK**.

Updateaufgaben im Web-Plug-in anpassen

So konfigurieren Sie die Aufgaben "Update-Verteilung", "Update der Programm-Datenbanken" oder "Update der Programm-Module":

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.

2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

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

3. Passen Sie im Abschnitt **Update-Quellen** die Einstellungen für die Update-Quelle an:

   - Geben Sie im Abschnitt **Quelle für das Update der Programm-Datenbanken** den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Update-Server als Update-Quelle für die Programmaktualisierung an. Sie können auch eine benutzerdefinierte Liste mit Update-Quellen erstellen, indem Sie andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen.

     Sie können die Verwendung der Kaspersky-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

     > Um einen freigegebenen SMB-Ordner als Update-Quelle zu verwenden, müssen Sie ein Benutzerkonto für den Aufgabenstart festlegen.

     > Wenn Sie eine Update-Aufgabe über die Cloud Console konfigurieren, stehen Ihnen nur die Optionen **Verteilungspunkte** und **Kaspersky-Update-Server** als Update-Quellen zur Verfügung.

   - Stellen Sie im Abschnitt **Verbindungseinstellungen** die Verwendung von Proxy-Servern für das Verbinden mit Kaspersky-Update-Servern und anderen Servern ein.

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

   - **Optimierung der Nutzung des Festplatten-Subsystems**
   - **Für die Optimierung genutztes Arbeitsspeichervolumen (400 - 9999 MB)**

5. 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).

6. Klicken Sie im Fenster **<Aufgabenname>** auf **OK**.

Einstellungen für die Fehlerdiagnose im Web-Plug-in anpassen

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

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

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsberechtigungen konfigurieren und nur bestimmten Benutzern den Zugriff auf Protokolle, Trace- und Dump-Dateien erlauben.

Um die Einstellungen für die Fehlerdiagnose in Kaspersky Security Center anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center das Fenster **Programmeinstellungen**.
2. Öffnen Sie den Abschnitt **Crash-Diagnose** und gehen Sie wie folgt vor:
   - Wenn Sie Debug-Informationen in eine Datei schreiben möchten, aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern**.
     - Geben Sie im Feld unten den Ordner an, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.
     - Passen Sie die Genauigkeitsstufe für die Debug-Informationen an.
     - Geben Sie die maximale Größe der Protokolldateien an.
     - Geben Sie die maximale Größe der Dateien für ein Protokoll an.

       Kaspersky Embedded Systems Security erstellt für jede zu debuggende Komponente so viele Protokolldateien, bis die maximale Anzahl erreicht ist.

     - 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).

Subsystemcodes in Kaspersky Embedded Systems Security

Code des Subsystems	Name des Subsystems
*	Alle Komponenten.
gui	Subsystem der Benutzeroberfläche, Snap-In von Kaspersky Embedded Systems Security in der Microsoft Management Console.
ak_conn	Subsystem zur Integration des Administrationsagenten von Kaspersky Security Center.

bl	Steuerungsprozess, implementiert Steuerungsaufgaben von Kaspersky Embedded Systems Security
wp	Arbeitsprozess, der die Aufgaben zum Antiviren-Schutz realisiert
blgate	Prozess zur Fernverwaltung von Kaspersky Embedded Systems Security
ods	Subsystem für Untersuchung auf Befehl
oas	Subsystem für den Echtzeitschutz für Dateien
qb	Subsystem für Quarantäne und Backup-Speicher
scandll	Hilfsmodul für die Untersuchung auf Viren.
core	Subsystem für die Antiviren-Basisfunktionalität
avscan	Subsystem für die Antiviren-Bearbeitung
avserv	Subsystem zur Steuerung des Antiviren-Kerns
prague	Subsystem für die Basisfunktionalität
updater	Subsystem für das Datenbanken-Update und das Update der Programm-Module
snmp	Subsystem für Unterstützung des SNMP-Berichts
perfcount	Subsystem für Leistungsindikatoren

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

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

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

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

3. Klicken Sie auf **OK**.

Die festgelegten Programmeinstellungen werden auf dem geschützten Gerät übernommen.

Arbeit mit dem Aufgabenzeitplan

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

Aufgaben planen

In der Programmkonsole können Sie lokale Systemaufgaben und benutzerdefinierte Aufgaben planen. Gruppenaufgaben können nicht über die Programmkonsole geplant werden.

So planen Sie Gruppenaufgaben mithilfe des Web-Plug-ins:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.
2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.
   Das Fenster **<Aufgabenname>** wird geöffnet.
3. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
4. Aktivieren Sie im Abschnitt **Zeitplan** das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.

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

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

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

   - **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 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.

6. Im Abschnitt **Einstellungen für das Anhalten der Aufgabe**:

   a. Aktivieren Sie das Kontrollkästchen **Dauer** und geben Sie in den Feldern auf der rechten Seite die maximale Anzahl der Stunden und Minuten für die Ausführung der Aufgabe ein.

   b. Aktivieren Sie das Kontrollkästchen **Aufgabe anhalten** und geben Sie in den Feldern auf der rechten Seite den Start- und Endwert eines Zeitintervalls für 24 Stunden ein, in dem die Ausführung der Aufgabe angehalten wird.

7. Im Abschnitt **Erweiterte Zeitplan-Einstellungen**:

a. Aktivieren Sie das Kontrollkästchen **Zeitplan deaktivieren** 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 **Startzeit der Aufgabe in diesem Intervall zufällig verteilen** und geben Sie einen Wert in Minuten ein.

8. Klicken Sie auf die Schaltfläche **Speichern**, 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 den Zeitplan für den Aufgabenstart zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.
2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.
   Das Fenster **<Aufgabenname>** wird geöffnet.
3. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Zeitplan** aus.
5. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**, wenn Sie den Aufgabenstart nach Zeitplan aktivieren möchten
   - Deaktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**, 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.

6. Klicken Sie auf **Speichern**.

Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden gespeichert.

Berichte in Kaspersky Security Center

Die Berichte von Kaspersky Security Center enthalten Informationen zum Status der verwalteten Geräte. Die Berichte basieren auf Informationen, die auf dem Administrationsserver gespeichert sind.

Ab Kaspersky Security Center 11 sind folgende Berichtstypen für Kaspersky Embedded Systems Security verfügbar:

- Bericht über den Status der Programmkomponenten
- Bericht über verbotene Programme
- Bericht über verbotene Programme im Testmodus

Detaillierte Informationen zu allen Berichten in Kaspersky Security Center und deren Konfiguration finden Sie in der *Hilfe zu Kaspersky Security Center*.

Bericht über den Status der Programmkomponenten von Kaspersky Embedded Systems Security

Sie können den Schutzstatus aller Netzwerkgeräte überwachen und eine strukturierte Übersicht der Komponentenauswahl auf jedem Gerät anzeigen lassen.

Der Bericht zeigt für jede Komponente eine der folgenden Statusvarianten an: *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, wird in der Web-Konsole von Kaspersky Security Center der Status "N/A" (Nicht verfügbar) zugewiesen.

Sie können eine Komponentenauswahl erstellen und den Filter verwenden, um Netzwerkgeräte mit einer festgelegten Auswahl an Komponenten samt Status anzuzeigen.

Nähere Informationen zur Erstellung und Verwendung einer Auswahl finden Sie in der *Hilfe zu Kaspersky Security Center*.

Um den aktuellen Status der Komponenten in den Programmeinstellungen zu überprüfen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Verwaltete Geräte** aus.
2. Klicken Sie auf den Namen des geschützten Geräts.
3. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Komponenten** aus.
4. Eine Tabelle mit Statusvarianten wird Ihnen angezeigt.

   Informationen über den Status der Komponente Exploit-Prävention sind in dieser Tabelle nicht verfügbar.

Um einen Standardbericht für die Web-Konsole von Kaspersky Security Center anzusehen, gehen Sie wie folgt vor:

1. Wählen Sie **Überwachung und Berichterstellung** → **Berichte** aus.
2. Wählen Sie das Listenelement **Bericht über den Status der Programmkomponenten** aus und klicken Sie auf die Schaltfläche **Bericht anzeigen**.

   Ein Bericht wird erstellt.
3. Sehen Sie sich die folgenden Berichtsdetails an:

- ein Schaubild
- eine Übersichtstabelle mit Komponenten und der Gesamtanzahl der Netzwerkgeräte, auf denen jede Komponente installiert ist, sowie die Gruppen, zu denen sie gehören
- eine detaillierte Tabelle mit dem Status, der Version, dem Gerät und der Gruppe der Komponente

Berichte über verbotene Programme im Modus "Aktiv" und "Statistik"

Basierend auf den Ergebnissen der Aufgabe zur Kontrolle des Programmstarts können zwei Arten von Berichten erstellt werden: ein Bericht über verbotene Programme (wenn die Aufgabe im 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 Geräten im Netzwerk. Jeder Bericht wird für alle Administrationsgruppen erstellt und sammelt die Daten aller Kaspersky-Programme, die auf den geschützten Geräten installiert sind.

Um einen Bericht über verbotene Programme im Modus "Nur Statistik" anzuzeigen, gehen Sie wie folgt vor:

1. Starten Sie die Aufgabe zur Kontrolle des Programmstarts im Modus Nur Statistik.
2. Wählen Sie **Überwachung und Berichterstellung** → **Berichte** aus.
3. Wählen Sie das Listenelement **Bericht über verbotene Programme im Testmodus** aus und klicken Sie auf die Schaltfläche **Bericht anzeigen**.

   Ein Bericht wird erstellt.
4. Sehen Sie sich die folgenden Berichtsdetails an:
   - Ein Schaubild mit den Top-10-Programmen, deren Start am häufigsten blockiert wurde.
   - Eine Übersichtstabelle mit den Fällen, in denen ein Programm blockiert wurde, mit Angabe des Namens der ausführbaren Datei, der Ursache, der Uhrzeit der Blockierung und der Anzahl der Geräte, auf denen sie stattgefunden hat.
   - Eine ausführliche Tabelle welche die Daten zum Gerät, dem Dateipfad und die Kriterien für das Blockieren angibt.

Um einen Bericht über verbotene Programme im Modus "Aktiv" anzuzeigen, gehen Sie wie folgt vor:

1. Starten Sie die Aufgabe zur Kontrolle des Programmstarts im Modus "Aktiv".
2. Wählen Sie **Überwachung und Berichterstellung** → **Berichte** aus.
3. Wählen Sie das Listenelement **Bericht über verbotene Programme im Testmodus** aus und klicken Sie auf die Schaltfläche **Bericht anzeigen**.

   Ein Bericht wird erstellt.

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

Kompaktes Diagnosefenster

In diesem Abschnitt wird beschrieben, wie Sie das kompakte Diagnosefenster zur Überprüfung des Status des geschützten Geräts oder der aktuellen Aktivität nutzen und das Erstellen von Dump-Dateien und Protokolldateien anpassen.

Über das kompakte Diagnosefenster

Die Komponente "Kompaktes Diagnosefenster" ("Compact Diagnostic Interface", im Weiteren auch "CDI") wird gemeinsam mit der Komponente "Taskleistensymbol" unabhängig von der Programmkonsole installiert und deinstalliert und kann verwendet werden, wenn die Programmkonsole nicht auf dem geschützten Gerät installiert ist. Das CDI wird aus dem über das Taskleistensymbol oder durch Ausführung von kavfsmui.exe aus dem Programmordner auf dem geschützten Gerät gestartet.

Im CDI-Fenster können Sie folgenden Aktionen ausführen:

- Informationen über den allgemeinen Programmstatus überprüfen.
- Eingetretene Sicherheitsereignisse überprüfen.
- Aktuelle Aktivitäten auf dem geschützten Gerät überprüfen.
- Das Erstellen von Dump-Dateien und Protokolldateien starten und stoppen.
- Öffnen Sie die Programmkonsole.
- Das Fenster **Über das Programm** mit der Liste der installierten Updates und verfügbaren Patches öffnen.

Das CDI ist auch verfügbar, wenn der Zugriff auf Kaspersky Embedded Systems Security kennwortgeschützt ist. Es ist kein Kennwort erforderlich.

Die CDI-Komponente kann nicht über Kaspersky Security Center angepasst werden.

Status von Kaspersky Embedded Systems Security mithilfe des kompakten Diagnosefensters überprüfen

Um das kompakte Diagnosefenster zu öffnen, führen Sie die folgenden Schritte aus:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompaktes Diagnosefenster öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.

Überprüfen Sie den aktuellen Status des Schlüssels sowie der Aufgaben zum Echtzeit-Computerschutz und Update auf der Registerkarte **Schutzstatus**. Verschiedene Farben vermitteln dem Benutzer den aktuellen Schutzstatus (s. Tabelle unten).

Schutzstatus des kompakten Diagnosefensters

Abschnitt	Status
Status des Echtzeitschutzes	Die Leiste ist *grün* bei einem der folgenden Szenarien (wenn eine der Bedingungen erfüllt ist): • Empfohlene Konfiguration: • Die Aufgabe zum Echtzeitschutz für Dateien wurde mit den Standardeinstellungen gestartet. • Die Aufgabe zur Kontrolle des Programmstarts wurde im Modus **Aktiv** mit den Standardeinstellungen gestartet. • Annehmbare Konfiguration: • Die Aufgabe zum Echtzeitschutz für Dateien wurde vom Benutzer angepasst. • Die Einstellungen der Aufgabe zur Kontrolle des Programmstarts wurden geändert.
	Die Leiste ist *gelb*, wenn eine oder mehrere der folgenden Bedingungen zutreffen: • Die Aufgabe zum Echtzeitschutz für Dateien wurde angehalten (durch Benutzer oder Zeitplan). • Die Aufgabe zur Kontrolle des Programmstarts wurde im Modus **Nur Statistik** gestartet. • Die Exploit-Prävention und die Kontrolle des Programmstarts wurden im Modus **Nur Statistik** gestartet.
	Die Leiste ist *rot*, wenn beide der folgenden Bedingungen zutreffen: • Die Komponente "Echtzeitschutz für Dateien" ist nicht installiert oder die Aufgabe wurde beendet oder angehalten. • Die Komponente "Kontrolle des Programmstarts" ist nicht installiert oder die Aufgabe wurde im Modus **Nur Statistik** gestartet.
Lizenzverwaltung	Die Leiste ist *grün*, wenn die aktuelle Lizenz gültig ist.
	Die Leiste ist *gelb*, wenn eines der folgenden Ereignisse eingetreten ist: • *Untersuchung des Lizenzstatus läuft*. • *Die Restlaufzeit der Lizenz beträgt noch 14 Tage, und es wurde kein Reserveschlüssel oder Aktivierungscode hinzugefügt.* • *Der hinzugefügte Schlüssel wurde in die Deny-Liste aufgenommen und seine Blockierung steht unmittelbar bevor.*
	Die Leiste ist *rot*, wenn eines der folgenden Ereignisse eingetreten ist: • *Das Programm wurde nicht aktiviert* • *Die Lizenz ist abgelaufen!* • *Verstoß gegen den Endbenutzer-Lizenzvertrag*

	• *Der Schlüssel befindet sich auf der Deny-Liste*
Update	Die Leiste ist *grün*, wenn die Programm-Datenbanken aktuell sind.
	Die Leiste ist *gelb*, wenn die Programm-Datenbanken veraltet sind.
	Die Leiste ist *rot*, wenn die Programm-Datenbanken stark veraltet sind.

Überprüfung der Sicherheitsereignis-Statistik

Auf der Registerkarte **Statistik** werden alle Sicherheitsereignisse angezeigt. Jede Schutzaufgaben-Statistik wird in einem separaten Block angezeigt, in dem die Anzahl der Vorfälle sowie Datum und Uhrzeit des letzten Vorfalls angegeben sind. Wenn ein Ereignis registriert wird, wechselt die Blockfarbe zu rot.

Um eine Statistik zu überprüfen:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompaktes Diagnosefenster öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.
3. Öffnen Sie die Registerkarte **Statistik**.
4. Überprüfen Sie die Sicherheitsvorfälle für die Schutzaufgaben.

Aktuelle Programmaktivität überprüfen

Auf dieser Registerkarte können Sie den Status der aktuellen Aufgaben und Programmprozesse überprüfen und erhalten sofort Benachrichtigungen über kritische Ereignisse, wenn sie auftreten.

Für die Darstellung der Programmaktivität werden verschiedene Farben verwendet:

- Im Abschnitt **Aufgaben**:
  - *Grün*. Es gibt keine Bedingungen, die Gelb oder Rot erfordern würden.
  - *Gelb*. Untersuchung wichtiger Bereiche liegt lange zurück.
  - *Rot*. Mindestens eine der folgenden Bedingungen trifft zu:
    - Es wurden keine Aufgaben gestartet und der Zeitplan für den Aufgabenstart wurde für keine Aufgabe konfiguriert.
    - Fehler beim Programmstart werden als kritische Ereignisse protokolliert.
- Im Abschnitt **Kaspersky Security Network**:
  - *Grün*. Die Aufgabe "Verwendung von KSN" wurde gestartet.
  - *Gelb*. Die KSN-Erklärung wurde akzeptiert, aber die Aufgabe wurde nicht gestartet.

Um die aktuelle Programmaktivität auf dem geschützten Gerät zu überprüfen, gehen Sie wie folgt vor:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.
2. Wählen Sie die Option **Kompaktes Diagnosefenster öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.
3. Öffnen Sie die Registerkarte **Aktuelle Programmaktivität**.
4. Überprüfen Sie die folgenden Informationen im Abschnitt **Aufgaben**:
   - **Kritische Bereiche wurden lange Zeit nicht untersucht**

     Dieses Feld wird nur angezeigt, wenn das Programm die entsprechenden Warnungen über die Untersuchung wichtiger Bereiche zurückgibt.
   - **Jetzt ausgeführt**
   - **Ausführung fehlgeschlagen**
   - **Nächster Start durch Zeitplan definiert**
5. Überprüfen Sie die folgenden Informationen im Abschnitt **Kaspersky Security Network**:
   - **KSN ist an. Datei-Reputationsdienste sind aktiviert** oder **Schutz ist deaktiviert**.
   - **KSN ist an. Datei-Reputationsdienste sind aktiviert, Die Programmstatistik wird an KSN gesendet**.

     Das Programm sendet während der Ausführung der Aufgaben zum Echtzeitschutz für Dateien und zur Untersuchung auf Befehl Informationen über Funde von Schadsoftware einschließlich Betrugssoftware sowie Debug-Informationen über Störungen während der Untersuchung.

     Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Statistiken an Kaspersky Security Network senden** in den Aufgabeneinstellungen für die Verwendung von KSN aktiviert ist.
6. Überprüfen Sie die folgenden Informationen im Abschnitt **Integration in Kaspersky Security Center**:
   - **Lokale Verwaltung ist erlaubt**.
   - **Eine Richtlinie wurde übernommen: <Name des Administrationsservers>**.

Erstellen von Dump-Dateien und Protokolldateien anpassen

Sie können das Erstellen von Dump-Dateien und Protokolldateien über das CDI anpassen.

Sie können außerdem die Crash-Diagnose über die Programmkonsole einrichten.

Um mit dem Erstellen von Dump-Dateien und Protokolldateien zu beginnen, führen Sie die folgenden Aktionen aus:

1. Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Taskleistensymbol von Kaspersky Embedded Systems Security.

2. Wählen Sie die Option **Kompaktes Diagnosefenster öffnen**.

   Das Fenster **Kompaktes Diagnosefenster** wird angezeigt.

3. Öffnen Sie die Registerkarte **Problembehandlung**.

4. Bei Bedarf können Sie folgende Protokollierungseinstellungen anpassen:

   a. Aktivieren Sie das Kontrollkästchen **Debug-Informationen in Protokolldatei in diesem Ordner speichern**.

   b. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner anzugeben, in dem Kaspersky Embedded Systems Security die Protokolldateien speichern soll.

      Die Ablaufverfolgung wird für alle Komponenten mit den Standardparametern aktiviert. Dabei werden die Genauigkeitsstufe für das *Debuggen* und die maximale Standardprotokollgröße von 50 MB verwendet.

5. Bei Bedarf können Sie folgende Einstellungen für Dump-Dateien anpassen:

   a. Aktivieren Sie das Kontrollkästchen **Bei Absturz Dump-Datei in diesem Ordner erstellen**.

   b. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner anzugeben, in dem Kaspersky Embedded Systems Security die Dump-Datei speichern soll.

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

   Die neue Konfiguration wird übernommen.

Datenbanken und Programm-Module für Kaspersky Embedded Systems Security aktualisieren

Dieser Abschnitt enthält Informationen über die Aufgaben zum Datenbanken-Update und Update der Programm-Module von Kaspersky Embedded Systems Security, über die Update-Verteilung und das Rollback eines Datenbanken-Updates in Kaspersky Embedded Systems Security, sowie Anweisungen zum Anpassen der Aufgabeneinstellungen bei Updates der Datenbank und des Programm-Moduls.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Über Update-Aufgaben

In Kaspersky Embedded Systems Security sind vier Systemaufgaben zum Update vorgesehen: Update der Programm-Datenbanken, Update der Programm-Module, Update-Verteilung und Rollback des Datenbanken-Updates.

Standardmäßig stellt Kaspersky Embedded Systems Security eine Verbindung zur Update-Quelle her (zu einem der Geräte-Updates von Kaspersky). Sie können alle Update-Aufgaben konfigurieren, mit Ausnahme der Aufgabe zum Rollback des Datenbanken-Updates. Nachdem Sie die Aufgabeneinstellungen geändert haben, übernimmt Kaspersky Embedded Systems Security die neuen Werte beim nächsten Aufgabenstart.

Update-Aufgaben können nicht angehalten und wieder fortgesetzt werden.

Update der Programm-Datenbanken

Kaspersky Embedded Systems Security kopiert die Datenbanken standardmäßig aus der Update-Quelle auf das Gerät und verwendet in der laufenden Aufgabe zum Echtzeit-Computerschutz sofort die aktualisierten Datenbanken. Die Aufgaben zur Untersuchung auf Befehl verwenden beim nächsten Aufgabenstart die aktualisierten Programm-Datenbanken.

Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe zum Update der Programm-Datenbanken stündlich.

Update der Programm-Module

Standardmäßig überprüft Kaspersky Embedded Systems Security die Verfügbarkeit von Updates der Programm-Module an der Update-Quelle. Zur Übernahme der installierten Programm-Module müssen Sie das geschützte Gerät und/oder Kaspersky Embedded Systems Security eventuell neu starten.

Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe Update der Programm-Module jeden Freitag um 16:00 Uhr (gemäß den regionalen Zeiteinstellungen des geschützten Geräts). Während der Aufgabenausführung untersucht das Programm, ob wichtige und planmäßige Updates für die Module von Kaspersky Embedded Systems Security vorhanden sind, ohne diese zu kopieren.

Update-Verteilung

Kaspersky Embedded Systems Security lädt die Dateien für das Update der Programm-Datenbanken standardmäßig während der Aufgabenausführung herunter und speichert sie im angegebenen Netzwerkordner oder lokalen Ordner, ohne sie zu installieren.

In der Grundeinstellung wird die Aufgabe Update-Verteilung nicht ausgeführt.

Rollback des Datenbanken-Updates

Kaspersky Embedded Systems Security kehrt während der Ausführung der Aufgabe zu den Datenbanken aus zuvor installierten Updates zurück.

Standardmäßig wird die Aufgabe Rollback des Datenbanken-Updates nicht ausgeführt.

Informationen zum Update der Programm-Module

Kaspersky stellt Updatepakete für die Module von Kaspersky Embedded Systems Security zur Verfügung. Es gibt *wichtige* (oder *kritische*) oder geplante Updates. Wichtige Updatepakete beheben Schwachstellen und Fehler. Geplante Updates fügen neue Funktionen hinzu oder verbessern vorhandene.

Wichtige Updatepakete werden auf den Kaspersky-Update-Servern veröffentlicht. Sie können festlegen, dass sie mit Hilfe der Aufgabe Update der Programm-Module automatisch installiert werden. Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe Update der Programm-Module jeden Freitag um 16:00 Uhr (gemäß den regionalen Zeiteinstellungen des geschützten Geräts).

Geplante Updatepakete werden von Kaspersky nicht auf den Update-Servern veröffentlicht, um sie automatisiert zu installieren. Sie können solche Updatepakete von der Kaspersky-Webseite downloaden. Mit Hilfe der Aufgabe Update der Programm-Module können Sie sich über das Erscheinen von geplanten Updates für Kaspersky Embedded Systems Security informieren.

Sie können dringende Updates entweder auf jedes einzelne geschützte Gerät aus dem Internet abrufen oder ein geschütztes Gerät als Verteiler einrichten. In diesem Fall werden Updates auf den Verteiler heruntergeladen, ohne sie zu installieren, und anschließend an die geschützten Geräte im Netzwerk verteilt. Um Datenbank-Updates zu kopieren und zu speichern, ohne Sie zu installieren, verwenden Sie die Aufgabe Update-Verteilung.

Bevor Updates für die Module installiert werden, kann Kaspersky Embedded Systems Security Backup-Kopien der zuvor installierten Module anlegen. Wenn das Update der Programm-Module unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zu den zuvor installierten Programm-Modulen zurück. Außerdem können Sie manuell ein Rollback des Updates der Module zu den zuvor installierten Updates ausführen.

Während der Installation von heruntergeladenen Updates wird Kaspersky Security Service automatisch beendet und anschließend neu gestartet.

Informationen zum Update der Programm-Datenbanken

Die auf einem geschützten Gerät gespeicherten Datenbanken von Kaspersky Embedded Systems Security veralten schnell. Die Virenanalytiker von Kaspersky entdecken täglich Hunderte neuer Bedrohungen, erstellen entsprechende Einträge und nehmen sie in die Updates der Programm-Datenbanken auf. Ein Datenbanken-Update besteht aus einer oder mehreren Dateien mit Einträgen, durch die sich Bedrohungen identifizieren lassen, die seit dem vorhergehenden Update erkannt wurden. Um das Infektionsrisiko für das Gerät auf ein Minimum zu reduzieren, sollten Sie regelmäßig ein Datenbanken-Update ausführen.

Standardmäßig tritt das Ereignis *Programm-Datenbanken sind veraltet* ein, wenn die Datenbanken von Kaspersky Embedded Systems Security seit der Erstellung der installierten Datenbanken-Updates eine Woche lang nicht aktualisiert wurden. Erfolgt binnen zwei Wochen kein Update, erscheint die Meldung *Programm-Datenbanken sind stark veraltet*. Informationen über den aktuellen Status der Datenbanken werden im Ergebnisbereich des **Kaspersky Embedded Systems Security** Hauptknotens der Programmkonsolenstruktur angezeigt. Sie können die allgemeinen Parameter von Kaspersky Embedded Systems Security verwenden, um eine andere Anzahl von Tagen anzugeben, nach denen diese Ereignisse eintreten. Sie können ferner die Benachrichtigungen des Administrators über diese Ereignisse anpassen.

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

Sie können die Updates auf jedes der geschützten Geräte herunterladen oder ein geschütztes Gerät als Verteiler einrichten, so dass die Updates darauf kopiert und anschließend an die geschützten Geräte verteilt werden. Wenn Sie Kaspersky Security Center für die zentralisierte Verwaltung des Geräteschutzes im Unternehmen verwenden, können Sie den Kaspersky Security Center-Administrationsserver als Verteiler für das Herunterladen von Updates einsetzen.

Sie können die Aufgabe für das Update der Programm-Datenbanken manuell oder nach Zeitplan starten. Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe zum Update der Programm-Datenbanken stündlich.

Wenn der Update-Download unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zu den Datenbanken aus den zuletzt installierten Updates zurück. Wenn die Datenbanken von Kaspersky Embedded Systems Security beschädigt werden, kann ein manuelles Rollback auf zuvor installierte Updates: durchgeführt werden.

Schemata für Updates der Antivirus-Programmdatenbanken und verwendeten Module in einem Unternehmen

Die Auswahl einer Update-Quelle bei den Update-Aufgaben hängt von dem verwendeten Schema für die Aktualisierung der Datenbank und Programm-Module im Unternehmen ab.

Sie können die Datenbanken und Module von Kaspersky Embedded Systems Security auf den geschützten Geräten nach folgendem Schemata aktualisieren:

- Download von Updates direkt aus dem Internet auf jedes der geschützten Geräte (Schema 1).
- Download von Updates aus dem Internet auf ein zwischengeschaltetes Gerät und Verteilung des Updates von diesem Gerät aus auf die geschützten Geräte.

  Als Verteiler kann jedes zwischengeschaltete Gerät dienen, auf dem eine der folgenden Anwendungen installiert ist:

  - Kaspersky Embedded Systems Security (Schema 2).
  - Kaspersky Security Center-Administrationsserver (Schema 3).

Das Update über ein zwischengeschaltetes Gerät spart nicht nur Internet-Datenverkehr ein, sondern bietet den geschützten Geräten auch zusätzliche Sicherheit.

Die Update-Schemata werden im Folgenden beschrieben.

Schema 1. Direktes Aktualisieren von Datenbanken und Modulen aus dem Internet

Um Updates für Kaspersky Embedded Systems Security direkt aus dem Internet anzupassen, gehen Sie wie folgt vor:

Geben Sie auf jedem geschützten Gerät in den Einstellungen der Aufgaben zum Update der Programm-Datenbanken und Update der Programm-Module als Update-Quelle die Kaspersky-Update-Server an.

Als Update-Quelle können auch andere HTTP- oder FTP-Server gewählt werden, auf denen sich ein Ordner mit den Update-Dateien befindet.

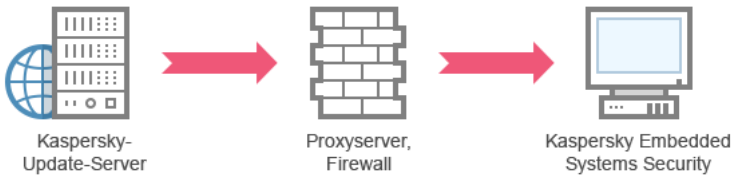


Abbildung 1: Direktes Aktualisieren von Datenbanken und Modulen aus dem Internet

Schema 2. Aktualisieren von Datenbanken und Modulen über eines der geschützten Geräte

Um die Updates für Kaspersky Embedded Systems Security über eines der geschützten Geräte anzupassen, gehen Sie wie folgt vor:

1. Kopieren Sie die Updates auf das ausgewählte geschützte Gerät. Gehen Sie hierzu wie folgt vor:
   - Passen Sie auf dem als Verteiler ausgewählten Gerät die Einstellungen der Aufgabe Update-Verteilung an:
     a. Geben Sie als Update-Quelle den Kaspersky-Update-Server an.
     b. Geben Sie als Ordner, in dem die Updates gespeichert werden sollen, einen freigegebenen Ordner an.
2. Verteilen Sie die Updates auf die übrigen geschützten Geräte. Gehen Sie hierzu wie folgt vor:
   - Passen Sie auf jedem geschützten Gerät die Aufgaben zum Update der Programm-Datenbanken und Update der Programm-Module an (siehe Abbildung unten):
     a. Geben Sie als Update-Quelle den Ordner auf dem Laufwerk des zwischengeschalteten Geräts an, in den die Updates kopiert werden.

Kaspersky Embedded Systems Security erhält die Updates dann über eines der geschützten Geräte.

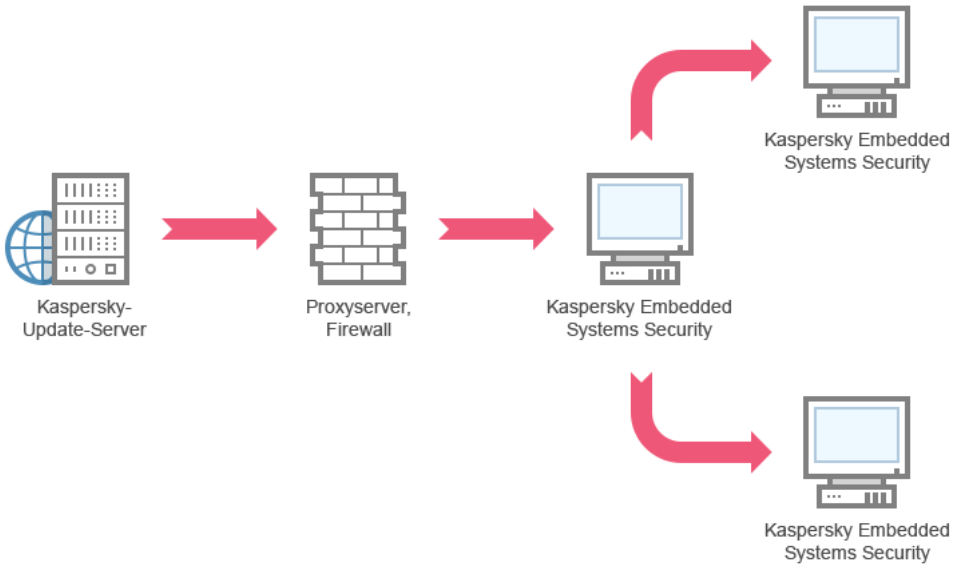


Abbildung 2: Aktualisieren von Datenbanken und Modulen über eines der geschützten Geräte

Schema 3. Aktualisieren von Datenbanken und Modulen über den Kaspersky Security Center-Administrationsserver

Wenn Sie Kaspersky Security Center für die zentrale Verwaltung des Antiviren-Schutzes für Geräte einsetzen, können Sie Updates über den Kaspersky Security Center-Administrationsserver downloaden (siehe Abbildung unten).

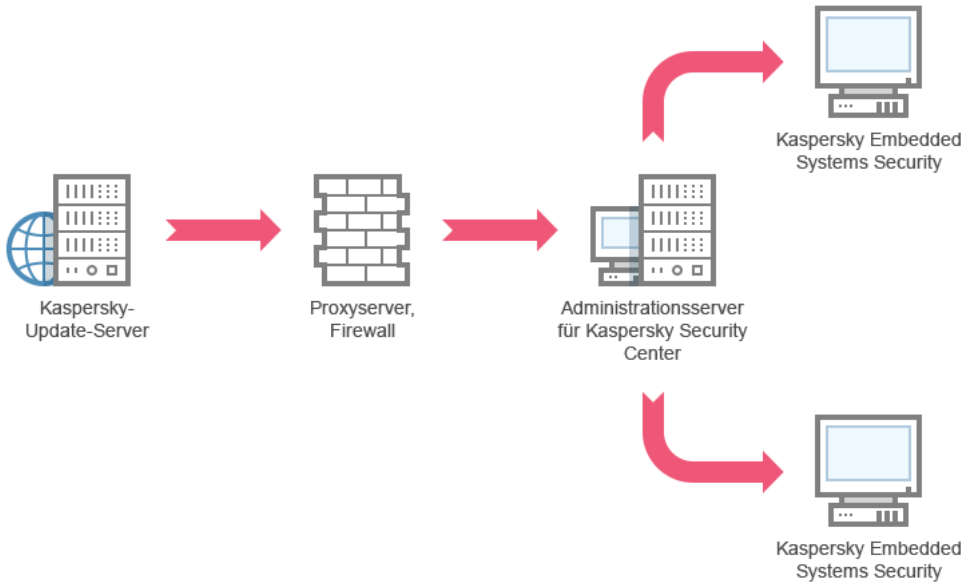


Abbildung 3: Aktualisieren von Datenbanken und Modulen über einen Kaspersky Security Center-Administrationsserver

Um den Erhalt von Updates für Kaspersky Embedded Systems Security über den Kaspersky Security Center Administrationsserver anzupassen, gehen Sie wie folgt vor:

1. Laden Sie die Updates von einem Kaspersky-Update-Server auf den Administrationsserver von Kaspersky Security Center herunter. Gehen Sie hierzu wie folgt vor:

   - Passen Sie die globale Aufgabe Update-Download durch Administrationsserver für die angegebenen Zusammenstellungen von geschützten Geräten an:

     a. Geben Sie als Update-Quelle die Kaspersky-Update-Server an.

2. Verteilen Sie die Updates auf die geschützten Geräte. Führen Sie hierzu eine der folgenden Aktionen aus:

   - Passen Sie in Kaspersky Security Center eine Gruppenaufgabe zum Update der Antiviren-Datenbanken (Programm-Modul) für die Verteilung der Updates an die geschützten Geräte an:

     a. Wählen Sie im Aufgabenzeitplan die Startfrequenz **Nach Update-Download durch den Administrationsserver**.

     Der Administrationsserver startet die Aufgabe jedes Mal, wenn er Updates empfängt (Diese Variante gilt als empfohlen).

   Die Startfrequenz **Nach Update-Download durch den Administrationsserver** kann in der Programmkonsole nicht angegeben werden.

   - Erstellen Sie auf jedem der geschützten Geräte die Aufgaben Update der Programm-Datenbanken und Update der Programm-Module:

     a. Geben Sie den Kaspersky Security Center-Administrationsserver als Update-Quelle an.

     b. Passen Sie den Zeitplan für die Aufgabe bei Bedarf an.

   Bei zu seltenen Updates der Antiviren-Datenbanken von Kaspersky Embedded Systems Security (einmal monatlich bis einmal jährlich) sinkt die Wahrscheinlichkeit, dass Bedrohungen entdeckt werden, während die Häufigkeit von Fehlalarmen der Programmkomponenten steigt.

   Kaspersky Embedded Systems Security erhält die Updates dann über den Kaspersky Security Center Administrationsserver.

Wenn Sie zur Update-Verteilung den Einsatz des Administrationsservers von Kaspersky Security Center planen, installieren Sie zuerst auf jedem geschützten Gerät die Programmkomponente Administrationsagent, die zum Lieferumfang von Kaspersky Security Center gehört. Er gewährleistet die Interaktion zwischen dem Administrationsserver und Kaspersky Embedded Systems Security auf dem geschützten Gerät. Ausführliche Informationen zum Administrationsagenten und seiner Konfiguration mithilfe von Kaspersky Security Center finden Sie in der *Hilfe für Kaspersky Security Center*.

Einstellung von Update-Aufgaben

Dieser Abschnitt enthält Anweisungen zum Anpassen der Update-Aufgaben von Kaspersky Embedded Systems Security.

Anpassen der Einstellungen für die Arbeit mit Update-Quellen für Kaspersky Embedded Systems Security

Für jede Update-Aufgabe, mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates der Programmdatenbanken, können Sie eine oder mehrere Update-Quellen angeben, benutzerdefinierte Update-Quellen hinzufügen und die Einstellungen zur Verbindung mit den angegebenen Update-Quellen konfigurieren.

Nach Anpassung der Einstellungen für die Update-Aufgaben werden die neuen Werte in laufenden Update-Aufgaben nicht sofort übernommen. Die vorgenommenen Einstellungen treten erst beim nächsten Aufgabenstart in Kraft.

Um den Typ der Update-Quelle festzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Update-Aufgabe entspricht, die Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Wählen Sie im Abschnitt **Update-Quelle** den Typ der Update-Quelle für Kaspersky Embedded Systems Security aus:
   - **Kaspersky Security Center-Administrationsserver**
   - **Kaspersky-Update-Server**
   - **Andere HTTP-, FTP-Server oder Netzwerkressourcen**
5. Passen Sie bei Bedarf die erweiterten Einstellungen für die benutzerdefinierten Update-Quellen an:
   a. Betätigen Sie den Link **Andere HTTP-, FTP-Server oder Netzwerkressourcen**.
      1. Aktivieren oder deaktivieren Sie im erscheinenden Fenster **Update-Server** die Kontrollkästchen neben benutzerdefinierten Update-Quellen, um deren Verwendung zu starten oder zu beenden.
      2. Klicken Sie auf **OK**.
   b. Aktivieren oder deaktivieren Sie im Abschnitt **Update-Quelle** auf der Registerkarte **Allgemein** das Kontrollkästchen **Kaspersky-Update-Server verwenden, wenn die angegebenen Server nicht verfügbar sind**.
6. Wählen Sie im Fenster **Aufgabeneinstellungen** die Registerkarte **Verbindungseinstellungen** aus, um die Einstellungen für die Verbindungsaufnahme mit der Update-Quelle zu konfigurieren:
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Proxyserver-Einstellungen für die Verbindung zu Kaspersky-Update-Servern verwenden**.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Proxyserver-Einstellungen für die Verbindung zu anderen Servern verwenden**.

   Informationen über das Konfigurieren der optionalen Proxyservereinstellungen und Authentifizierungseinstellungen für den Zugriff auf den Proxyserver finden Sie im Abschnitt Aufgabe zum Update der Datenbank von Kaspersky Embedded Systems Security starten und anpassen.
7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Update-Quelle für Kaspersky Embedded Systems Security werden gespeichert und beim nächsten Aufgabenstart verwendet.

Sie können die Liste der benutzerdefinierten Update-Quellen für Kaspersky Embedded Systems Security bearbeiten.

Gehen Sie wie folgt vor, um die Liste der benutzerdefinierten Update-Quellen für das Programm zu ändern:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Update-Aufgabe entspricht, die Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Betätigen Sie den Link **Andere HTTP-, FTP-Server oder Netzwerkressourcen**.

   Daraufhin wird das Fenster **Update-Server** geöffnet.
5. Führen Sie folgende Aktionen aus:

   - Um eine neue benutzerdefinierte Update-Quelle hinzuzufügen, klicken Sie auf **Hinzufügen** und geben Sie in das Eingabefeld die Adresse des Ordners ein, in dem die Update-Dateien auf dem FPT- oder HTTP-Server gespeichert sind. Geben Sie den lokalen oder Netzwerkordner im UNC-Format (Universal Naming Convention) an. Drücken Sie die Taste **EINGABE**.

     Standardmäßig wird der hinzugefügte Ordner als Update-Quelle verwendet.
   - Um die Verwendung einer benutzerdefinierten Quelle zu deaktivieren, entfernen Sie in der Liste das Kontrollkästchen neben der Quelle.
   - Um die Verwendung einer benutzerdefinierten Quelle zu aktivieren, aktivieren Sie in der Liste das Kontrollkästchen neben der Quelle.
   - Um die Reihenfolge zu ändern, in der Kaspersky Embedded Systems Security auf benutzerdefinierte Update-Quellen zugreift, verschieben Sie die gewünschte Quelle mithilfe der Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Stelle der Liste, je nachdem, wann auf die Quelle zugegriffen werden soll.
   - Um den Pfad einer benutzerdefinierten Quelle zu ändern, markieren Sie die Quelle in der Liste und klicken auf die Schaltfläche **Ändern**. Nehmen Sie dann im Eingabefeld die erforderlichen Änderungen vor und klicken Sie die **EINGABE**-Taste.
   - Um eine benutzerdefinierte Quelle zu löschen, markieren Sie sie in der Liste und klicken Sie auf die Schaltfläche **Löschen**.

     Ist nur eine einzige benutzerdefinierte Quelle in der Liste enthalten, können Sie diese nicht entfernen.
6. Klicken Sie auf **OK**.

Die Änderungen an der Liste der benutzerdefinierten Update-Quellen für das Programm werden gespeichert.

Optimierung des Festplatten-Subsystems bei der Ausführung der Aufgabe zum Update der Programm-Datenbanken

Bei Ausführung der Aufgabe zum Update der Programm-Datenbanken legt Kaspersky Embedded Systems Security die Update-Dateien auf der lokalen Festplatte des geschützten Geräts ab. Sie können die Belastung des Festplatten-Subsystems des geschützten Geräts verringern, indem Sie die Update-Dateien während der Ausführung der Update-Aufgabe auf einer virtuellen Festplatte im Arbeitsspeicher ablegen.

Diese Funktion ist für die Betriebssysteme Microsoft Windows 7 und höher verfügbar.

Bei Nutzung dieser Funktion kann während der Ausführung der Aufgabe Update der Programm-Datenbanken eine zusätzliche logische Festplatte im Betriebssystem erscheinen. Nach Abschluss der Aufgabe verschwindet diese logische Festplatte wieder aus dem Betriebssystem.

So verringern Sie die Belastung des Festplatten-Subsystems auf dem geschützten Gerät während der Aufgabe "Update der Programm-Datenbanken":

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten **Update der Programm-Datenbanken** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Update der Programm-Datenbanken** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Nehmen Sie im Abschnitt **Optimierung der Nutzung des Festplatten-Subsystems** die folgenden Einstellungen vor:

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern**.
   - Geben Sie im Feld **Für die Optimierung genutztes Arbeitsspeichervolumen (MB)** das Arbeitsspeichervolumen in Megabyte an. Das Betriebssystem stellt dieses Arbeitsspeichervolumen temporär für die Speicherung der Update-Dateien während der Aufgabenausführung zur Verfügung. Standardmäßig ist ein Arbeitsspeichervolumen von 512 MB eingestellt. Das minimale Arbeitsspeichervolumen beträgt 400 MB.

     Wenn Sie die Aufgabe zum Update der Programm-Datenbanken mit aktivierter Funktion zur Optimierung des Festplattensubsystems ausführen, kann abhängig von der für die Funktion zugewiesenen RAM-Größe eine der folgenden Situationen eintreten:

     - Wenn der Wert zu klein ist, reicht die zugewiesene RAM-Größe möglicherweise nicht aus, um die Aufgabe zum Update der Programm-Datenbanken abzuschließen (z. B. während der ersten Aktualisierung), wodurch die Aufgabe mit einem Fehler abgeschlossen wird.

       In diesem Fall wird empfohlen, mehr RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.

     - Wenn der Wert zu Beginn der Aufgabe zur Aktualisierung der Datenbank zu groß ist, kann es vorkommen, dass es unmöglich ist, ein virtuelles Laufwerk mit der ausgewählten Größe im RAM zu erstellen. Die Funktion zur Optimierung des Festplattensubsystems wird daher automatisch deaktiviert und die Aufgabe zur Aktualisierung der Datenbank wird ohne die Funktion zur Optimierung ausgeführt.

       In diesem Fall wird empfohlen, weniger RAM für die Funktion zur Optimierung des Festplattensubsystems zuzuweisen.
5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und beim nächsten Aufgabenstart verwendet.

Einstellungen der Aufgabe zur Update-Verteilung anpassen

Um die Einstellungen der Aufgabe zur Update-Verteilung anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten **Update-Verteilung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Update-Verteilung** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Passen Sie auf den Registerkarten **Allgemein** und **Verbindungseinstellungen** die Einstellungen für die Arbeit mit den Updaten-Quellen an.
5. Führen Sie auf der Registerkarte **Allgemein** im Abschnitt **Einstellungen für die Update-Verteilung** folgende Schritte aus:
   - Geben Sie die Bedingungen für die Update-Verteilung des Programms an:
     - **Updates der Programm-Datenbanken verteilen**.
     - **Wichtige Updates der Programm-Module verteilen**.
     - **Updates der Programm-Datenbanken und wichtige Updates der Programm-Module verteilen**.
   - Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in den Kaspersky Embedded Systems Security die erhaltenen Updates kopieren soll.
6. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an.
7. Konfigurieren Sie auf der Registerkarte **Mit folgenden Rechten starten** die Aufgabe zum Start mithilfe eines bestimmten Benutzerkontos.
8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und beim nächsten Aufgabenstart verwendet.

Einstellungen der Aufgabe Update der Programm-Module anpassen

Um die Einstellungen der Aufgabe zum Update der Programm-Module zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten **Update der Programm-Module** aus.
3. Klicken Sie im Ergebnisfenster des Knotens **Update der Programm-Module** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Passen Sie auf den Registerkarten **Allgemein** und **Verbindungseinstellungen** die Einstellungen für die Arbeit mit den Updaten-Quellen an.

5. Konfigurieren Sie auf der Registerkarte **Allgemein** im Abschnitt **Update-Einstellungen** die Einstellungen für das Update der Programm-Module:

   - **Nur auf wichtige Updates der Programm-Module überprüfen**
   - **Wichtige Updates der Programm-Module verteilen und installieren**
   - **Neustart des Betriebssystems zulassen**
   - **Über verfügbare planmäßige Updates der Programm-Module informieren**

6. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an. Standardmäßig startet Kaspersky Embedded Systems Security die Aufgabe Update der Programm-Module jeden Freitag um 16:00 Uhr (gemäß den regionalen Zeiteinstellungen des geschützten Geräts).

7. Konfigurieren Sie auf der Registerkarte **Mit folgenden Rechten starten** die Aufgabe zum Start mithilfe eines bestimmten Benutzerkontos.

8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und beim nächsten Aufgabenstart verwendet.

Geplante Updatepakete werden von Kaspersky nicht auf den Update-Servern veröffentlicht, um sie automatisch zu installieren. Sie können solche Updatepakete von der Kaspersky-Webseite downloaden. Sie können einstellen, dass der Administrator eine Benachrichtigung über das Ereignis *Kritische und planmäßige Updates sind verfügbar* erhält. Die Benachrichtigung enthält die URL der Webseite, auf der das planmäßige Update heruntergeladen werden kann.

Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security

Vor der Übernahme des Datenbanken-Updates legt Kaspersky Embedded Systems Security Backup-Kopien der bis dahin verwendeten Datenbanken an. Wenn eine Aktualisierung unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Embedded Systems Security automatisch zum zuletzt installierten Datenbank-Update zurück.

Wenn nach einem Update der Programm-Datenbanken Probleme auftreten, können Sie die Datenbanken mit den zuvor installierten Updates wiederherstellen. Starten Sie dazu die Aufgabe zum Rollback des Datenbanken-Updates.

Um die Aufgabe Rollback des Datenbanken-Updates zu starten,

Klicken Sie auf den Link **Starten** im Ergebnisfenster des Knotens **Rollback des Programm-Datenbanken-Updates**.

Rollback des Updates für Programm-Module

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

Bevor Updates der Programm-Module installiert werden, legt Kaspersky Embedded Systems Security Backup-Kopien der bisher verwendeten Module an. Wenn die Aktualisierung von Modulen unterbrochen oder fehlerhaft abgeschlossen wurde, kehrt Kaspersky Embedded Systems Security automatisch zu den Modulen aus den zuletzt installierten Updates zurück.

Um ein Rollback der Programm-Module auszuführen, verwenden Sie die Funktion **Programme ändern und löschen** in Microsoft Windows.

Statistik zu Update-Aufgaben

Während die Update-Aufgabe ausgeführt wird, können Sie in Echtzeit Informationen über das seit dem Aufgabenstart heruntergeladene Volumen der Daten, sowie eine Statistik über die Aufgabenausführung anzeigen.

Wenn die Aufgabe abgeschlossen ist oder abgebrochen wurde, ist die Information im Protokoll der Aufgabenausführung verfügbar.

So zeigen Sie Aufgabenstatistiken an:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Update**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe entspricht, deren Statistik Sie ansehen möchten.

Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Wenn Sie die Aufgabe zum Update der Programm-Datenbanken oder die Aufgabe zur Update-Verteilung anzeigen, wird im Abschnitt **Statistik** das Volumen der Daten anzeigt, die bis zum jetzigen Zeitpunkt von Kaspersky Embedded Systems Security empfangen wurden (**Empfangene Daten**).

Die folgende Tabelle enthält Informationen für die Aufgabe zum Update der Programm-Module.

Informationen über die Aufgabe Update der Programm-Module

Feld	Beschreibung
Empfangene Daten	Gesamtvolumen der empfangenen Daten.
Wichtige Updates sind verfügbar	Anzahl der kritischen Updates, die zur Installation bereitstehen.
Planmäßige Updates sind verfügbar	Anzahl der geplanten Updates, die zur Installation bereitstehen.
Fehler beim Übernehmen von Updates	Wenn dieser Wert ungleich Null ist, wurde das Update nicht übernommen. Der Name des Updates, bei dem ein Fehler aufgetreten ist, finden Sie im Protokoll der Aufgabenausführung.

Objekte isolieren und Backups kopieren

Dieser Abschnitt enthält Informationen über das Verschieben von gefundenen schädlichen Objekten ins Backup, bevor diese desinfiziert oder gelöscht werden, sowie Information über die Isolation möglicherweise infizierter Objekte.

Isolierung möglicherweise infizierter Objekte. Quarantäne

Dieser Abschnitt enthält Informationen über die Isolierung von möglicherweise infizierten Objekten, also über die Verschiebung dieser Objekte in die Quarantäne sowie über die Anpassung der Quarantäneeinstellungen.

Über die Isolierung möglicherweise infizierter Objekte

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

Quarantäneobjekte anzeigen

Die unter Quarantäne stehenden Objekte können im Knoten **Quarantäne** der Programmkonsole angezeigt werden.

So zeigen Sie Quarantäneobjekte an:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.

   Die Informationen über die in der Quarantäne befindlichen Objekte werden im Ergebnisbereich des ausgewählten Knotens angezeigt.

Um das gewünschte Objekt in der Liste der Quarantäne-Objekte zu finden,

sortieren Sie die Objekte oder verwenden Sie einen Filter.

Quarantäneobjekte sortieren

Die Objekte in der Liste mit den Quarantäneobjekten sind standardmäßig in umgekehrter chronologischer Reihenfolge nach dem Quarantänedatum angeordnet. Um das gewünschte Objekt zu finden, können Sie die Objekte nach Spalten mit Objektinformationen sortieren. Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne** schließen und erneut öffnen, oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und dann erneut aus dieser Datei öffnen.

So sortieren Sie Objekte:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.
3. Klicken Sie im Ergebnisfenster des Knotens **Quarantäne** auf den Titel der Spalte, nach deren Inhalt die Objekte in der Liste sortiert werden sollen.

Die Listenobjekte werden nach dem ausgewählten Parameter sortiert.

Quarantäneobjekte filtern

Um das gewünschte Objekt in der Quarantäne zu finden, können Sie die Objekte in der Liste filtern. Das heißt, es werden nur Objekte angezeigt, die den von Ihnen definierten Filterkriterien (Filtern) entsprechen. Das Filterergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne** schließen und erneut öffnen, oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und sie erneut aus dieser Datei öffnen.

So geben Sie mindestens einen Filter an:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.
3. Wählen Sie im Kontextmenü des Knotennamens den Punkt **Filter** aus.

   Das Fenster **Filtereinstellungen** wird geöffnet.
4. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie in der Liste **Feldname** das Feld aus, das die Grundlage für den Filter darstellt.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen aus. Die Filterbedingungen in der Liste können unterschiedlich sein, je nachdem, welchen Wert Sie in der Liste **Feldname** gewählt haben.
   c. Geben Sie im Feld **Feldwert** einen Wert für den Filter an oder wählen Sie ihn in der Liste aus.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt. Wiederholen Sie die Schritte a-d für jeden Filter, den Sie hinzufügen. Beachten Sie beim Arbeiten mit Filtern die folgenden Anweisungen:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.
   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.
   - Um einen Filter zu entfernen, markieren Sie ihn in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.
   - Um einen Filter zu ändern, wählen Sie den Filter in der Liste im Fenster **Filtereinstellungen** aus. Ändern Sie dann die benötigten Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.
5. Nachdem alle Filter hinzugefügt wurden, klicken Sie auf **Übernehmen**.

Die erstellten Filter werden gespeichert.

Um zur Ansicht mit allen Objekten in Quarantäne zurückzukehren,

wählen Sie im Kontextmenü des Knotens **Quarantäne** den Punkt **Filter entfernen** aus.

Untersuchung von Quarantäne-Objekten

Kaspersky Embedded Systems Security führt in der Grundeinstellung nach jedem Update der Programm-Datenbanken die lokalen Systemaufgabe Untersuchung von Quarantäne-Objekten aus. Die Aufgabenparameter werden in folgender Tabelle genannt. Sie können die Einstellungen für die Aufgabe Untersuchung von Quarantäne-Objekten ändern.

Sie können einen Zeitplan für den Aufgabenstart einrichten, die Aufgabe manuell starten sowie die Rechte des Benutzerkontos ändern, unter dem die Aufgabe gestartet werden soll.

Wenn die Quarantäne-Objekte nach einem Update der Programm-Datenbanken untersucht wurden, stuft Kaspersky Embedded Systems Security bestimmte Objekte möglicherweise als nicht infiziert ein: Der Status dieser Objekte ändert sich in der Liste auf **Fehlalarm**. Kaspersky Embedded Systems Security stuft andere Objekte möglicherweise als infiziert ein und führt für sie Aktionen aus, die in den Einstellungen der Aufgabe Untersuchung von Quarantäne-Objekten vorgegeben sind: Desinfizieren bzw. irreparable Objekte löschen.

Einstellungen der Aufgabe Untersuchung von Quarantäne-Objekten

Parameter der Aufgabe Untersuchung von Quarantäne-Objekten	Bedeutung
Untersuchungsbereich	Quarantäneordner
Sicherheitseinstellungen	Identisch für den gesamten Untersuchungsbereich; ihre Werte stehen in der folgenden Tabelle

Sicherheitsparameter der Aufgabe Untersuchung von Quarantäne-Objekten

Sicherheitsparameter	Bedeutung
Objekte untersuchen	Alle Objekte im Untersuchungsbereich
Optimierung	Deaktiviert
Aktion für infizierte und andere Objekte	Desinfizieren, irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte	Überspringen
Dateien ausschließen	Nein
Nicht erkennen	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	Nicht festgelegt.
Objekte nicht untersuchen, wenn größer als (MB)	Nicht festgelegt.
Alternative NTFS-Ströme	Aktiviert
Bootsektoren und MBR	Deaktiviert
iChecker-Technologie verwenden	Deaktiviert
iSwift-Technologie verwenden	Deaktiviert
Zusammengesetzte Objekte untersuchen	• **Archive*** • **SFX-Archive***

	• **Gepackte Objekte*** • **Eingebettete OLE-Objekte*** * **Nur neue und veränderte Dateien untersuchen** ist deaktiviert.
Dateien auf Microsoft-Signatur überprüfen	Wird nicht ausgeführt.
Heuristische Analyse verwenden	Die Analysestufe **Tief** ist eingestellt.
Vertrauenswürdige Zone	Wird nicht verwendet

Wiederherstellung von Objekten aus der Quarantäne

Kaspersky Embedded Systems Security verschiebt möglicherweise infizierte Objekte verschlüsselt in den Quarantäne-Ordner, damit das geschützte Gerät vor jeglichen schädlichen Auswirkungen bewahrt wird.

Sie können jedes Objekt aus der Quarantäne wiederherstellen. Das kann in folgenden Fällen notwendig sein:

- Nach der Untersuchung von Quarantäne-Objekten anhand der aktualisierten Datenbanken wechselt der Status des Objektes auf **Fehlalarm** oder **Desinfiziert**.
- Sie schätzen das Objekt als nicht gefährlich für das geschützte Gerät ein und wollen es benutzen. Damit Kaspersky Embedded Systems Security das Objekt bei künftigen Untersuchungen nicht isoliert, können Sie das Objekt von der Untersuchung in der Aufgabe zum Echtzeitschutz für Dateien und in den Aufgaben zur Untersuchung auf Befehl ausschließen. Geben Sie dazu das Objekt in der Sicherheitseinstellung **Dateien ausschließen** (nach Dateiname) oder **Nicht erkennen** in diesen Aufgaben an oder fügen Sie es zur vertrauenswürdigen Zone hinzu.

Beim Wiederherstellen eines Objektes können Sie entscheiden, wo das wiederhergestellte Objekt gespeichert werden soll: am ursprünglichen Ort (Standard), in einem speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Gerät oder in einem benutzerdefinierten Ordner auf dem geschützten Gerät, auf dem die Programmkonsole installiert ist, oder auf einem anderen Gerät des Netzwerks.

Sie können den Ordner angeben, der zum Speichern wiederhergestellter Objekte auf dem geschützten Gerät verwendet wird. Sie können für seine Untersuchung spezielle Sicherheitsparameter festlegen. Der Pfad dieses Ordners wird in den Quarantäneeinstellungen angegeben.

Die Wiederherstellung von Objekten aus der Quarantäne kann das geschützte Gerät infizieren.

Sie können ein Objekt wiederherstellen, nachdem eine Kopie im Quarantäne-Ordner gespeichert worden ist, damit Sie es weiter benutzen können, beispielsweise, um das Objekt nach einem Datenbanken-Update noch einmal zu untersuchen.

Wenn ein in die Quarantäne verschobenes Objekt zu einem zusammengesetzten Objekt gehört (z. B. zu einem Archiv), fügt Kaspersky Embedded Systems Security das Quarantäne-Objekt bei der Wiederherstellung nicht mehr in das zusammengesetzte Objekt ein, sondern speichert das Quarantäne-Objekt separat im festgelegten Ordner.

Sie können ein Objekt oder mehrere Objekte wiederherstellen.

Um eine Datei aus der Quarantäne wiederherzustellen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.

2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.

3. Führen Sie im Ergebnisfenster des Knotens **Quarantäne** eine der folgenden Aktionen aus:

   - Wählen Sie zur Wiederherstellung eines Objekts im Kontextmenü des Objekts, das Sie wiederherstellen wollen, den Punkt **Wiederherstellen** aus.

   - Um mehrere Objekte wiederherzustellen, wählen Sie in der Liste die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der markierten Objekte, und wählen Sie den Punkt Wiederherstellen aus.

   Das Fenster **Objektwiederherstellung** wird geöffnet.

4. Geben Sie im Fenster **Objektwiederherstellung** für jedes ausgewählte Objekt den Ordner an, in dem das wiederhergestellte Objekt gespeichert werden soll.

   Der Name des Objekts wird im Feld **Objekt** im oberen Bereich des Fensters angezeigt. Wenn Sie mehrere Objekte ausgewählt haben, wird der Name des ersten Objekts in der Liste der ausgewählten Objekte angezeigt.

5. Führen Sie eine der Aktionen durch:

   - Um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im Ursprungsordner wiederherstellen**.

   - Um ein Objekt in einem Ordner wiederherzustellen, den Sie in den Quarantäneeinstellungen als Ordner für wiederhergestellte Objekte angegeben haben, wählen Sie **Im Standard-Ordner wiederherstellen** aus.

   - Um ein Objekt in einem anderen Ordner auf dem geschützten Gerät, auf dem die Programmkonsole installiert ist, oder in einem freigegebenen Ordner zu speichern, wählen Sie **In einem Ordner auf dem lokalem Rechner wiederherstellen** und anschließend den gewünschten Ordner aus oder geben dessen Pfad ein.

6. Wenn Sie nach der Wiederherstellung eines Objekts eine Kopie des Objekts im *Quarantäne*-Ordner speichern möchten, deaktivieren Sie das Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Speicher löschen**.

7. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

   Alle ausgewählten Objekte werden wiederhergestellt und in dem angegebenen Verzeichnis gespeichert. Bei Auswahl der Variante **Im Ursprungsordner wiederherstellen** wird jedes Objekt an seinem ursprünglichen Speicherort gespeichert. Bei Auswahl der Variante **Im Standard-Ordner wiederherstellen** oder **In einem Ordner auf dem lokalem Rechner wiederherstellen** werden alle Objekte im angegebenen Ordner gespeichert.

8. Klicken Sie auf **OK**.

   Kaspersky Embedded Systems Security beginnt damit, das erste ausgewählte Objekt wiederherzustellen.

9. Wenn am angegebenen Ort bereits ein Objekt mit diesem Namen vorhanden ist, wird das Fenster **Ein Objekt mit diesem Namen ist bereits vorhanden** geöffnet.

   a. Wählen Sie eine der folgenden Aktionen für Kaspersky Embedded Systems Security aus:

      - **Ersetzen**, um das vorhandene Objekt mit dem wiederhergestellten Objekt zu ersetzen.

- **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie den Dateinamen und den vollständigen Pfad für das neue wiederhergestellte Objekt ein.

- **Umbenennen und Suffix hinzufügen**, um das wiederhergestellte Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie im Eingabefeld das Suffix ein.

b. Wenn Sie mehrere Objekte zur Wiederherstellung ausgewählt haben, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**, um die ausgewählte Aktion (**Ersetzen** oder **Umbenennen**) auf die übrigen ausgewählten Objekte anzuwenden. Wenn Sie **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, steht das Kontrollkästchen **Umbenennen** nicht zur Verfügung.

c. Klicken Sie auf **OK**.

Das Objekt wird wiederhergestellt. Informationen über den Wiederherstellungsvorgang werden im Systemaudit-Protokoll aufgezeichnet.

Wenn Sie im Fenster **Objektwiederherstellung** nicht **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, öffnet sich das Fenster **Objektwiederherstellung** noch einmal. Verwenden Sie dieses Fenster, um den Speicherort anzugeben, an dem das folgende ausgewählte Objekt wiederhergestellt werden soll (s. Schritt 4 dieser Anleitung).

Verschieben von Objekten in die Quarantäne

Sie können manuell Dateien in die Quarantäne verschieben.

So verschieben Sie eine Datei in die Quarantäne:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Quarantäne**.
2. Wählen Sie den Punkt **Hinzufügen** aus.
3. Geben Sie im Fenster **Öffnen** die Datei an, die Sie in die Quarantäne verschieben möchten.
4. Klicken Sie auf **OK**.

Kaspersky Embedded Systems Security verschiebt die ausgewählte Datei in die Quarantäne.

Objekte aus der Quarantäne löschen

Auf Grundlage der Einstellungen der Aufgabe zur Untersuchung von Quarantäne-Objekten löscht Kaspersky Embedded Systems Security Objekte automatisch aus dem Quarantäne-Ordner, wenn sich deren Status bei der Quarantäne-Untersuchung anhand aktualisierter Datenbanken in *Infiziert oder gefunden* ändert und Kaspersky Embedded Systems Security diese nicht desinfizieren kann. Andere Objekte werden von Kaspersky Embedded Systems Security nicht aus der Quarantäne gelöscht.

Sie können ein oder mehrere Objekte aus der Quarantäne entfernen.

So löschen Sie mindestens ein Objekt aus der Quarantäne:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Quarantäne** aus.

3. Führen Sie eine der Aktionen durch:

   - Wählen Sie zum Entfernen eines Objekts im Kontextmenü des Objektnamens den Punkt **Löschen** aus.
   - Um mehrere Objekte zu löschen, markieren Sie die entsprechenden Objekte mithilfe der Taste **Strg** oder **Umschalt** die entsprechenden Objekte. Öffnen Sie anschließend das Kontextmenü für eines der gewählten Objekte und wählen Sie den Punkt **Löschen** aus.

4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um die Operation zu bestätigen.

Die ausgewählten Objekte werden aus der Quarantäne gelöscht.

Möglicherweise infizierte Quarantäneobjekte zur Analyse an Kaspersky einschicken

Wenn das Verhalten einer bestimmten Datei den Verdacht nahelegt, dass sie eine Bedrohung enthält, Kaspersky Embedded Systems Security die Datei aber als virenfrei einstuft, handelt es sich möglicherweise um eine neue, unbekannte Bedrohung, deren Beschreibung noch nicht in den Datenbanken verzeichnet ist. Sie können diese Datei zur Analyse in das Virenlabor von Kaspersky einschicken. Die Viren-Analytiker von Kaspersky untersuchen die Datei. Wenn sie eine neue Bedrohung finden, wird den Datenbanken ein entsprechender Eintrag und ein Desinfektionsalgorithmus hinzugefügt. Wenn Sie das Objekt nach einem Datenbanken-Update erneut untersuchen, ist es wahrscheinlich, dass Kaspersky Embedded Systems Security die Datei als infiziert einstuft und sie desinfizieren kann. Dadurch können Sie nicht nur das Objekt retten, sondern auch dabei helfen, eine Virenepidemie zu verhindern.

Nur Dateien aus der Quarantäne können zur Analyse eingeschickt werden. Die in der Quarantäne befindlichen Dateien werden in verschlüsselter Form gespeichert und beim Verschicken nicht von der auf dem Mail-Server installierten Antiviren-Anwendung gelöscht.

Ein Objekt in Quarantäne kann nach Ablauf der Lizenz nicht an Kaspersky zur Analyse geschickt werden.

So senden Sie eine Datei zur Analyse an Kaspersky:

1. Wenn sich die Datei nicht in der Quarantäne befindet, verschieben Sie sie zuerst in die **Quarantäne**.
2. Öffnen Sie im Knoten **Quarantäne** in der Liste der Quarantäneobjekte das Kontextmenü der Datei, die zur Analyse an Kaspersky geschickt werden soll, und wählen Sie den Punkt **Objekt zur Analyse einschicken**.
3. Klicken Sie im erscheinenden Bestätigungsfenster auf **Ja**, wenn Sie das ausgewählte Objekt tatsächlich zur Untersuchung versenden möchten.
4. Wenn auf dem geschützten Gerät, auf dem die Programmkonsole installiert ist, ein Mail-Client eingerichtet ist, wird eine neue E-Mail-Nachricht erstellt. Prüfen Sie die Nachricht und klicken Sie anschließend auf die Schaltfläche **Senden**.

   Das Feld **Empfänger** enthält die E-Mail-Adresse von Kaspersky newvirus@kaspersky.com. Das Feld mit dem Betreff enthält den Text "Quarantäneobjekt".

   Der Nachrichtenkörper enthält den Text "Datei wurde zur Analyse an Kaspersky geschickt". Sie können der Nachricht zusätzliche Informationen über die Datei hinzufügen: z. B. warum Sie die Datei für möglicherweise infiziert oder gefährlich halten, wie sich die Datei verhält und wie sie das System beeinflusst.

   Die Nachricht enthält als Anlage das Archiv mit dem Namen <Objektname>.cab. Es enthält eine Datei <uuid>.klq mit dem Objekt in verschlüsselter Form, eine Datei <uuid>.txt mit Daten, die Kaspersky Embedded Systems Security über das Objekt abgerufen hat, und eine Datei Sysinfo.txt, die folgende Informationen über Kaspersky Embedded Systems Security und das auf dem geschützten Gerät installierte Betriebssystem enthält:

- Name und Version des Betriebssystems.
- Name und Version von Kaspersky Embedded Systems Security.
- Veröffentlichungsdatum der zuletzt installierten Updates der Programm-Datenbanken.
- Aktiver Schlüssel.

Diese Informationen benötigen die Virenanalytiker von Kaspersky zur schnellen und effektiven Analyse einer Datei. Wenn Sie diese Daten jedoch nicht senden möchten, können Sie die Datei Sysinfo.txt aus dem Archiv entfernen.

Falls auf dem geschützten Gerät, auf dem die Programmkonsole installiert ist, kein Mail-Client vorhanden ist, schlägt das Programm vor, das ausgewählte verschlüsselte Objekt in einer Datei zu speichern. Schicken Sie die Datei manuell an Kaspersky.

So speichern Sie ein verschlüsseltes Objekt in einer Datei:

1. Klicken Sie im nächsten Fenster zum Speichern des Objekts auf **OK**.
2. Wählen Sie den Ordner auf einem Laufwerk des geschützten Geräts oder den Netzwerkordner, in den Sie die Datei mit dem Objekt speichern möchten.

Das Objekt wird in einer CAB-Datei gespeichert.

Anpassen der Quarantäne-Einstellungen

Sie können die Quarantäne-Einstellungen anpassen. Neue Quarantäne-Einstellungen werden unmittelbar nach dem Speichern übernommen.

So konfigurieren Sie die Quarantäne-Einstellungen:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Quarantäne**.
3. Wählen Sie den Menüpunkt **Eigenschaften**.
4. Passen Sie im Fenster **Quarantäne der Quarantäne** die Quarantäne-Einstellungen entsprechend an:
   - Im Abschnitt **Quarantäne-Einstellungen**:
     - **Quarantäneordner**
     - **Maximale Größe der Quarantäne (MB)**
     - **Grenzwert für verfügbaren Speicherplatz (MB)**

     Überschreitet der Umfang der in der Quarantäne befindlichen Objekte die maximale Größe der Quarantäne oder den Grenzwert für den verfügbaren Speicherplatz, so werden Sie von Kaspersky Embedded Systems Security hierüber benachrichtigt, wobei die Objekte jedoch trotzdem in die Quarantäne verschoben werden.

- Im Abschnitt **Einstellungen für die Wiederherstellung von Objekten**:
  - Ordner für die Wiederherstellung von Objekten

5. Klicken Sie auf **OK**.

Die neu vorgenommenen Quarantäne-Einstellungen werden gespeichert.

Quarantäne-Statistik

Sie können Informationen über die Anzahl der Quarantäneobjekte anzeigen, z. B. eine Statistik für die Quarantäne.

Um eine Statistik für die Quarantäne anzuzeigen,

wählen Sie im Kontextmenü des Knotens **Quarantäne** in der Struktur der Programmkonsole den Punkt **Statistik** aus.

Im Fenster **Quarantäne-Statistik** werden Informationen über die aktuelle Anzahl der Quarantäneobjekte angezeigt (s. Tabelle unten):

Feld	Beschreibung
Möglicherweise infizierte Objekte	Anzahl der von Kaspersky Embedded Systems Security gefundenen Objekte, die als möglicherweise infiziert eingestuft wurden
Aktuelle Größe der Quarantäne	Gesamtmenge der Daten im Quarantäne-Ordner.
Fehlalarme	Anzahl der Objekte, die den Status *Fehlalarm* erhielten, weil sie bei der Untersuchung von Quarantäne-Objekten unter Verwendung von aktualisierten Datenbanken als nicht infiziert eingestuft wurden.
Desinfizierte Objekte	Anzahl der Objekte, denen nach der Untersuchung von Quarantäne-Objekten der Status *Desinfiziert* zugewiesen wurde.
Objekte insgesamt	Anzahl der Quarantäneobjekte.

Backup-Kopien von Objekten erstellen. Backup

Dieser Abschnitt enthält Informationen über das Verschieben von gefundenen schädlichen Objekten ins Backup, bevor diese desinfiziert oder gelöscht werden, sowie Anleitungen zur Anpassung der Backup-Einstellungen.

Über das Verschieben von Objekten vor der Desinfektion oder dem Löschen ins Backup

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

Wenn ein Objekt Bestandteil eines zusammengesetzten Objekts ist (z. B. zu einem Archiv gehört), wird das gesamte zusammengesetzte Objekt von Kaspersky Embedded Systems Security ins Backup kopiert. Wenn Kaspersky Embedded Systems Security z. B. ein Objekt aus einer Mail-Datenbank als infiziert einstuft, wird die komplette Mail-Datenbank gesichert.

Wenn ein Objekt, das von Kaspersky Embedded Systems Security ins Backup kopiert wird, umfangreich ist, kann sich das System verlangsamen und der verfügbare Festplattenplatz kann sich verringern.

Sie können Dateien aus dem Backup entweder im ursprünglichen Ordner oder in einem anderen Ordner auf dem geschützten Gerät oder einem anderen Gerät des lokalen Netzwerks wiederherstellen. Eine Datei kann aus dem Backup wiederhergestellt werden, z. B. wenn eine infizierte Datei wichtige Informationen enthält, aber Kaspersky Embedded Systems Security nicht in der Lage ist, die Datei zu desinfizieren ohne die Integrität zu beschädigen und Daten zu verlieren.

Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des geschützten Geräts führen.

Objekte im Backup anzeigen

Die Objekte im Backup-Ordner können nur über die Programmkonsole im Knoten **Backup** angezeigt werden. Sie können die Dateien nicht mit den Dateimanagern von Microsoft Windows anzeigen.

Um Objekte im Backup anzuzeigen,

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Backup** aus.

   Die Informationen über die im Backup befindlichen Objekte werden im Ergebnisbereich des ausgewählten Knotens angezeigt.

Um ein bestimmtes Objekt in der Liste der Backup-Objekte zu finden,

sortieren Sie die Objekte oder verwenden Sie einen Filter.

Dateien im Backup sortieren

Standardmäßig werden die Dateien im Backup nach ihrem Backup-Datum in umgekehrter chronologischer Reihenfolge sortiert. Um die gewünschte Datei zu finden, können Sie die Dateien nach dem Inhalt einer beliebigen Spalte im Ergebnisfenster sortieren.

Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen und erneut öffnen, oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und sie erneut aus dieser Datei öffnen.

So sortieren Sie Dateien im Backup:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.

2. Wählen Sie den untergeordneten Knoten **Backup** aus.

3. Wählen Sie In der Dateiliste im **Backup** den Titel der Spalte aus, nach deren Inhalt Sie die Objekte sortieren möchten.

Die im Backup befindlichen Dateien werden nach dem ausgewählten Kriterium sortiert.

Dateien im Backup filtern

Um die gewünschte Datei im Backup zu finden, können Sie die Dateien filtern, das heißt, im Knoten **Backup** nur Dateien anzeigen, die den von Ihnen definierten Filterbedingungen (Filtern) entsprechen.

Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Backup** schließen oder wenn Sie die Programmkonsole schließen, die msc-Datei speichern und sie wieder aus dieser Datei öffnen.

So filtern Sie Dateien im Backup:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Knoten **Backup** und wählen Sie den Punkt **Filter** aus.

   Das Fenster **Filtereinstellungen** wird geöffnet.

2. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

   a. Wählen Sie in der Liste **Feldname** das Feld aus, das die Grundlage für den Filter darstellt.

   b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterbedingungen in der Liste können unterschiedlich sein, je nachdem, welchen Wert Sie im Feld **Feldname** gewählt haben.

   c. Geben Sie im Feld **Feldwert** einen Wert für den Filter an oder wählen Sie ihn aus.

   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt. Wiederholen Sie die Schritte für jeden Filter, den Sie hinzufügen. Beachten Sie beim Arbeiten mit Filtern die folgenden Anweisungen:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.

   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.

   - Um einen Filter zu entfernen, markieren Sie ihn in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.

   - Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Fensters **Filtereinstellungen**, ändern Sie die entsprechenden Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

   Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**. In der Liste werden nur die Dateien angezeigt, die den von Ihnen definierten Filtern entsprechen.

Damit wieder alle Dateien in der Liste der Backup-Dateien angezeigt werden,

wählen Sie im Kontextmenü des Knotens **Backup** den Punkt **Filter entfernen** aus.

Dateien aus Backup wiederherstellen

Kaspersky Embedded Systems Security speichert Dateien im Backup im verschlüsselten Format, damit das geschützte Gerät vor schädlichen Wirkungen bewahrt wird.

Sie können Dateien aus dem Backup wiederherstellen.

In den folgenden Fällen müssen Sie möglicherweise eine Datei wiederherstellen:

- Die Ursprungsdatei, die sich als infiziert herausgestellt hat, enthielt wichtige Informationen und Kaspersky Embedded Systems Security konnte bei der Reparatur dieser Datei deren Integrität nicht retten, sodass auf die Informationen deshalb nicht mehr zugegriffen werden kann.

- Sie schätzen die Datei als nicht gefährlich für das geschützte Gerät ein und wollen sie benutzen. Damit Kaspersky Embedded Systems Security diese Datei bei künftigen Untersuchungen nicht als infiziert oder möglicherweise infiziert einstuft, können Sie sie von der Untersuchung in der Aufgabe zum Echtzeitschutz für Dateien und in den Aufgaben zur Untersuchung auf Befehl ausschließen. Geben Sie dazu die Datei in der Einstellung **Dateien ausschließen** oder in der Einstellung **Nicht erkennen** für diese Aufgaben an.

  Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des geschützten Geräts führen.

Beim Wiederherstellen einer Datei können Sie entscheiden, wo sie gespeichert werden soll: am ursprünglichen Speicherplatz (Standard), in einen speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Gerät oder in einen benutzerdefinierten Ordner auf dem geschützten Gerät, auf dem die Programmkonsole installiert ist, oder auf einem anderen Gerät im Netzwerk.

Sie können den Ordner zum Speichern wiederhergestellter Objekte auf dem geschützten Gerät angeben. Sie können für seine Untersuchung spezielle Sicherheitsparameter festlegen. Der Pfad dieses Ordners wird durch die Backup-Einstellungen angegeben.

Wenn Kaspersky Embedded Systems Security eine Datei wiederherstellt, wird standardmäßig eine Kopie im Backup angelegt. Nach der Wiederherstellung können Sie die Backup-Kopie aus dem Backup entfernen.

So stellen Sie Dateien aus Backup wieder her:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.

2. Wählen Sie den untergeordneten Knoten **Backup** aus.

3. Führen Sie im Ergebnisfenster des Knotens **Backup** eine der folgenden Aktionen aus:

   - Wählen Sie zur Wiederherstellung eines Objekts im Kontextmenü des Objekts, das Sie wiederherstellen wollen, den Punkt **Wiederherstellen** aus.

   - Um mehrere Objekte wiederherzustellen, wählen Sie in der Liste die entsprechenden Objekte mithilfe der Taste **STRG** oder **UMSCHALT** aus. Öffnen Sie anschließend das Kontextmenü eines der markierten Objekte, und wählen Sie den Punkt Wiederherstellen aus.

   Das Fenster **Objektwiederherstellung** wird geöffnet.

4. Geben Sie im Fenster **Objektwiederherstellung** für jedes ausgewählte Objekt den Ordner an, in dem das wiederhergestellte Objekt gespeichert werden soll.

Der Name des Objekts wird im Feld **Objekt** im oberen Bereich des Fensters angezeigt. Wenn Sie mehrere Objekte ausgewählt haben, wird der Name des ersten Objekts in der Liste der ausgewählten Objekte angezeigt.

5. Führen Sie eine der Aktionen durch:

   - Um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im Ursprungsordner wiederherstellen**.
   - Um ein Objekt in einem Ordner wiederherzustellen, den Sie in den Quarantäneeinstellungen als Ordner für wiederhergestellte Objekte angegeben haben, wählen Sie **Im Standard-Ordner wiederherstellen** aus.
   - Um ein Objekt in einem anderen Ordner auf dem geschützten Gerät, auf dem die Programmkonsole installiert ist, oder in einem freigegebenen Ordner zu speichern, wählen Sie **In einem Ordner auf dem lokalem Rechner wiederherstellen** und anschließend den gewünschten Ordner aus oder geben dessen Pfad ein.

6. Wenn Sie nach der Wiederherstellung keine Kopie der Datei im Backup-Ordner speichern möchten, aktivieren Sie das Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Speicher löschen** (standardmäßig deaktiviert).

7. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

   Alle ausgewählten Objekte werden wiederhergestellt und in dem angegebenen Verzeichnis gespeichert. Bei Auswahl der Variante **Im Ursprungsordner wiederherstellen** wird jedes Objekt an seinem ursprünglichen Speicherort gespeichert. Bei Auswahl der Variante **Im Standard-Ordner wiederherstellen** oder **In einem Ordner auf dem lokalem Rechner wiederherstellen** werden alle Objekte im angegebenen Ordner gespeichert.

8. Klicken Sie auf **OK**.

   Kaspersky Embedded Systems Security beginnt damit, das erste ausgewählte Objekt wiederherzustellen.

9. Wenn am angegebenen Ort bereits ein Objekt mit diesem Namen vorhanden ist, wird das Fenster **Ein Objekt mit diesem Namen ist bereits vorhanden** geöffnet.

   a. Wählen Sie eine der folgenden Aktionen für Kaspersky Embedded Systems Security aus:

      - **Ersetzen**, um das vorhandene Objekt mit dem wiederhergestellten Objekt zu ersetzen.
      - **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie den Dateinamen und den vollständigen Pfad für das neue wiederhergestellte Objekt ein.
      - **Umbenennen und Suffix hinzufügen**, um das wiederhergestellte Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie im Eingabefeld das Suffix ein.

   b. Wenn Sie mehrere Objekte zur Wiederherstellung ausgewählt haben, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**, um die ausgewählte Aktion (**Ersetzen** oder **Umbenennen**) auf die übrigen ausgewählten Objekte anzuwenden. Wenn Sie **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, steht das Kontrollkästchen **Umbenennen** nicht zur Verfügung.

   c. Klicken Sie auf **OK**.

Das Objekt wird wiederhergestellt. Informationen über den Wiederherstellungsvorgang werden im Systemaudit-Protokoll aufgezeichnet.

Wenn Sie im Fenster **Objektwiederherstellung** nicht **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, öffnet sich das Fenster **Objektwiederherstellung** noch einmal. Verwenden Sie dieses Fenster, um den Speicherort anzugeben, an dem das folgende ausgewählte Objekt wiederhergestellt werden soll (s. Schritt 4 dieser Anleitung).

Dateien aus Backup löschen

So löschen Sie mindestens eine Datei aus Backup:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Wählen Sie den untergeordneten Knoten **Backup** aus.
3. Führen Sie eine der Aktionen durch:
   - Wählen Sie zum Entfernen eines Objekts im Kontextmenü des Objektnamens den Punkt **Löschen** aus.
   - Um mehrere Objekte zu löschen, markieren Sie die entsprechenden Objekte mithilfe der Taste **Strg** oder **Umschalt** die entsprechenden Objekte. Öffnen Sie anschließend das Kontextmenü für eines der gewählten Objekte und wählen Sie den Punkt **Löschen** aus.
4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um die Operation zu bestätigen.

Die ausgewählten Dateien werden aus dem Backup gelöscht.

Backup-Einstellungen anpassen

So passen Sie die Backup-Einstellungen an:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Backup**.
3. Wählen Sie den Menüpunkt **Eigenschaften**.
4. Passen Sie im Fenster **Backup Backups** die Backup-Einstellungen entsprechend an:
   Im Abschnitt **Backup-Einstellungen**:
   - Backup-Ordner
   - Maximale Größe des Backups (MB)
   - Grenzwert für verfügbaren Speicherplatz (MB)

     Überschreitet der Umfang der im Backup befindlichen Objekte die maximale Größe des Backups oder den Grenzwert für den verfügbaren Speicherplatz, so werden Sie von Kaspersky Embedded Systems Security hierüber benachrichtigt, wobei die Objekte jedoch trotzdem ins Backup verschoben werden.

   Im Abschnitt **Einstellungen für die Wiederherstellung von Objekten**:
   - Ordner für die Wiederherstellung von Objekten

5. Klicken Sie auf **OK**.

Die vorgenommenen Backup-Einstellungen werden gespeichert.

Backup-Statistik

In der so genannten Backup-Statistik können Sie Informationen über den aktuellen Status des Backups erhalten.

Um eine Statistik für das Backup anzuzeigen,

öffnen Sie in der Programmkonsolenstruktur das Kontextmenü für den Knoten **Backup** und wählen Sie den Befehl **Statistik**. Das Fenster **Backup-Statistik** wird geöffnet.

Im Fenster **Backup-Statistik** werden Informationen über den aktuellen Status des Backups angezeigt (s. Tabelle unten).

Informationen über den aktuellen Backup-Status

Feld	Beschreibung
Aktuelle Größe des Backups	Datenmenge im Backup-Ordner. Die Größe bezieht sich auf die verschlüsselten Dateien.
Objekte insgesamt	Aktuelle Anzahl der Objekte im Backup

Zugriff auf Netzwerkressourcen blockieren. Blockierte Hosts

In diesem Abschnitt wird beschrieben, wie Remote-Geräte blockiert und die Einstellungen des Speichers der blockierten Hosts konfiguriert werden.

Über den Speicher der blockierten Hosts

Der Speicher der blockierten Hosts wird standardmäßig während der Installation auf einer der folgenden Komponenten installiert: Echtzeitschutz für Dateien, Schutz vor Netzwerkbedrohungen. Diese Komponenten erkennen Versuche auf den Remote-Hosts, Objekte auf dem geschützten Gerät oder ins Netzwerk eingebundener Speicher zu verschlüsseln, zu öffnen oder auszuführen, gemäß der Liste der blockierten Hosts. Informationen über blockierte Hosts auf allen geschützten Geräten werden an das Kaspersky Security Center gesendet. Kaspersky Embedded Systems Security blockiert für alle Remote-Hosts auf der Liste der blockierten Hosts den Zugriff auf die freigegebenen Ordner oder ins Netzwerk eingebundener Speicher des geschützten Geräts.

Der Speicher der blockierten Hosts wird befüllt, wenn zumindest eine der folgenden Aufgaben im aktiven Modus gestartet wird (unter festgelegten Bedingungen):

- Für die Aufgabe "Echtzeitschutz für Dateien": Es wurde eine bösartige Aktivität eines Geräts gefunden, das auf einen freigegebenen Netzwerkordner zugreift, und in den Einstellungen der Aufgabe zum Echtzeitschutz für Dateien ist das Kontrollkästchen **Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen** aktiviert.
- Für die Aufgabe "Schutz vor Netzwerkbedrohung": Die für Netzwerkangriffe typische Aktivität wird erkannt.

Nachdem eine schädliche Aktivität oder ein Verschlüsselungsversuch erkannt wurde, sendet die Aufgabe Informationen über den angreifenden Host an den Speicher der blockierten Hosts, und das Programm erstellt ein Ereignis mit der Ereigniskategorie *Warnung* für die Blockierung des Hosts. Alle Versuche, über diesen Host auf geschützte gemeinsame Netzwerkordner zuzugreifen, werden blockiert.

Falls der lokal eindeutige Identifikator (LUID) des Computers eines angreifenden Hosts auf die Liste mit blockierten Hosts gesetzt wird, ermittelt Kaspersky Embedded Systems Security die IP-Adresse dieses Hosts und fügt diese anstelle des LUID des angreifenden Hosts zur Liste der blockierten Hosts hinzu.

Standardmäßig entfernt Kaspersky Embedded Systems Security blockierte Hosts 30 Minuten, nachdem sie zur Liste hinzugefügt wurden, aus der Liste. Der Zugriff von Computers auf die freigegebenen Netzwerkordner wird automatisch wiederhergestellt, nachdem sie aus der Liste der blockierten Hosts gelöscht wurden. Sie können einen Zeitpunkt angeben, nach dem die blockierten Computer automatisch freigegeben werden.

Beachten Sie, dass der Speicher der blockierten Hosts weiterhin verfügbar ist, wenn Sie für ein beliebiges Benutzerkonto den Zugriff auf die Speicherverwaltung beschränken. Die Einstellungen "Blockierte Hosts" kann nicht geändert werden, es sei denn, das ausgewählte Benutzerkonto verfügt über die Stufe **Änderungsrechte** für die Verwaltung von Kaspersky Embedded Systems Security.

Blockierte Hosts über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Einstellungen für den Speicher der blockierten Hosts über die Benutzeroberfläche des Verwaltungs-Plug-ins anpassen.

Blockieren des Zugriffs auf Netzwerk-Dateiressourcen aktivieren

Damit Sie Computer, die eine Art von schädlicher Aktivität oder Verschlüsselungsaktivität zeigen, zum Speicher für **Blockierte Geräte** hinzufügen und den Zugriff auf freigegebene Netzwerkordner für diese Computer blockieren können, muss zumindest eine der folgenden Aufgaben im aktiven Modus ausgeführt werden:

- Echtzeitschutz für Dateien
- Schutz vor Netzwerkbedrohungen

Aufgabe zum Echtzeitschutz für Dateien anpassen:

1. Öffnen Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Wählen Sie die Registerkarte **Richtlinien** aus und öffnen Sie **<Name der Richtlinie>** > **Echtzeit-Computerschutz** > **Einstellungen** im Block **Echtzeitschutz für Dateien**.

   Das Fenster **Echtzeit-Computerschutz** wird geöffnet.
3. Aktivieren Sie im Block **Integration mit anderen Komponenten** das Kontrollkästchen **Computer, von denen schädliche Aktivitäten ausgehen, in die Liste der nicht vertrauenswürdigen Computer aufnehmen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security den Zugriff auf freigegebene Netzwerkordner für Computer blockiert, bei denen schädliche Aktivitäten festgestellt wurden, während die Aufgabe zum Echtzeitschutz für Dateien läuft.
4. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Aufgabenverwaltung**:

a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.

b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.

5. Klicken Sie im Fenster **Echtzeit-Computerschutz** auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Passen Sie die Aufgabe "Schutz vor Netzwerkbedrohungen" an:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt aus.
6. Klicken Sie auf **Einstellungen** im Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

   Das Fenster **Schutz vor Netzwerkbedrohungen** wird geöffnet.
7. Öffnen Sie die Registerkarte **Allgemein**.
8. In dem Abschnitt **Verarbeitungsmodus** wählen Sie den Verarbeitungsmodus **Verbindungen bei erkanntem Angriff blockieren**.

   Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, zur Liste der blockierten Hosts.

   Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten und fügt die IP-Adressen von Hosts, welche die für Netzwerkangriffe typischen Aktivitäten zeigen, der Liste der blockierten Hosts hinzu.

   Dieser Modus ist standardmäßig eingestellt.

   Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

   Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.
9. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Aufgabenverwaltung**:

   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.

   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.
10. Klicken Sie auf **OK** im Fenster.
11. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Einstellungen für blockierte Geräte anpassen

Um die Einstellungen für den Speicher der blockierten Hosts anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

   Das Fenster **Speichereinstellungen** wird angezeigt.
5. Geben Sie im Abschnitt **Zeitraum für die Blockierung von Hosts** auf der Registerkarte **Speicher der blockierten Hosts** die Anzahl der Tage, Stunden und Minuten an, nach deren Ablauf die blockierten Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.
6. Klicken Sie auf **OK**.

Blockierte Hosts über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Einstellungen für den Speicher der blockierten Hosts über die Benutzeroberfläche der Programmkonsole anpassen.

Blockieren des Zugriffs auf Netzwerk-Dateiressourcen aktivieren

Um Hosts, die schädliche Aktivität oder Verschlüsselungsaktivität zeigen, zum Speicher der **Blockierte Hosts** hinzufügen und den Zugriff auf freigegebene Netzwerkordner für diese Computer blockieren zu können, muss zumindest eine der folgenden Aufgaben im aktiven Modus ausgeführt werden:

- Echtzeitschutz für Dateien
- Schutz vor Netzwerkbedrohungen

Aufgabe zum Echtzeitschutz für Dateien anpassen:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien** aus.
3. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Wählen Sie im Abschnitt **Tief** das Kontrollkästchen **Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security Hosts blockiert, auf denen schädliche Aktivitäten erkannt werden, während die Aufgabe zum Echtzeitschutz für Dateien ausgeführt wird.
5. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Zeitplan**:
   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.
   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.
6. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Passen Sie die Aufgabe "Schutz vor Netzwerkbedrohungen" an:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Schutz vor Netzwerkbedrohungen** aus.
3. Klicken Sie im Detailbereich des Knotens **Eigenschaften** auf den Link **Schutz vor Netzwerkbedrohungen**.
4. Das Fenster **Aufgabeneinstellungen** wird geöffnet.
5. Öffnen Sie die Registerkarte **Allgemein**.
6. In dem Abschnitt **Verarbeitungsmodus** wählen Sie den Verarbeitungsmodus **Verbindungen bei erkanntem Angriff blockieren**.

   Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, zur Liste der blockierten Hosts.

   Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten und fügt die IP-Adressen von Hosts, welche die für Netzwerkangriffe typischen Aktivitäten zeigen, der Liste der blockierten Hosts hinzu.

   Dieser Modus ist standardmäßig eingestellt.

   Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

   Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.
7. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datenverkehrsanalyse nicht stoppen, wenn die Aufgabe nicht ausgeführt wird**.

Ist dieses Kontrollkästchen aktiviert, wenn die Aufgabe zum Schutz vor Netzwerkbedrohungen angehalten wird, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert Netzwerkaktivitäten vom angreifenden Computer abhängig vom ausgewählten Verarbeitungsmodus.

Ist dieses Kontrollkästchen deaktiviert, wenn die Aufgabe "Schutz vor Netzwerkbedrohungen" angehalten wird, untersucht Kaspersky Security für Windows Server den eingehenden Netzwerkverkehr nicht auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

Das Kontrollkästchen ist standardmäßig deaktiviert.

8. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Zeitplan**:
   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.
   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.
9. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Einstellungen für blockierte Geräte anpassen

Um die Einstellungen für den Speicher der blockierten Hosts anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Speicher**.
2. Öffnen Sie das Kontextmenü des Knotens **Blockierte Hosts**.
3. Wählen Sie den Punkt **Eigenschaften** aus.
   Das Fenster **Einstellungen für blockierte Hosts** wird angezeigt.
4. Geben Sie im Abschnitt **Zeitraum für die Blockierung von Hosts** die Anzahl der Tage, Stunden und Minuten an, nach deren Ablauf die blockierten Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.
5. Klicken Sie auf **OK**.
6. Um den Zugriff für alle blockierten Computer wiederherzustellen, gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü des Knotens **Blockierte Hosts**.
   b. Wählen Sie den Punkt **Alle entsperren** aus.
      Alle Computer werden aus der Liste entfernt und entsperrt.
7. Um mehrere Hosts aus der Liste der blockierten Hosts zu löschen, gehen Sie wie folgt vor:
   a. Wählen Sie im Ergebnisbereich in der Liste der blockierten Hosts einen oder mehrere Hosts aus.
   b. Öffnen Sie das Kontextmenü des Knotens **Blockierte Hosts**.
   c. Wählen Sie den Punkt **Auswahl entsperren** aus.
      Die ausgewählten Computer werden entsperrt.

Blockierte Hosts über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Einstellungen für den Speicher der blockierten Hosts über die Benutzeroberfläche des Web-Plug-ins anpassen.

Blockieren von Hosts aktivieren

Damit Sie Computer, die eine Art von schädlicher Aktivität oder Verschlüsselungsaktivität zeigen, zum Speicher für **Blockierte Hosts** hinzufügen und den Zugriff auf freigegebene Netzwerkordner für diese Computer blockieren können, muss zumindest eine der folgenden Aufgaben im aktiven Modus ausgeführt werden:

- Echtzeitschutz für Dateien
- Schutz vor Netzwerkbedrohungen

Aufgabe zum Echtzeitschutz für Dateien anpassen:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**.
6. Wählen Sie im Abschnitt **Integration mit anderen Komponenten** das Kontrollkästchen **Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen**, wenn Sie möchten, dass Kaspersky Embedded Systems Security den Zugriff auf freigegebene Netzwerkordner durch solche Hosts blockiert, auf denen schädliche Aktivitäten erkannt werden, während die Aufgabe zum Echtzeitschutz für Dateien ausgeführt wird.
7. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Aufgabenverwaltung**:
   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.
   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.
8. Klicken Sie auf **Speichern**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Einstellungen für blockierte Geräte anpassen

Um die Einstellungen für den Speicher der blockierten Hosts anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.

4. Wählen Sie den Abschnitt **Zusätzlich**.

5. Klicken Sie im Unterabschnitt **Speicher** auf **Einstellungen**.

6. Klicken Sie im Abschnitt **Zusätzlich** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Speicher**.

   Das Fenster **Speicher** wird angezeigt.

7. Geben Sie im Abschnitt **Zeitraum für die Blockierung von Hosts** auf der Registerkarte **Speicher der blockierten Hosts** die Anzahl der Tage, Stunden und Minuten an, nach deren Ablauf die blockierten Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

8. Klicken Sie auf **OK**.

Registrierung von Ereignissen. Berichte in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält die Informationen über die Arbeit mit den Berichten von Kaspersky Embedded Systems Security: Systemaudit-Protokoll, Bericht über Aufgabenausführung und Ereignisbericht.

Möglichkeiten zur Registrierung der Dienste von Kaspersky Embedded Systems Security

Ereignisse werden in Kaspersky Embedded Systems Security in zwei Gruppen aufgeteilt:

- Ereignisse im Zusammenhang mit der Verarbeitung von Objekten in den Aufgaben von Kaspersky Embedded Systems Security.
- Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security, beispielsweise Programmstart, Erstellen oder Löschen von Aufgaben, Bearbeiten der Aufgabeneinstellungen.

Kaspersky Embedded Systems Security verwendet die folgenden Methoden zum Protokollieren von Ereignissen:

- **Protokolle der Aufgabenausführung**. Ein Protokoll der Aufgabenausführung enthält Informationen über die aktuellen Aufgabenparameter, den aktuellen Aufgabenstatus und Ereignisse, die während der Aufgabenausführung eingetreten sind.
- **Systemaudit-Protokoll**. Das Systemaudit-Protokoll enthält Informationen über Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security.
- **Ereignisbericht**. Das Ereignisprotokoll enthält Informationen über Ereignisse, die für die Crash-Diagnose von Kaspersky Embedded Systems Security erforderlich sind. Der Ereignisbericht ist in der Konsole "Event Viewer" von Microsoft Windows verfügbar.
- **Sicherheitsprotokoll**. Das Sicherheitsprotokoll enthält Informationen über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Gerät verbunden sind.

Wenn bei der Ausführung von Kaspersky Embedded Systems Security ein Problem auftreten sollte (z. B. Kaspersky Embedded Systems Security oder eine bestimmte Aufgabe stürzen ab) und Sie das Problem diagnostizieren möchten, können Sie eine Protokolldatei und eine Dump-Datei für die Prozesse von Kaspersky Embedded Systems Security anlegen und diese Dateien zur Diagnose an den Technischen Support von Kaspersky schicken.

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

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet. Der Ordner, in dem die Dateien gespeichert werden, wird vom Benutzer ausgewählt und durch die Konfiguration des Betriebssystems sowie durch die Einstellungen von Kaspersky Embedded Systems Security verwaltet. Sie können die Zugriffsberechtigungen konfigurieren und nur bestimmten Benutzern den Zugriff auf Protokolle, Trace- und Dump-Dateien erlauben.

Die unter den folgenden Links zum Download verfügbaren Dateien enthalten Tabellen mit allen Ereignissen von Kaspersky Embedded Systems Security für folgende Kategorien:

- Ereignisse, die von Kaspersky Embedded Systems Security in das Ereignisprotokoll geschrieben werden.

  DOWNLOAD KESS-WEL-EVENTS.ZIP

- Ereignisse, die von Kaspersky Embedded Systems Security an den Administrationsserver gesendet werden.

  DOWNLOAD KESS-KSC-EVENTS.ZIP

Systemaudit-Protokoll

Kaspersky Embedded Systems Security führt für Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Embedded Systems Security ein Systemaudit durch. Das Programm sammelt beispielsweise Informationen über den Programmstart, den Start und die Beendigung von Aufgaben in Kaspersky Embedded Systems Security, die Änderung von Aufgabeneinstellungen sowie das Erstellen und Löschen von Aufgaben zur Untersuchung auf Befehl. Einträge zu diesen Ereignissen werden im Ergebnisbereich angezeigt, wenn Sie in der Programmkonsole den Knoten **Systemaudit-Protokoll** auswählen.

Standardmäßig speichert Kaspersky Embedded Systems Security die Ereignisse des Systemaudit-Protokolls für unbegrenzte Zeit. Sie können die Aufbewahrungsdauer der Einträge im Systemaudit-Protokoll anpassen.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Embedded Systems Security die Log-Dateien des Systemaudit-Protokolls speichert.

Ereignisse im Systemaudit-Protokoll sortieren

Standardmäßig werden die Ereignisse im Systemaudit-Protokoll in umgekehrter chronologischer Reihenfolge dargestellt.

Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte außer der Spalte **Ereignis** sortieren.

Um Ereignisse im Systemaudit-Protokoll zu sortieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Systemaudit-Protokoll**.
3. Klicken Sie im Ergebnisbereich auf den Titel der Spalte, nach deren Inhalt die Ereignisse in der Ereignisliste sortiert werden sollen.

Die Ergebnisse der Sortierung bleiben bis zur nächsten Anzeige des Systemaudit-Protokolls erhalten.

Ereignisse im Systemaudit-Protokoll filtern

Sie können im Systemaudit-Protokoll nur die Einträge jener Ereignisse anzeigen, die Ihren Filterkriterien (Filtern) entsprechen.

So filtern Sie Ereignisse im Systemaudit-Protokoll:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.

2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Systemaudit-Protokoll** und wählen Sie den Punkt **Filter**.

   Das Fenster **Filtereinstellungen** wird geöffnet.

3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

   a. Wählen Sie im Feld **Feldname** eine Spalte aus, in der Ereignisse gefiltert werden sollen.

   b. Wählen Sie in der Liste **Operator** die Filterbedingungen aus. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.

   c. Wählen Sie unter **Feldwert** den Filterwert.

   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.

4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.

   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.

5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Filterkriterien für Ereignisse im Systemaudit-Protokoll zu speichern.

   In der Ereignisliste des Systemaudit-Protokolls werden nur Ereignisse angezeigt, die den Filterkriterien entsprechen. Die Filterergebnisse bleiben bis zur nächsten Anzeige des Systemaudit-Protokolls erhalten.

Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.

2. Öffnen Sie das Kontextmenü des untergeordneten Knotens **Systemaudit-Protokoll** und wählen Sie den Punkt **Filter entfernen**.

   In der Ereignisliste des Systemaudit-Protokolls werden alle Ereignisse angezeigt.

Ereignisse aus dem Systemaudit-Bericht löschen

Standardmäßig speichert Kaspersky Embedded Systems Security die Ereignisse des Systemaudit-Protokolls für unbegrenzte Zeit. Sie können die Aufbewahrungsdauer der Einträge im Systemaudit-Protokoll anpassen.

Sie können manuell alle Ereignisse aus dem Systemaudit-Protokoll entfernen.

Um Ereignisse aus dem Systemaudit-Protokoll zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.

2. Öffnen Sie das Kontextmenü des Knotens **Systemaudit-Protokoll** und wählen Sie den Punkt **Leeren**.

3. Führen Sie eine der Aktionen durch:

- Wenn Sie den Inhalt des Systemaudit-Protokolls vor dem Löschen der Ereignisse aus dem Bericht in einer csv-Datei oder txt-Datei speichern möchten, klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Ja**. Geben Sie im folgenden Fenster den Namen und den Speicherort der Datei an.

- Wenn Sie den Inhalt des Berichts nicht in einer Datei speichern möchten, klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Nein**.

Das Systemaudit-Protokoll wird gelöscht.

Protokolle der Aufgabenausführung

Dieser Abschnitt enthält Informationen zu den Protokollen der Aufgabenausführung in Kaspersky Embedded Systems Security sowie Anweisungen für deren Ausführung.

Über Protokolle der Aufgabenausführung

Informationen über die Ausführung von Aufgaben in Kaspersky Embedded Systems Security werden im Ergebnisbereich angezeigt, wenn in der Programmkonsole der Knoten **Protokolle der Aufgabenausführung** ausgewählt ist.

Im Protokoll der Aufgabenausführung können Sie eine Statistik über die Aufgabenausführung, Informationen für alle Objekte, die seit dem Aufgabenstart bis zum aktuellen Zeitpunkt vom Programm verarbeitet wurden, sowie die Aufgabeneinstellungen anzeigen.

Standardmäßig werden Einträge in den Protokollen der Aufgabenausführung von Kaspersky Embedded Systems Security 30 Tage lang ab der Beendigung der Aufgabe aufbewahrt. Sie können die Aufbewahrungsdauer der Einträge in den Berichten über Aufgabenausführung ändern.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Embedded Systems Security die Dateien der Protokolle der Aufgabenausführung speichert. Ferner können Sie die Ereignisse auswählen, über die Kaspersky Embedded Systems Security Einträge in Protokollen der Aufgabenausführung speichert.

Ereignisliste in den Protokollen der Aufgabenausführung anzeigen

Um Protokolle der Aufgabenausführung anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.

2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.

   Die Liste der Ereignisse, die in dem Protokoll der Aufgabenausführung von Kaspersky Embedded Systems Security gespeichert sind, wird im Ereignisbereich angezeigt.

Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte sortieren oder einen Filter anwenden.

Protokolle der Aufgabenausführung sortieren

Standardmäßig werden Protokolle der Aufgabenausführung in umgekehrter chronologischer Reihenfolge dargestellt. Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte sortieren.

Um Protokolle der Aufgabenausführung zu sortieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Klicken Sie im Ergebnisbereich auf den Titel der Spalte, nach deren Inhalt die Protokolle der Aufgabenausführung in Kaspersky Embedded Systems Security sortiert werden sollen.

Die Ergebnisse der Sortierung bleiben bis zur nächsten Anzeige der Protokolle der Aufgabenausführung erhalten.

Protokolle der Aufgabenausführung filtern

Sie können in der Ereignisliste der Protokolle der Aufgabenausführung nur die Protokolle der Aufgabenausführung anzeigen, die Ihren Filterkriterien (Filtern) entsprechen.

Um Protokolle der Aufgabenausführung zu filtern, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des Knotens **Protokolle der Aufgabenausführung** und wählen Sie den Punkt **Filter**.

   Das Fenster **Filtereinstellungen** wird geöffnet.
3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

   a. Wählen Sie im Feld **Feldname** eine Spalte aus, in der Protokolle der Aufgabenausführung gefiltert werden sollen.

   b. Wählen Sie in der Liste **Operator** die Filterbedingungen aus. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.

   c. Wählen Sie unter **Feldwert** den Filterwert.

   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.
4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.
   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Filterkriterien für Ereignisse in den Protokollen der Aufgabeausführung zu speichern.

In der Liste der Protokolle der Aufgabenausführung werden nur Protokolle der Aufgabenausführung angezeigt, die den Filterkriterien entsprechen. Die Filterergebnisse der Sortierung bleiben bis zur nächsten Anzeige der Protokolle der Aufgabenausführung erhalten.

Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Öffnen Sie das Kontextmenü des Knotens **Protokolle der Aufgabenausführung** und wählen Sie den Punkt **Filter entfernen**.

In der Liste der Protokolle der Aufgabenausführung werden alle Protokolle der Aufgabenausführung angezeigt.

Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in den Berichten über Aufgabenausführung anzeigen

In den Protokollen der Aufgabenausführung können Sie detaillierte Informationen über alle Ereignisse, die in den Aufgaben seit ihrem Start aufgetreten sind, sowie eine Statistik über die Aufgabenausführung und die Aufgabeneinstellungen anzeigen.

Um Statistiken und Informationen über eine Aufgabe von Kaspersky Embedded Systems Security in den Berichten über Aufgabenausführung anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Öffnen Sie im Ergebnisfenster das Fenster **Protokolle** auf eine der folgenden Arten:
   - Doppelklicken Sie auf das Protokoll der Aufgabenausführung, das Sie anzeigen möchten.
   - Öffnen Sie das Kontextmenü des Protokolls der Aufgabenausführung, das Sie anzeigen möchten, und wählen Sie den Punkt **Protokoll anzeigen**.
4. Im folgenden Fenster werden folgende Informationen angezeigt:
   - Auf der Registerkarte **Statistik** werden der Startzeit und der Zeitpunkt der Beendigung der Aufgabe sowie deren Statistik angezeigt.
   - Die Registerkarte **Ereignisse** zeigt eine Liste von Ereignissen, die während der Ausführung der Aufgabe aufgetreten sind.
   - Auf der Registerkarte **Einstellungen** werden die Aufgabeneinstellungen angezeigt.
5. Klicken Sie erforderlichenfalls auf die Schaltfläche **Filter**, um die Ereignisse im Protokoll der Aufgabenausführung zu filtern.
6. Klicken Sie erforderlichenfalls auf die Schaltfläche **Export**, um Informationen aus dem Protokoll der Aufgabenausführung in eine csv-Datei oder eine txt-Datei zu exportieren.
7. Klicken Sie auf die Schaltfläche **Schließen**.

Das Fenster **Protokolle** wird geschlossen.

Informationen aus einem Protokoll der Aufgabenausführung exportieren

Sie können Informationen aus dem Protokoll der Aufgabenausführung in eine csv-Datei oder in eine txt-Datei exportieren.

Um Informationen aus dem Protokoll der Aufgabenausführung zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Öffnen Sie im Ergebnisfenster das Fenster **Protokolle** auf eine der folgenden Arten:
   - Doppelklicken Sie auf das Protokoll der Aufgabenausführung, das Sie anzeigen möchten.
   - Öffnen Sie das Kontextmenü des Protokolls der Aufgabenausführung, das Sie anzeigen möchten, und wählen Sie den Punkt **Protokoll anzeigen**.
4. Klicken Sie im unteren Bereich des Fensters **Protokolle** auf die Schaltfläche **Export**.

   Das Fenster **Speichern unter** wird angezeigt.
5. Geben Sie den Namen, den Speicherort, den Typ und die Codierung der Datei an, in die Sie die Information aus dem Protokoll der Aufgabenausführung exportieren möchten.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die vorgenommenen Einstellungen werden gespeichert.

Protokolle der Aufgabenausführung löschen

Standardmäßig werden Einträge in den Protokollen der Aufgabenausführung von Kaspersky Embedded Systems Security 30 Tage lang ab der Beendigung der Aufgabe aufbewahrt. Sie können die Aufbewahrungsdauer der Einträge in den Berichten über Aufgabenausführung ändern.

Sie können bereits abgeschlossene Protokolle der Aufgabenausführung manuell löschen.

Ereignisse aus den Protokollen über Aufgaben, die zum aktuellen Zeitpunkt ausgeführt werden, sowie aus Protokollen, die von anderen Benutzern verwendet werden, können nicht entfernt werden.

Um das Protokoll der Aufgabenausführung zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Protokolle und Benachrichtigungen**.
2. Wählen Sie den untergeordneten Knoten **Protokolle der Aufgabenausführung**.
3. Führen Sie eine der Aktionen durch:
   - Wenn Sie die Protokolle der Aufgabenausführung aller Aufgaben, die bereits abgeschlossen sind, löschen möchten, öffnen Sie das Kontextmenü für den untergeordneten Knoten **Protokolle der Aufgabenausführung** und wählen Sie den Punkt **Leeren**.
   - Wenn Sie das Protokoll einer einzelnen Aufgabe löschen möchten, öffnen Sie im Ergebnisbereich das Kontextmenü des Protokolls der Aufgabenausführung, das Sie löschen möchten, und wählen Sie **Löschen**.
   - Um Protokolle mehrerer Aufgaben zu löschen, gehen Sie wie folgt vor:

a. Wählen Sie im Ergebnisbereich mithilfe der Tasten **Strg** oder **Umschalt** die Protokolle der Aufgabenausführung aus, die Sie leeren möchten.

b. Öffnen Sie das Kontextmenü eines beliebigen ausgewählten Protokolls der Aufgabenausführung und wählen Sie den Punkt **Löschen**.

4. Klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Ja**, um das Löschen zu bestätigen.

Die ausgewählten Protokolle der Aufgabenausführung werden gelöscht. Das Löschen von Protokollen der Aufgabenausführung wird im Systemaudit-Protokoll aufgezeichnet.

Sicherheitsprotokoll

Kaspersky Embedded Systems Security führt ein Sicherheits-Ereignisprotokoll über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Gerät 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 Echtzeit-Computerschutz, 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 ein Systemauditereignis, wenn das Sicherheitsprotokoll geleert wird.

Ereignisbericht von Kaspersky Embedded Systems Security in der Ereignisanzeige anzeigen

Mithilfe des Snap-ins "Ereignisanzeige für Microsoft Management Console" können Sie das Ereignisprotokoll von Kaspersky Embedded Systems Security anzeigen. Darin protokolliert Kaspersky Embedded Systems Security Ereignisse, die für die Crash-Diagnose erforderlich sind.

Sie können auf Grundlage folgender Kriterien Ereignisse auswählen, die im Ereignisprotokoll eingetragen werden sollen:

- **nach Ereignistypen**.
- **nach der Genauigkeitsstufe**. Die Genauigkeitsstufe entspricht der Prioritätsstufe von Ereignissen, die im Bericht registriert werden (informative, wichtige oder kritische Ereignisse). Die Stufe "Informative Ereignisse" bietet die meisten Informationen, da hier die Ereignisse aller Kategorien aufgezeichnet werden. Die Stufe "Kritische Ereignisse" bietet weniger ausführliche Informationen, da hier ausschließlich kritische Ereignisse aufgezeichnet werden.

Um den Ereignisbericht für Kaspersky Embedded Systems Security anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Start**, geben Sie in der Suchzeile den Befehl `mmc` ein und drücken Sie die Taste **EINGABE**.

   Die Microsoft Management Console wird geöffnet.

2. Wählen Sie **Datei** > **Snap-in hinzufügen oder löschen** aus.

   Das Fenster **Snap-in hinzufügen und löschen** wird geöffnet.

3. Wählen Sie aus der Liste der verfügbaren Snap-ins das Snap-in **Ereignisanzeige** aus und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Computer auswählen** wird geöffnet.

4. Geben Sie im Fenster **Computer auswählen** das geschützte Gerät an, auf dem Kaspersky Embedded Systems Security installiert ist, und klicken Sie auf die Schaltfläche **OK**.

5. Klicken Sie im Fenster **Snap-ins hinzufügen/entfernen** auf **OK**.

   In der Struktur der Microsoft Management Console erscheint der Knoten **Ereignisanzeige**.

6. Öffnen Sie in der Konsolenstruktur den Knoten **Ereignisanzeige** und wählen Sie den untergeordneten Knoten **Anwendungs- und Dienstprotokolle** > **Kaspersky Embedded Systems Security** aus.

Der Ereignisbericht für Kaspersky Embedded Systems Security wird geöffnet.

Anpassen der Protokolleinstellungen im Verwaltungs-Plug-in

Sie können folgenden Einstellungen der Protokolle von Kaspersky Embedded Systems Security anpassen:

- Aufbewahrungsdauer der Ereignisse in den Protokollen der Aufgabenausführung und im Systemaudit-Protokoll.
- Pfad des Ordners, in dem Kaspersky Embedded Systems Security die Log-Dateien der Protokolle der Aufgabenausführung und die Systemaudit-Protokolldatei speichert.
- Grenzwerte für Ereignisdarstellung von *Programm-Datenbanken sind veraltet*, *Programm-Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt*.
- Ereignisse, die Kaspersky Embedded Systems Security in den Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisbericht von Kaspersky Embedded Systems Security in der Ereignisanzeige speichert.
- Einstellungen der Veröffentlichung der Audit-Ereignisse und der Ereignisse bei der Aufgabenausführung auf dem syslog-Server über das syslog-Protokoll.

Um die Berichte für Kaspersky Embedded Systems Security anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Knoten **Protokolle und Benachrichtigungen** und wählen Sie den Punkt **Eigenschaften** aus.

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

2. Passen Sie im Fenster **Einstellungen für Protokolle und Benachrichtigungen** die Einstellungen für Protokolle nach Bedarf an. Gehen Sie hierzu wie folgt vor:

   - Wählen Sie auf der Registerkarte **Allgemein** erforderlichenfalls jene Ereignisse aus, die Kaspersky Embedded Systems Security in den Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisprotokoll von Kaspersky Embedded Systems Security in der Ereignisanzeige speichern soll. Gehen Sie hierzu wie folgt vor:

     - Wählen Sie in der Liste **Komponente** die Komponente von Kaspersky Embedded Systems Security, deren Genauigkeitsstufe für Ereignisse Sie festlegen möchten.

Für die Komponenten Echtzeitschutz für Dateien, Untersuchung auf Befehl und Update werden Ereignisse in Protokollen der Aufgabenausführung und im Ereignisprotokoll registriert. Für diese Komponenten enthält die Ereignistabelle die Spalten **Protokoll der Aufgabenausführung** und **Windows-Ereignisprotokoll**. Für die Komponenten Quarantäne und Backup werden die Ereignisse im Systemaudit-Protokoll und im Ereignisbericht protokolliert. Für diese Komponenten enthält die Ereignistabelle die Spalten **Audit** und **Windows-Ereignisprotokoll**.

- Wählen Sie in der Liste **Prioritätsstufe** die Genauigkeitsstufe der Ereignisse in den Protokollen der Aufgabenausführung und im Systemaudit-Protokoll für die ausgewählte Funktionskomponente.

  In der untenstehenden Tabelle der Ereignisliste sind die Kontrollkästchen neben jenen Ereignissen aktiviert, die in Protokollen der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisprotokoll gemäß der ausgewählten Genauigkeitsstufe protokolliert werden.

- Wenn Sie den Eintrag einzelner Ereignisse für die ausgewählte Funktionskomponente manuell aktivieren möchten, gehen Sie wie folgt vor:

a. Wählen Sie in der Liste **Prioritätsstufe** die Option **Benutzerdefiniert** aus.

b. Aktivieren Sie in der Tabelle Ereignisliste die Kontrollkästchen neben jenen Ereignissen, für die Sie den Eintrag in das Protokoll der Aufgabenausführung, im Systemaudit-Protokoll und im Ereignisbericht aktivieren möchten.

- Passen Sie auf der Registerkarte **Erweitert** die Einstellungen der Speicherung von Protokollen und die Grenzwerte für Ereignisdarstellung über den Schutzstatus des Geräts an:
  - Im Abschnitt **Protokoll speichern**:
    - **Ordner für Protokolle**
    - **Protokolle der Aufgabenausführung löschen, die älter sind als (Tage)**
    - **Ereignisse aus dem Systemaudit-Protokoll löschen, die älter sind als (Tage)**
  - Im Abschnitt **Grenzwerte für Ereigniserstellung**:
    - Geben Sie die Anzahl der Tage an, nach deren Ablauf die Ereignisse *Programm-Datenbanken sind veraltet*, *Programm-Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt* eintreten
- Passen Sie auf der Registerkarte **SIEM-Integration** die Einstellungen der Veröffentlichung von Audit-Ereignissen und Ereignissen bei der Aufgabenausführung auf dem syslog-Server an.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Über die SIEM-Integration

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

Ein syslog-Server ist ein externer Server für Ereignis-Management (SIEM), der eingehende Ereignisse speichert und analysiert sowie andere Protokollverwaltungsaktionen ausführt.

Sie können die SIEM-Integration in zwei Modi verwenden:

- Ereignisse auf dem syslog-Server duplizieren: In diesem Modus werden alle Ereignisse der Aufgabenausführung, deren Veröffentlichung in den Protokolleinstellungen konfiguriert wurde, sowie alle Ereignisse des Systemaudits nach dem Versand an SIEM auch weiterhin auf dem geschützten Gerät gespeichert.

  Wir empfehlen, dass Sie diesen Modus verwenden, um die Last für das geschützte Gerät so gering wie möglich zu halten.

- Lokale Kopien der Ereignisse löschen: In diesem Modus werden alle Ereignisse, die während der Programmausführung registriert und in SIEM veröffentlicht wurden, vom geschützten Gerät gelöscht.

  > Das Programm löscht niemals lokale Versionen des Sicherheitsprotokolls.

Kaspersky Embedded Systems Security kann die Ereignisse in den Programmprotokollen in die vom syslog-Server unterstützten Formate konvertieren, damit sie von SIEM-Server empfangen und erfolgreich identifiziert werden können. Das Programm unterstützt die Konvertierung von Ereignissen in ein Format für strukturierte Daten und in das JSON-Format.

Es wird empfohlen, sich bei der Auswahl des Ereignisformats an der Konfiguration des verwendeten SIEM-Servers zu orientieren.

Einstellungen für Zuverlässigkeit

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

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

Kaspersky Embedded Systems Security verwendet Systemaudit-Ereignisse, um Sie über erfolglose Verbindungsversuche zum SIEM-Server und Fehler beim Senden von Ereignissen an den SIEM-Server zu benachrichtigen.

Anpassen der Einstellungen der SIEM-Integration

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

Einstellungen für die SIEM-Integration

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

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

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Protokolle und Benachrichtigungen**.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Einstellungen für Protokolle und Benachrichtigungen** wird geöffnet.
3. Wählen Sie die Registerkarte **SIEM-Integration** aus.
4. Aktivieren Sie im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Ereignisse über das syslog-Protokoll an den externen syslog-Server senden**.
5. Aktivieren Sie bei Bedarf im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen**.

   Der Status des Kontrollkästchens **Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen** beeinflusst nicht die Einstellungen zum Speichern der Ereignisse des Sicherheitsprotokolls: Das Programm löscht niemals automatisch die Ereignisse des Sicherheitsprotokolls.
6. Geben Sie im Abschnitt **Format der Ereignisse** das Format an, in das Sie die Ereignisse bei der Programmausführung für den Versand an den SIEM-Server konvertieren möchten.

   Standardmäßig konvertiert das Programm die Ereignisse in ein Format für strukturierte Daten.
7. Gehen Sie im Abschnitt **Verbindungseinstellungen** wie folgt vor:

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

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

- Aktivieren Sie das Kontrollkästchen **Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist**, wenn Sie möchten, dass das Programm andere Verbindungseinstellungen verwendet, wenn der Versand der Ereignisse an den primären syslog-Server nicht verfügbar ist.

  Geben Sie die folgenden Einstellungen für die Verbindung mit dem zusätzlichen syslog-Server an: **Adresse** und **Port**.

  Die Felder **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 kann nur im Format IPv4 angegeben werden.

8. Klicken Sie auf **OK**.

   Die angepassten Einstellungen der SIEM-Integration werden übernommen.

Über die Konfiguration von Protokollen und Benachrichtigungen

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

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerks, die auf das geschützte Gerät zugreifen, sowie die Terminalbenutzer des geschützten Geräts können Informationen über Ereignisse *Objekt gefunden* erhalten.

Sie können die Ereignisbenachrichtigungen für Kaspersky Embedded Systems Security entweder für ein einzelnes geschütztes Gerät im Fenster **Eigenschaften: <Name des geschützten Geräts>** oder für eine Gruppe von geschützten Geräten im Fenster **Eigenschaften: <Name der Richtlinie>** der ausgewählten Administrationsgruppe anpassen.

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

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

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

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

Protokolleinstellungen anpassen

Um die Berichte für Kaspersky Embedded Systems Security anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

Die vorgenommenen Einstellungen für Berichte werden gespeichert.

Sicherheitsprotokoll

Kaspersky Embedded Systems Security führt ein Sicherheits-Ereignisprotokoll über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Gerät 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 Echtzeit-Computerschutz, 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 ein Systemaudit-Ereignis, wenn das Sicherheitsprotokoll geleert wird.

Anpassen der Einstellungen der SIEM-Integration

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

Ein syslog-Server ist ein externer Server für Ereignis-Management (SIEM), der eingehende Ereignisse speichert und analysiert sowie andere Protokollverwaltungsaktionen ausführt.

Sie können die SIEM-Integration in zwei Modi verwenden:

- Ereignisse auf dem syslog-Server duplizieren: In diesem Modus werden alle Ereignisse der Aufgabenausführung, deren Veröffentlichung in den Protokolleinstellungen konfiguriert wurde, sowie alle Ereignisse des Systemaudits nach dem Versand an SIEM auch weiterhin auf dem geschützten Gerät gespeichert.

  Wir empfehlen, dass Sie diesen Modus verwenden, um die Last für das geschützte Gerät so gering wie möglich zu halten.

- Lokale Kopien der Ereignisse löschen: In diesem Modus werden alle Ereignisse, die während der Programmausführung registriert und in SIEM veröffentlicht wurden, vom geschützten Gerät gelöscht.

  > Das Programm löscht niemals lokale Versionen des Sicherheitsprotokolls.

Kaspersky Embedded Systems Security kann die Ereignisse in den Programmprotokollen in die vom syslog-Server unterstützten Formate konvertieren, damit sie von SIEM-Server empfangen und erfolgreich identifiziert werden können. Das Programm unterstützt die Konvertierung von Ereignissen in ein Format für strukturierte Daten und in das JSON-Format.

Um das Risiko zu minimieren, dass Ereignisse ohne Erfolg an den SIEM-Server weitergeleitet werden, können Sie Einstellungen für den Verbindungsaufbau zu einem zusätzlichen Syslog-Server festlegen.

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 Einstellungen konfigurieren (s. Tabelle unten).

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	Wird nicht verwendet	Sie können die Speicherung lokaler Kopien der Protokolle nach ihrem Versand an den SIEM-Server mithilfe dieses

auf einen externen syslog-Server löschen		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 vom SIEM-Server erfolgreich identifiziert werden können.
Verbindungsprotokoll	TCP	Sie können mithilfe der Dropdown-Liste die Verbindung mit dem primären syslog-Server über die Protokolle UPD oder TCP und mit dem zusätzlichen syslog-Server über das TCP-Protokoll anpassen.
Einstellungen der Verbindung mit dem primären syslog-Server	IP-Adresse: 127.0.0.1 Port: 514	Sie können in den entsprechenden Feldern die Werte für IP-Adresse und Port angeben, um die Verbindung mit dem primären syslog-Server anzupassen. Der Wert der IP-Adresse darf nur im Format IPv4 angegeben werden.
Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist	Wird nicht verwendet	Sie können mithilfe dieses Kontrollkästchens die Verwendung eines syslog-Spiegelservers aktivieren und deaktivieren.
Einstellungen der Verbindung mit dem zusätzlichen syslog-Server	IP-Adresse: 127.0.0.1 Port: 514	Sie können in den entsprechenden Feldern die Werte für IP-Adresse und Port angeben, um die Verbindung mit dem gespiegelten syslog-Server anzupassen. Der Wert der IP-Adresse darf nur im Format IPv4 angegeben werden.

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

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

   Das Fenster **Einstellungen für Protokolle und Benachrichtigungen** wird geöffnet.
5. Wählen Sie die Registerkarte **SIEM-Integration** aus.
6. Aktivieren Sie im Abschnitt **Integrationseinstellungen** das Kontrollkästchen **Ereignisse über das syslog-Protokoll an den externen syslog-Server senden**.

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

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

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

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

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

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

     Die IP-Adresse kann nur im Format IPv4 angegeben werden.
   - Aktivieren Sie das Kontrollkästchen **Zusätzlichen syslog-Server verwenden, wenn der primäre syslog-Server nicht verfügbar ist**, wenn Sie möchten, dass das Programm andere Verbindungseinstellungen verwendet, wenn der Versand der Ereignisse an den primären syslog-Server nicht verfügbar ist.

     Geben Sie die folgenden Einstellungen für die Verbindung mit dem zusätzlichen syslog-Server an: **Adresse** und **Port**.

     Die Felder **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 kann nur im Format IPv4 angegeben werden.

10. Klicken Sie auf **OK**.

Die angepassten Einstellungen der SIEM-Integration werden übernommen.

Benachrichtigungseinstellungen anpassen

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

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:

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

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

4. Klicken Sie im Abschnitt **Protokolle und Benachrichtigungen** im Unterabschnitt **Ereignisbenachrichtigungen** auf die Schaltfläche **Einstellungen**.

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

   - Wählen Sie in der Liste **Benachrichtigungen anpassen** den Benachrichtigungstyp aus, dessen Einstellungen Sie anpassen möchten.

   - Passen Sie im Abschnitt **Benachrichtigung für die Benutzer** die Methode für die Benachrichtigung der Benutzer an. Geben Sie bei Bedarf einen Benachrichtigungstext ein.

   - Passen Sie im Abschnitt **Benachrichtigung für die Administratoren** die Methode für die Benachrichtigung von Administratoren an. Geben Sie bei Bedarf einen Benachrichtigungstext ein. Passen Sie bei Bedarf die erweiterten Benachrichtigungseinstellungen über die Schaltfläche **Einstellungen** an.

   - Geben Sie im Abschnitt **Grenzwerte für Ereigniserstellung** die Zeitintervalle an, nach deren Ablauf Kaspersky Embedded Systems Security die Ereignisse *Programm-Datenbanken sind veraltet*, *Programm-Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt* protokolliert.

     - Programm-Datenbanken sind veraltet (Tage)
     - Programm-Datenbanken sind stark veraltet (Tage)
     - Untersuchung wichtiger Bereiche des Computers wurde lange nicht durchgeführt (Tage)

6. Klicken Sie auf **OK**.

Die festgelegten Benachrichtigungseinstellungen werden gespeichert.

Konfigurieren der Interaktion mit dem Administrationsserver

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

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

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

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

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

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

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

   - Quarantäneobjekte.
   - Objekte im Backup.

6. Klicken Sie auf **OK**.

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

Benachrichtigungen anpassen

Dieser Abschnitt enthält Informationen über Möglichkeiten zur Benachrichtigung von Benutzern und Administratoren von Kaspersky Embedded Systems Security über Programmereignisse und den Schutzstatus des Geräts sowie Anleitungen zur Anpassung von Benachrichtigungen.

Methoden zur Benachrichtigung von Administrator und Benutzer

Sie können die Benachrichtigung des Administrators und der Benutzer, die auf das Gerät zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Embedded Systems Security und dem Status des Antiviren-Schutzes auf dem Gerät zusammenhängen, anpassen.

Das Programm gewährleistet die Ausführung folgender Aufgaben:

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerks, die auf das geschützte Gerät zugreifen, sowie die Terminalbenutzer des Servers können Informationen über Ereignisse des Typs *Objekt gefunden* erhalten, die in der Aufgabe "Echtzeitschutz für Dateien" auftreten.

In der Programmkonsole können Sie die Benachrichtigungen für den Administrator oder die Benutzer auf unterschiedliche Weise aktivieren:

- Methoden für die Benachrichtigung der Benutzer:
  a. Werkzeuge für Terminaldienst.

     Sie können diese Methode für die Benachrichtigung von Terminalserverbenutzer anwenden, wenn das geschützte Gerät ein Terminalserver ist.

  b. Werkzeuge für den Windows Messenger Dienst.

     Sie können diese Methode für die Benachrichtigung über den Windows Messenger Dienst anwenden.

- Methoden für Benachrichtigung von Administratoren:
  a. Werkzeuge für den Windows Messenger Dienst.

     Sie können diese Methode für die Benachrichtigung über den Windows Messenger Dienst anwenden.

  b. Starten einer ausführbaren Datei.

     Mit dieser Methode wird eine ausführbare Datei ausgeführt, die auf einem lokalen Laufwerk auf einem geschützten Gerät gespeichert ist, wenn ein Ereignis auftritt.

  c. Per E-Mail senden.

     Diese Methode dient der Zustellung von Nachrichten per E-Mail-Nachricht.

Sie können den Text einer Nachricht verfassen, um individuelle Ereignistypen zu erstellen. In den Text können Sie Felder mit Informationen zum Ereignis aufnehmen. Standardmäßig wird für die Benachrichtigung von Benutzern ein Standard-Nachrichtentext verwendet.

Benachrichtigungen an Administrator und Benutzer anpassen

Sollen Benachrichtigungen über Ereignisse eingestellt werden, müssen zunächst die Art der Benachrichtigung und der Inhalt der Textnachricht festgelegt sein.

So konfigurieren Sie die Benachrichtigungseinstellungen von Ereignissen:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü für den Knoten **Protokolle und Benachrichtigungen** und wählen Sie den Punkt **Eigenschaften** aus.

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

2. Geben Sie auf der Registerkarte **Benachrichtigungen** den Modus der Benachrichtigungen an:

   a. Wählen Sie in der Liste **Ereignistyp** das Ereignis aus, für das Sie eine Benachrichtigungsmethode festlegen möchten.

   b. Aktivieren Sie in der Parametergruppe **Benachrichtigung für die Administratoren** oder **Benachrichtigung für die Benutzer** das Kontrollkästchen für die Benachrichtigungsarten, die Sie verwenden möchten.

   > Sie können Benutzerbenachrichtigungen nur für folgende Ereignisse konfigurieren: **Objekt gefunden**, **Nicht vertrauenswürdiges externes Gerät erkannt und eingeschränkt** und **Host wurde der Liste der nicht vertrauenswürdigen Hosts hinzugefügt**.

3. Um einen Benachrichtigungstext zu erstellen, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Text der Nachricht**.

   b. Geben Sie im nächsten Fenster den Text ein, der in der Benachrichtigung über das Ereignis angezeigt werden soll.

   > So können Sie den gleichen Nachrichtentext für mehrere Ereignistypen festlegen: Wählen Sie zuerst die Benachrichtigungsmethode für einen Ereignistyp aus. Markieren Sie dann mithilfe der Tasten **Strg** oder **Umschalt** die übrigen Ereignistypen, für die Sie den gleichen Nachrichtentext festlegen möchten. Klicken Sie erst dann auf die Schaltfläche **Text der Nachricht**.

   a. Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Makros** und wählen Sie die entsprechenden Punkte in der Dropdown-Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   b. Um den standardmäßigen Benachrichtigungstext für ein Ereignis wiederherzustellen, klicken Sie auf die Schaltfläche **Standard**.

4. Um Administrator-Benachrichtigungsarten für das ausgewählte Ereignis anzupassen, wählen Sie die Registerkarte **Einstellungen** aus, klicken Sie auf die Schaltfläche **Benachrichtigungen** im Abschnitt **Benachrichtigung für die Administratoren** und passen Sie im Fenster **Erweiterte Einstellungen** die ausgewählten Einstellungen an. Gehen Sie hierzu wie folgt vor:

   a. Für Benachrichtigungen, die per E-Mail erfolgen sollen, öffnen Sie die Registerkarte **E-Mail** und tragen in die entsprechenden Felder die E-Mail-Adressen der Empfänger (durch Semikolon getrennt), den Namen oder die Netzwerkadresse des SMTP-Servers sowie dessen Port ein. Tragen Sie bei Bedarf den Text ein, der in den Feldern **Betreff** und **Von** angezeigt werden soll. In den Text des Feldes **Betreff** können auch Variable mit Informationen über Ereignisse aufgenommen werden (s. Tabelle unten).

      Wenn Sie bei der Verbindung mit einem SMTP-Server die Authentifizierung für Benutzerkonten verwenden möchten, aktivieren Sie in der Gruppe **Einstellungen für die Authentifizierung** das Kontrollkästchen **SMTP-Authentifizierung verwenden** und tragen Sie Name und Kennwort des Benutzers ein, dessen Benutzerkonto geprüft werden soll.

b. Damit Benachrichtigung über den Windows Messenger Dienst erfolgen, erstellen Sie auf der Registerkarte **Windows Messenger Dienst** eine Liste der geschützten Geräte, die Benachrichtigungen erhalten sollen: Klicken Sie für jedes geschützte Gerät, das Sie hinzufügen möchten, auf **Hinzufügen** und tragen Sie im Eingabefeld den entsprechenden Netzwerknamen ein.

c. Um eine ausführbare Datei zu starten, wählen Sie auf der Registerkarte **Ausführbare Datei** eine Datei auf einem lokalen Laufwerk des geschützten Geräts aus, die nach Eintreten des Ereignisses auf dem geschützten Gerät ausgeführt werden soll, oder geben Sie den vollständigen Pfad der Datei auf der Registerkarte an. Tragen Sie Name und Kennwort des Benutzers ein, unter dessen Benutzerkonto die Datei ausgeführt werden soll.

   Wenn Sie den Pfad einer ausführbaren Datei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable können hingegen nicht verwendet werden.

   Wenn Sie die Anzahl der Benachrichtigungen eines Ereignistyps innerhalb eines bestimmten Zeitraums begrenzen möchten, aktivieren Sie auf der Registerkarte **Erweitert** das Kontrollkästchen **Die gleiche Benachrichtigung senden höchstens** und legen Sie eine Anzahl und ein Zeitintervall fest.

5. Klicken Sie auf **OK**.

Die festgelegten Benachrichtigungseinstellungen werden gespeichert.

Felder mit Informationen über Ereignisse

Variable	Beschreibung
%EVENT_TYPE%	Ereignistyp.
%EVENT_TIME%	Zeitpunkt, zu dem ein Ereignis eingetreten ist.
%EVENT_SEVERITY%	Prioritätsstufe.
%OBJECT%	Name des Objekts (in den Aufgaben zum Echtzeit-Computerschutz und zur Untersuchung auf Befehl). In der Aufgabe Update der Programm-Module steht der Name des Updates und die Adresse der Internetseite mit näheren Angaben zum Update.
%VIRUS_NAME%	Name des Objekts gemäß der Klassifizierung der Viren-Enzyklopädie. Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Embedded Systems Security beim Fund eines Objekts zurückgibt. Den vollständigen Namen des gefundenen Objekts finden Sie im Protokoll der Aufgabenausführung.
%VIRUS_TYPE%	Typ des gefundenen Objekts gemäß der Klassifizierung von Kaspersky, beispielsweise "Virus" oder "Trojaner". Gehört zur vollständigen Bezeichnung eines gefundenen Objekts, die Kaspersky Embedded Systems Security zurückgibt, nachdem ein Objekt als infiziert oder möglicherweise infiziert eingestuft wurde. Den vollständigen Namen des gefundenen Objekts finden Sie im Protokoll der Aufgabenausführung.
%USER_COMPUTER%	In der Aufgabe zum Echtzeitschutz für Dateien ist das der Name des geschützten Geräts für den Benutzer, der auf das Objekt auf dem Gerät zugegriffen hat.
%USER_NAME%	In der Aufgaben zum Echtzeitschutz für Dateien ist das der Name des Benutzers, der auf das Objekt auf dem Gerät zugegriffen hat.
%FROM_COMPUTER%	Name des geschützten Geräts, von dem die Benachrichtigung geschickt wurde.
%EVENT_REASON%	Grund für Eintreten eines Ereignisses (Dieses Feld ist für bestimmte Ereignisse nicht verfügbar).
%ERROR_CODE%	Fehlercode (nur das Ereignis "Interner Aufgabenfehler").
%TASK_NAME%	Aufgabenname (nur für Ereignisse, die mit der Aufgabenausführung verbunden

	sind).

Starten und Beenden von Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zum Start der Programmkonsole sowie zum Start und zum Beenden von Kaspersky Security Service.

Verwaltungs-Plug-in für Kaspersky Embedded Systems Security starten

In Kaspersky Security Center sind für den Start des Verwaltungs-Plug-ins für Kaspersky Embedded Systems Security keine weiteren Aktionen erforderlich. Nach der Installation des Plug-ins auf dem geschützten Gerät 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*.

Konsole für Kaspersky Embedded Systems Security aus dem Startmenü starten

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

*So öffnen Sie die Programmkonsole über das **Startmenü**:*

1. Wählen Sie im **Startmenü Programme** > **Kaspersky Embedded Systems Security** > **Administrations-Tools** > **Konsole für Kaspersky Embedded Systems Security**.

Wenn Sie planen, andere Snap-ins zur Programmkonsole hinzuzufügen, starten Sie die Programmkonsole im Autorenmodus.

So starten Sie die Programmkonsole im Autorenmodus:

1. Wählen Sie im **Startmenü Programme** > **Kaspersky Embedded Systems Security** > **Administrations-Tools** aus.
2. Wählen Sie im Kontextmenü der Programmkonsole den Befehl **Autor**.

   Die Programmkonsole wird im Autorenmodus gestartet.

Wenn die Programmkonsole auf dem geschützten Gerät gestartet wurde, wird das Fenster der Programmkonsole geöffnet.

Wenn Sie die Programmkonsole auf einem nicht geschützten Gerät gestartet haben, stellen Sie eine Verbindung mit dem geschützten Gerät her.

Gehen Sie wie folgt vor, um eine Verbindung mit dem geschützten Gerät herzustellen:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.
2. Wählen Sie den Befehl **Verbindung mit anderem Computer herstellen** aus.

   Das Fenster **Geschütztes Gerät auswählen** wird geöffnet.
3. Wählen Sie im folgenden Fenster **Anderes Gerät** aus.

4. Geben Sie im Eingabefeld den Netzwerknamen des geschützten Geräts ein.

5. Klicken Sie auf **OK**.

Die Programmkonsole wird mit dem geschützten Gerät verbunden.

Wenn das Benutzerkonto, mit dem Sie sich bei Microsoft Windows angemeldet haben, nicht über die erforderlichen Rechte für den Zugriff auf den Dienst zur Verwaltung von Kaspersky Security Management Service auf dem geschützten Gerät verfügt, aktiveren Sie das Kontrollkästchen **Verbindung mit Rechten des folgenden Benutzerkontos herstellen** und geben Sie ein anderes Benutzerkonto an, das über die entsprechenden Rechte verfügt.

Kaspersky Security Service starten und anhalten

Standardmäßig wird Kaspersky Security Service automatisch unmittelbar nach dem Hochfahren des Betriebssystems gestartet. Kaspersky Security Service verwaltet die Programmprozesse, welche die Aufgaben zum Echtzeit-Computerschutz, zur Computer-Kontrolle, zur Untersuchung auf Befehl und zum Update ausführen.

Beim Start von Kaspersky Embedded Systems Security werden standardmäßig folgende Aufgaben gestartet: Echtzeitschutz für Dateien, Untersuchung beim Hochfahren des Betriebssystems, sowie andere Aufgaben, für deren Zeitplan die Startfrequenz **Bei Programmstart** gilt.

Wenn Sie den Dienst von Kaspersky Security Service beenden, werden alle laufenden Aufgaben beendet. Nachdem Sie Kaspersky Security Service neu gestartet haben, startet das Programm nur jene Aufgaben automatisch, bei denen im Zeitplan das Startintervall **Bei Programmstart** festgelegt ist; die anderen Aufgaben müssen manuell gestartet werden.

Sie können den Dienst Kaspersky Security Service über das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens oder mithilfe des Snap-Ins Dienste von Microsoft Windows starten und beenden.

Sie können Kaspersky Embedded Systems Security starten und beenden, wenn Sie auf dem geschützten Gerät zur Gruppe "Administratoren" gehören.

So starten oder beenden Sie das Programm mithilfe der Programmkonsole:

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.

Start der Komponenten von Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems

Dieser Abschnitt enthält Informationen zu Kaspersky Embedded Systems Security bei der Ausführung im abgesicherten Modus des Betriebssystems.

Über Kaspersky Embedded Systems Security im abgesicherten Modus des Betriebssystems

Die Komponenten von Kaspersky Embedded Systems Security können beim Laden des Betriebssystems im abgesicherten Modus gestartet werden. Zusätzlich zu dem Kaspersky Security Service (kavfs.exe) wird auch der Treiber "klam.sys" geladen. Er wird verwendet, um den Kaspersky Security Service beim Hochfahren des Betriebssystems als geschützten Dienst zu registrieren. Ausführliche Informationen finden Sie im Abschnitt Kaspersky Security Service als geschützten Dienst registrieren.

Kaspersky Embedded Systems Security kann in den folgenden abgesicherten Modi des Betriebssystems gestartet werden:

- Minimaler abgesicherter Modus – Dieser Modus wird gestartet, wenn die Standardoption für den abgesicherten Modus ausgewählt wird. Kaspersky Embedded Systems Security kann bei Auswahl dieser Option die folgenden Komponenten starten:
  - Echtzeitschutz für Dateien
  - Untersuchung auf Befehl
  - Kontrolle des Programmstarts und Erstellen von Regeln für die Kontrolle des Programmstarts
  - Protokollanalyse
  - Überwachung der Datei-Integrität
  - Überwachung der Baseline-Integrität
  - Integritätsprüfung für Programme

Abgesicherter Modus mit Netzwerktreibern – In diesem Modus wird das Betriebssystem im abgesicherten Modus mit Netzwerktreibern geladen. Zusätzlich zu den im minimalen abgesicherten Modus startenden Komponenten kann Kaspersky Embedded Systems Security die folgenden Komponenten in diesem Modus starten:

- Update der Programm-Datenbanken
- Update der Programm-Module

Kaspersky Embedded Systems Security im abgesicherten Modus starten

Standardmäßig wird Kaspersky Embedded Systems Security nicht gestartet, wenn das Betriebssystem im abgesicherten Modus geladen wird.

So starten Sie Kaspersky Embedded Systems Security im abgesicherten Modus:

1. Starten Sie den Windows-Registrierungs-Editor (C:\Windows\regedit.exe).
2. Öffnen Sie den Schlüssel [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] der Systemregistrierung.
3. Öffnen Sie den Parameter "LoadInSafeMode".

4. Legen Sie den Wert auf `1` fest.

5. Klicken Sie auf **OK**.

So brechen Sie den Start von Kaspersky Embedded Systems Security im abgesicherten Modus ab:

1. Starten Sie den Windows-Registrierungs-Editor (C:\Windows\regedit.exe).

2. Öffnen Sie den Schlüssel [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] der Systemregistrierung.

3. Öffnen Sie den Parameter "LoadInSafeMode".

4. Setzen Sie den Wert auf `0`.

5. Klicken Sie auf **OK**.

Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zu den Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security.

Über die Selbstverteidigungsmechanismen in Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security beinhaltet Selbstverteidigungsmechanismen, die das Programm davor schützt, dass Ordner, Speicherprozesse und Einträge in der Systemregistrierung gelöscht oder geändert werden.

Schutz vor Änderungen an Ordnern mit installierten Komponenten von Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security blockiert das Umbenennen und Löschen von Ordnern mit den installierten Programmkomponenten durch jedes Benutzerkonto. Standardmäßig lauten die Pfade zu den Installationsordnern des Programms wie folgt:

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

Schutz vor Änderungen der Registrierungsschlüssel von Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security beschränkt den Zugriff auf die folgenden Zweige und Schlüssel der Registrierung, die das Laden von Treibern und Diensten des Programms ermöglichen:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1] (auf der 64-Bit-Version von Microsoft Windows)
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\Trace]

Die Rechte zum Ändern dieser Registrierungszweige und -schlüssel werden lediglich dem Konto "Lokales System" (SYSTEM) gewährt. Die Konten "Benutzer" und "Administrator" verfügen nur über Leseberechtigung.

Schutz vor Veränderungen im Speicher der Prozesse des Programms

Um die Prozesse des Programms gegen Prozesse von Dritten zu schützen, blockiert Kaspersky Embedded Systems Security den Zugriff auf die folgenden ausführbare Dateien:

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

Der Zugriff durch Prozesse von Dritten auf den Speicher von Prozessen von Kaspersky Embedded Systems Security wird standardmäßig blockiert.

Sie können die Funktionen zum Selbstschutz in den Richtlinieneinstellungen der Kaspersky Embedded Systems Security Console und dem Verwaltungs-Plug-in für Kaspersky Embedded Systems Security aktivieren.

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 Gerät ein Treiber für den *frühen Start der Antischadsoftware* installiert sein.

Ein Treiber für den *frühen Start der Antischadsoftware* (auch "ELAM" genannt) schützt die Geräte in Ihrem Netzwerk beim Start und vor der Initialisierung der Drittanbietertreiber.

Der ELAM-Treiber wird automatisch während der Installation von Kaspersky Embedded Systems Security installiert und wird für die Registrierung von Kaspersky Security Service als PPL beim Start des Betriebssystems verwendet. Wenn Kaspersky Security Service (KAVFS) als systemgeschützter Prozess gestartet wird, können andere nicht geschützte Prozesse keine Threads einschleusen, nicht in den virtuellen Speicher des geschützten Prozesses schreiben und den Dienst nicht anhalten.

Wenn ein Prozess als PPL gestartet wird, kann er unabhängig von den zugewiesenen Benutzerberechtigungen nicht von Benutzern verwaltet werden. Die Registrierung von Kaspersky Security Service als PPL mittels ELAM-Treiber wird von den Betriebssystemen Microsoft Windows 10 und höher unterstützt. Wenn Sie Kaspersky Embedded Systems Security auf einem Server installieren, auf dem ein Betriebssystem mit PPL-Unterstützung läuft, steht die Berechtigungsverwaltung für Kaspersky Security Service (KAVFS) nicht zur Verfügung.

Um Kaspersky Embedded Systems Security als PPL zu installieren, führen Sie folgenden Befehl aus:

```
msiexec /i ess_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security

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

Über Rechte zur Verwaltung von Kaspersky Embedded Systems Security

Standardmäßig haben die Benutzer der Gruppe "Administratoren" auf dem geschützten Gerät und die Benutzer der Gruppe der ESS-Administratoren, die auf einem geschützten Gerät bei der Installation von Kaspersky Embedded Systems Security erstellt wird, und die Gruppe "SYSTEM" Zugriff auf alle Funktionen von Kaspersky Embedded Systems Security.

Benutzer mit der Zugriffsstufe "Rechte ändern" für Kaspersky Embedded Systems Security können auch anderen Benutzern, die am geschützten Gerät registriert sind oder zur Domäne gehören, den Zugriff auf Funktionen von Kaspersky Embedded Systems Security gewähren.

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

Sie können für einen Benutzer oder eine Benutzergruppe eine der folgenden vordefinierten Zugriffsstufen auswählen:

- **Vollständige Kontrolle** – Zugriff auf alle Programmfunktionen: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Embedded Systems Security, der Komponenteneinstellungen, der Rechte von Benutzern von Kaspersky Embedded Systems Security, sowie Anzeigen der Statistik für Kaspersky Embedded Systems Security.

- **Änderung** – Zugang zu allen Programmfunktionen mit Ausnahme der Veränderung der Benutzerrechte: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Embedded Systems Security und der Einstellungen der Komponenten von Kaspersky Embedded Systems Security.

- **Lesen** – Anzeigen der allgemeinen Einstellungen von Kaspersky Embedded Systems Security, der Einstellungen der Komponenten von Kaspersky Embedded Systems Security, der Statistik für Kaspersky Embedded Systems Security und der Benutzerrechte für Kaspersky Embedded Systems Security.

Sie können ferner erweiterte Zugriffsberechtigungen anpassen: Zugriff auf bestimmte Funktionen von Kaspersky Embedded Systems Security erlauben oder verweigern.

Wenn Sie die Zugriffsrechte für einen Benutzer oder eine Gruppe manuell konfiguriert haben, so wird für diesen Benutzer bzw. diese Gruppe die Zugriffsstufe **Sonderrechte** festgelegt.

Über Zugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security

Zugriffsrechte	Beschreibung
Aufgabenverwaltung	Berechtigung zum Starten, Beenden, Anhalten bzw. Fortsetzen der Aufgaben von Kaspersky Embedded Systems Security.
Erstellen und Löschen von Aufgaben zur Untersuchung auf	Berechtigung zum Erstellen und Löschen von Aufgabe zur Untersuchung auf Befehl.

Befehl	
Ändern von Parametern	Berechtigungen: • Einstellungen von Kaspersky Embedded Systems Security aus einer Konfigurationsdatei importieren • Programmeinstellungen bearbeiten
Lesen von Parametern	Berechtigungen: • Allgemeine Einstellungen und Aufgabeneinstellungen für Kaspersky Embedded Systems Security anzeigen. • Exportieren der Einstellungen von Kaspersky Embedded Systems Security in eine Konfigurationsdatei. • Einstellungen für Protokolle der Aufgabenausführung, für das Systemaudit-Protokoll und für Benachrichtigungen anzeigen.
Datenverwaltung verwalten	Berechtigungen: • Objekte in Quarantäne verschieben • Objekte aus der Quarantäne und dem Backup löschen • Objekte aus der Quarantäne und dem Backup wiederherstellen
Verwaltung von Berichten	Berechtigung zum Löschen von Protokollen der Aufgabenausführung und zum Leeren des Systemaudit-Protokolls
Lesen von Berichten	Berechtigung zur Anzeige der Ereignisse von Anti-Virus in Protokollen der Aufgabenausführung und im Systemaudit-Protokoll.
Lesen der Statistik	Berechtigung zum Anzeigen der Statistik für die einzelnen Aufgaben von Kaspersky Embedded Systems Security.
Lizenzverwaltung für das Programm	Berechtigung zum Aktivieren von Kaspersky Embedded Systems Security.
Programm entfernen	Berechtigung zum Deinstallieren von Kaspersky Embedded Systems Security.
Lesen von Benutzerrechten	Berechtigung zum Anzeigen der Liste der Benutzer von Kaspersky Embedded Systems Security und der Benutzerzugriffsrechte.
Ändern von Rechten	Berechtigungen: • Liste der Benutzer ändern, die Zugriff auf die Programmverwaltung haben • Benutzerzugriffsrechte für die Funktionen von Kaspersky Embedded Systems Security bearbeiten

Über die Rechte zur Verwaltung von registrierten Diensten

Während der Installation registriert Kaspersky Embedded Systems Security in Windows den Dienst Kaspersky Security Service (KAVFS), den Programmverwaltungsdienst Kaspersky Security Management Service (KAVFSGT) in Windows und Kaspersky Security Exploit-Prävention (KAVFSSLP).

Die Registrierung von Kaspersky Security Service als Protected Process Light mittels ELAM-Treiber wird von den Betriebssystemen Microsoft Windows 10 und höher unterstützt. Wenn ein Prozess als PPL gestartet wird, kann er unabhängig von den zugewiesenen Benutzerberichten nicht von Benutzern verwaltet werden. Wenn Sie Kaspersky Embedded Systems Security auf einem geschützten Gerät installieren, auf dem ein Betriebssystem mit PPL-Unterstützung läuft, steht die Berechtigungsverwaltung für Kaspersky Security Service (KAVFS) nicht zur Verfügung.

Kaspersky Security Service

Standardmäßig haben diejenigen Benutzer Zugriff auf die Verwaltung von Kaspersky Security Service, die auf dem geschützten Gerät der Administratoren-Gruppe angehören, sowie die Systemgruppen "SERVICE" und "INTERACTIVE" mit Leserechten und die Systemgruppe "SYSTEM" mit Rechten zum Lesen und Ausführen.

Benutzer mit Zugriff der Stufe "Rechte ändern" können anderen Benutzern, die auf dem geschützten Gerät registriert sind oder zur Domäne gehören, Zugriff auf die Verwaltung von Kaspersky Security Service gewähren.

Dienst von Kaspersky Security Management Service

Zur Verwaltung des Programms über die auf einem anderen geschützten Gerät installierte Programmkonsole muss das Benutzerkonto, mit dessen Rechten die Verbindung zu Kaspersky Embedded Systems Security hergestellt wird, unbeschränkten Zugriff auf Kaspersky Security Management Service auf dem geschützten Gerät haben.

Folgende Benutzer besitzen standardmäßig Zugriff zur Verwaltung von Kaspersky Security Management Service: Benutzer, die auf dem geschützten Gerät zur Gruppe "Administratoren" gehören, und Benutzer der Gruppe der ESS-Administratoren, die bei der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät erstellt wird.

Sie können Kaspersky Security Management Service nur über das Snap-In Dienste von Microsoft Windows verwalten.

Kaspersky Security-Exploit-Prävention

Standardmäßig haben diejenigen Benutzer Zugriff auf die Verwaltung von Kaspersky Security Exploit Prevention Service, die der Gruppe "Administratoren" auf dem geschützten Gerät angehören, sowie der Systemgruppe "SYSTEM" mit Rechten zum Lesen und Ausführen.

Über Zugriffsrechte für Kaspersky Security Management Service

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

Während der Installation registriert Kaspersky Embedded Systems Security den Dienst Kaspersky Security Management Service (KAVFSGT). Zur Verwaltung des Programms über die auf einem anderen Computer installierte Programmkonsole muss das Benutzerkonto, das für die Verbindung zu Kaspersky Embedded Systems Security verwendet wird, unbeschränkten Zugriff auf Kaspersky Security Management Service auf dem geschützten Gerät haben.

Folgende Benutzer besitzen standardmäßig Zugriff zur Verwaltung von Kaspersky Security Management Service: Benutzer, die auf dem geschützten Gerät zur Gruppe "Administratoren" gehören, und Benutzer der Gruppe der ESS-Administratoren, die bei der Installation von Kaspersky Embedded Systems Security auf dem geschützten Gerät erstellt wird.

Sie können Kaspersky Security Management Service nur über das Snap-In Dienste von Microsoft Windows verwalten.

Sie können den Benutzerzugriff auf Kaspersky Security Management Service nicht durch Anpassen von Kaspersky Embedded Systems Security erlauben oder verweigern.

Sie können unter dem lokalen Benutzerkonto eine Verbindung mit Kaspersky Embedded Systems Security herstellen, wenn auf dem geschützten Gerät ein Konto mit dem gleichen Benutzernamen und dem gleichen Kennwort registriert ist.

Über die Rechte zur Verwaltung des Dienstes Kaspersky Security Service

Bei der Installation registriert Kaspersky Embedded Systems Security in Windows den Dienst Kaspersky Security Service (KAVFS) und aktiviert intern die funktionellen Komponenten, die beim Hochfahren des Betriebssystems gestartet werden. Um die Gefahr des Zugriffs Unbefugter auf die Programmfunktionen und Sicherheitseinstellungen auf einem geschützten Gerät über die Verwaltung von Kaspersky Security Service zu reduzieren, können Sie die Rechte zur Verwaltung von Kaspersky Security Service mithilfe der Programmkonsole oder des Verwaltungs-Plug-ins beschränken.

Standardmäßig werden die Zugriffsrechte für die Verwaltung von Kaspersky Security Service Benutzern in der Gruppe "Administratoren" auf dem geschützten Gerät gewährt. Leserechte werden den Gruppen "SERVICE" und "INTERACTIVE" erteilt, Lese- und Ausführungsrechte werden der Gruppe "SYSTEM" gewährt.

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

Benutzer, die Zugriff auf Funktionen haben, welche Änderungsrechte erfordern, können anderen Benutzern, die auf dem geschützten Gerät registriert sind oder zur Domäne gehören, Zugriff auf die Verwaltung von Kaspersky Security Service gewähren.

Sie können für einen Benutzer oder eine Benutzergruppe von Kaspersky Embedded Systems Security eine der folgenden vordefinierten Rechtestufen für die Verwaltung von Kaspersky Security Service auswählen:

- **Vollständige Kontrolle** – Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Security Service sowie zum Starten und Beenden von Kaspersky Security Service.
- **Lesen** – Berechtigung zum Aufrufen der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
- **Änderung** – Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
- **Ausführung** – Berechtigung zum Starten und Beenden von Kaspersky Security Service.

Außerdem können Sie erweiterte Einstellungen für die Zugriffsrechte vornehmen: Zugriff auf bestimmte Funktionen von Kaspersky Embedded Systems Security erlauben oder verbieten (siehe Tabelle unten).

Wenn Sie die Zugriffsrechte für einen Benutzer oder eine Gruppe manuell konfiguriert haben, so wird für diesen Benutzer bzw. diese Gruppe die Zugriffsstufe **Sonderrechte** festgelegt.

Zugriffsrechte für Kaspersky Security Service-Funktionen

Funktion	Beschreibung
Einstellungen des Dienstes lesen	Berechtigung zum Anzeigen der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
Status des Dienstes beim Service Control Manager abfragen	Berechtigung zur Abfrage des Ausführungsstatus von Kaspersky Security Service beim Service Control Manager von Microsoft Windows
Status beim Dienst abfragen	Berechtigung zur Abfrage des Ausführungsstatus des Dienstes bei Kaspersky Security Service.
Liste der abhängigen Dienste auslesen	Berechtigung zum Aufruf einer Liste der Dienste, von denen Kaspersky Security Service abhängt, sowie der Dienste, die von Kaspersky Security Service abhängen.
Einstellungen des Dienstes anpassen	Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
Dienst starten	Berechtigung zum Starten von Kaspersky Security Service.
Dienst beenden	Berechtigung zum Beenden von Kaspersky Security Service.
Dienst anhalten / fortsetzen	Berechtigung zum Anhalten und Fortsetzen von Kaspersky Security Service.
Lesen von Benutzerrechten	Berechtigung zum Anzeigen der Benutzerlisten von Kaspersky Security Service und der Zugriffsrechte der einzelnen Benutzer
Ändern von Rechten	Berechtigungen: • Benutzer von Kaspersky Security Service hinzufügen und löschen. • Zugriffsrechte der Benutzer auf Kaspersky Security Service ändern.
Dienst entfernen	Berechtigung zum Entfernen von Kaspersky Security Service aus der Registrierung über den Service Control Manager von Microsoft Windows.
Benutzeranfragen an den Dienst	Berechtigung zur Erstellung und zum Versand von Benutzeranfragen an Kaspersky Security Service.

Zugriffsrechte über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Zugriffsrechte für ein oder alle Geräte im Netzwerk konfigurieren.

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

Sie können die Liste der Benutzer und Benutzergruppen, die Zugriff auf die Funktionen von Kaspersky Embedded Systems Security haben und Kaspersky Security Service verwalten dürfen, bearbeiten. Sie können auch die Zugriffsrechte dieser Benutzer und Benutzergruppen ändern.

Gehen Sie wie folgt vor, um Benutzer oder Gruppen zur Liste hinzuzufügen oder aus dieser zu entfernen:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen aus:
   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.
   - Klicken Sie im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die über Zugriffsrechte zur Verwaltung des Dienstes Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security 3.1** wird geöffnet.
5. Im nächsten 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.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die ausgewählten Benutzer (Gruppen) werden hinzugefügt bzw. entfernt.

Gehen Sie wie folgt vor, um die Rechte eines Benutzers oder einer Gruppe zur Verwaltung von Kaspersky Embedded Systems Security oder von Kaspersky Security Service zu ändern:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen aus:

   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.

   - Klicken Sie im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung des Programms mithilfe von Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** wird geöffnet.

5. Wählen Sie im nächsten Fenster in der Liste **Gruppen- oder Benutzernamen** den Benutzer oder die Benutzergruppe aus, dessen bzw. deren Rechte Sie ändern möchten.

6. Aktivieren Sie im Abschnitt **Berechtigungen für "<Benutzer (Gruppe)>"** die Kontrollkästchen **Erlauben** oder **Verbieten** für die folgenden Zugriffsstufen:

   - **Vollständige Kontrolle**: Uneingeschränkte Rechte zur Verwaltung von Kaspersky Embedded Systems Security oder Kaspersky Security Service.

   - **Lesen**:

     - Folgende Rechte für die Verwaltung von Kaspersky Embedded Systems Security: **Statistik abrufen**, **Einstellungen lesen**, **Protokolle lesen** und **Leserechte**.

     - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Lesen der Einstellungen des Dienstes**, **Statusanfrage beim Service Control Manager**, **Statusanfrage beim Dienst**, **Lesen der Liste der abhängigen Dienste**, **Leserechte**.

   - **Änderung**:

     - Alle Rechte zur Verwaltung von Kaspersky Embedded Systems Security mit Ausnahme von **Änderungsrechte**.

     - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Diensteinstellungen konfigurieren**, **Leserechte**.

   - **Sonderrechte**: Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Dienst starten**, **Dienst beenden**, **Dienst anhalten/fortsetzen**, **Leserechte**, **Benutzeranfragen an den Dienst**.

7. Um erweiterte Rechte für einen Benutzer oder eine Gruppe (**Sonderrechte**) anzupassen, klicken Sie auf die Schaltfläche **Erweitert**.

a. Wählen Sie im nächsten Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Embedded Systems Security** den gewünschten Benutzer bzw. die Gruppe aus.

b. Klicken Sie auf die Schaltfläche **Ändern**.

c. Wählen Sie in der Dropdown-Liste im oberen Fensterbereich die Art der Zugriffskontrolle aus (**Erlauben** oder **Blockieren**).

d. Aktivieren Sie die Kontrollkästchen neben denjenigen Funktionen, die Sie dem betreffenden Benutzer bzw. der betreffenden Gruppe erlauben oder verbieten möchten.

e. Klicken Sie auf **OK**.

f. Klicken Sie im Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Security für Windows Server** auf Kaspersky Embedded Systems Security.

8. 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 oder Kaspersky Security Service werden gespeichert.

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste mithilfe der Einstellungen der Rechte der Benutzer beschränken. Außerdem können Sie kritische Vorgänge zusätzlich schützen, indem Sie in den Einstellungen von Kaspersky Embedded Systems Security einen Kennwortschutz einrichten.

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

- Verbindung mit der Programmkonsole
- Deinstallation von Kaspersky Embedded Systems Security
- Änderung der Einstellungen von Kaspersky Embedded Systems Security
- Ausführung von Befehlen in der Befehlszeile

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

Kaspersky Embedded Systems Security prüft nicht die Kennwortstärke und sperrt auch nicht die Kennworteingabe nach mehreren Fehleingaben.

Wenn Sie ein Kennwort erstellen, sollten Sie folgende Empfehlungen beachten:

- Das Kennwort darf weder Kontoname noch Computername enthalten.
- Das Kennwort ist mindestens 8 Zeichen lang.

- Das Kennwort enthält Zeichen aus mindestens drei der folgenden Kategorien:
  - lateinische Großbuchstaben (A-Z)
  - lateinische Kleinbuchstaben (a-z)
  - Ziffern (0-9)
  - Symbole wie Ausrufezeichen (!), Dollarzeichen ($), Raute (#) und Prozentzeichen (%)

Sie können die Einstellungen des kennwortgeschützten Programms exportieren und importieren. Eine Konfigurationsdatei, die durch den 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 Funktionen von Kaspersky Embedded Systems Security zu schützen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte**. Wählen Sie die Administrationsgruppe aus, für deren geschützte Geräte Sie die Programmeinstellungen konfigurieren möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie die Eigenschaften von **<Name der Richtlinie>** über das Kontextmenü, um die Richtlinieneinstellungen für eine Gruppe von geschützten Geräten anzupassen.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, öffnen Sie die gewünschten Einstellungen im Fenster **Programmeinstellungen** in Kaspersky Security Center.
3. Klicken Sie im Abschnitt **Sicherheit und Zuverlässigkeit** der Registerkarte **Programmeinstellungen** auf die Schaltfläche **Einstellungen**.

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

   Die Felder **Kennwort** und **Kennwort bestätigen** werden aktiv.
5. Geben Sie im Feld **Kennwort** das Kennwort ein, das Sie für den Schutz des Zugriffes auf die Funktionen von Kaspersky Embedded Systems Security 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 fragt das festgelegte Kennwort für den 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 Gerät entfernt werden.

Sie können das Kennwort jederzeit zurücksetzen. Deaktivieren Sie dazu das Kontrollkästchen **Kennwortschutz verwenden** und speichern Sie die Änderungen. Der Kennwortschutz wird deaktiviert und die alte Prüfsumme des Kennworts entfernt. Wiederholen Sie den Kennworterstellungsprozess mit einem neuen Kennwort.

Zugriffsrechte über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Zugriffsrechte auf einem geschützten Gerät konfigurieren.

Konfiguration der Zugriffsrechte zur Verwaltung von Kaspersky Embedded Systems Security und Kaspersky Security Service

Sie können die Liste der Benutzer und Benutzergruppen, die Zugriff auf die Funktionen von Kaspersky Embedded Systems Security haben und Kaspersky Security Service verwalten dürfen, bearbeiten. Sie können auch die Zugriffsrechte dieser Benutzer und Benutzergruppen ändern.

Gehen Sie wie folgt vor, um Benutzer oder Gruppen zur Liste hinzuzufügen oder aus dieser zu entfernen:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen aus:
   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.
   - Klicken Sie im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die über Zugriffsrechte zur Verwaltung von Kaspersky Security Service verfügen.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security 3.1** wird geöffnet.

5. Im nächsten 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.

6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die ausgewählten Benutzer (Gruppen) werden hinzugefügt bzw. entfernt.

Gehen Sie wie folgt vor, um eine Rechte eines Benutzers oder einer Gruppe zur Verwaltung von Kaspersky Embedded Systems Security oder Kaspersky Security Service zu bearbeiten:

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

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

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Führen Sie im Abschnitt **Zusätzlich** eine der folgenden Aktionen aus:

   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.

   - Klicken Sie im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung des Programms mithilfe von Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** wird geöffnet.

5. Wählen Sie im nächsten Fenster in der Liste **Gruppen- oder Benutzernamen** den Benutzer oder die Benutzergruppe aus, dessen bzw. deren Rechte Sie ändern möchten.

6. Aktivieren Sie im Abschnitt **Berechtigungen für "<Benutzer (Gruppe)>"** die Kontrollkästchen **Erlauben** oder **Verbieten** für die folgenden Zugriffsstufen:

   - **Vollständige Kontrolle**: Uneingeschränkte Rechte zur Verwaltung von Kaspersky Embedded Systems Security oder Kaspersky Security Service.

   - **Lesen**:

- Folgende Rechte für die Verwaltung von Kaspersky Embedded Systems Security: **Statistik abrufen**, **Einstellungen lesen**, **Protokolle lesen** und **Leserechte**.

- Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Lesen der Einstellungen des Dienstes**, **Statusanfrage beim Service Control Manager**, **Statusanfrage beim Dienst**, **Lesen der Liste der abhängigen Dienste**, **Leserechte**.

- **Änderung**:

  - Alle Rechte zur Verwaltung von Kaspersky Embedded Systems Security mit Ausnahme von **Änderungsrechte**.

  - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Diensteinstellungen konfigurieren**, **Leserechte**.

- **Sonderrechte**: Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Dienst starten**, **Dienst beenden**, **Dienst anhalten/fortsetzen**, **Leserechte**, **Benutzeranfragen an den Dienst**.

7. Um erweiterte Rechte für einen Benutzer oder eine Gruppe (**Sonderrechte**) anzupassen, klicken Sie auf die Schaltfläche **Erweitert**.

   a. Wählen Sie im nächsten Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Embedded Systems Security** den gewünschten Benutzer bzw. die Gruppe aus.

   b. Klicken Sie auf die Schaltfläche **Ändern**.

   c. Wählen Sie in der Dropdown-Liste im oberen Fensterbereich die Art der Zugriffskontrolle aus (**Erlauben** oder **Blockieren**).

   d. Aktivieren Sie die Kontrollkästchen neben denjenigen Funktionen, die Sie dem betreffenden Benutzer bzw. der betreffenden Gruppe erlauben oder verbieten möchten.

   e. Klicken Sie auf **OK**.

   f. Klicken Sie im Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Security für Windows Server** auf Kaspersky Embedded Systems Security.

8. Klicken Sie im Gruppenfenster **Rechte für Kaspersky Embedded Systems Security** auf die Schaltfläche **Übernehmen**.

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

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste mithilfe der Einstellungen der Rechte der Benutzer beschränken. Außerdem können Sie kritische Vorgänge zusätzlich schützen, indem Sie in den Einstellungen von Kaspersky Embedded Systems Security einen Kennwortschutz einrichten.

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

- Verbindung mit der Programmkonsole

- Deinstallation von Kaspersky Embedded Systems Security
- Änderung der Einstellungen von Kaspersky Embedded Systems Security
- Ausführung von Befehlen in der Befehlszeile

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

Sie können die Einstellungen des kennwortgeschützten Programms exportieren und importieren. Eine Konfigurationsdatei, die durch den 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 Funktionen von Kaspersky Embedded Systems Security zu schützen, gehen Sie wie folgt vor:

1. Wählen Sie in der Struktur der Programmkonsole den **Kaspersky Embedded Systems Security** Hauptknoten aus und führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie im Ergebnisbereich des Knotens auf den Link **Eigenschaften des Programms**.
   - Wählen Sie im Kontextmenü des Knotens den Punkt **Eigenschaften** aus.

   Das Fenster **Programmeinstellungen** wird geöffnet.
2. Klicken Sie auf der Registerkarte **Sicherheit und Zuverlässigkeit** im Abschnitt **Einstellungen für den Kennwortschutz** auf das Kontrollkästchen **Kennwortschutz verwenden**.

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

Das festgelegte Kennwort kann nicht wiederhergestellt werden. Wenn Sie das Kennwort verlieren, führt das zum vollständigen Verlust der Kontrolle über das Programm. Darüber hinaus kann das Programm nicht vom geschützten Gerät entfernt werden.

Sie können das Kennwort jederzeit zurücksetzen. Deaktivieren Sie dazu das Kontrollkästchen **Kennwortschutz verwenden** und speichern Sie die Änderungen. Der Kennwortschutz wird deaktiviert und die alte Prüfsumme des Kennworts entfernt. Wiederholen Sie den Kennworterstellungsprozess mit einem neuen Kennwort.

Zugriffsrechte über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Web-Plug-ins navigieren und Zugriffsrechte für ein oder alle geschützten Geräte im Netzwerk konfigurieren.

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

Für die Konfiguration der Zugriffsberechtigungen für einen Benutzer oder eine Gruppe müssen Sie die Zeichenfolge des Sicherheitsdescriptors mithilfe der Security Descriptor Definition Language (SDDL) angeben. Detaillierte Informationen über die Zeichenfolge des Sicherheitsdescriptors finden Sie auf der Microsoft-Website.

So konfigurieren Sie die Zugriffsberechtigungen für einen Benutzer oder eine Gruppe:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Zusätzlich**.
5. Führen Sie eine der Aktionen durch:
   - Klicken Sie im Unterabschnitt **Benutzerrechte für die Programmverwaltung** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Embedded Systems Security haben.
   - Klicken Sie im Unterabschnitt **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** auf **Einstellungen**, wenn Sie die Liste der Benutzer ändern möchten, die über Zugriffsrechte zur Verwaltung des Dienstes Kaspersky Security Service haben.
6. Fügen Sie einen Benutzer oder eine Gruppe hinzu, indem Sie im Fenster **Benutzerrechte für die Programmverwaltung** oder **Benutzerzugriffsrechte für die Verwaltung von Kaspersky Security Service** die Zeichenfolge des Sicherheitsdescriptors eingeben.
7. Klicken Sie auf **OK**.

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Embedded Systems Security

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste mithilfe der Einstellungen der Rechte der Benutzer beschränken. Außerdem können Sie kritische Vorgänge zusätzlich schützen, indem Sie in den Einstellungen von Kaspersky Embedded Systems Security einen Kennwortschutz einrichten.

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

- Verbindung mit der Programmkonsole
- Deinstallation von Kaspersky Embedded Systems Security

- Änderung der Einstellungen von Kaspersky Embedded Systems Security
- Ausführung von Befehlen in der Befehlszeile

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

Sie können die Einstellungen des kennwortgeschützten Programms exportieren und importieren. Eine Konfigurationsdatei, die durch den 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 Funktionen von Kaspersky Embedded Systems Security zu schützen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Programmeinstellungen** aus.
5. Klicken Sie im Abschnitt **Sicherheit und Zuverlässigkeit** auf **Einstellungen.**
6. Aktivieren Sie im Abschnitt **Einstellungen für den Kennwortschutz** das Kontrollkästchen **Kennwortschutz verwenden**.
7. Geben Sie im Feld **Kennwort** das Kennwort ein, das Sie für den Schutz des Zugriffes auf die Funktionen von Kaspersky Embedded Systems Security verwenden möchten.
8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert. Kaspersky Embedded Systems Security fragt das festgelegte Kennwort für den 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 Gerät entfernt werden.

Sie können das Kennwort jederzeit zurücksetzen. Deaktivieren Sie dazu das Kontrollkästchen **Kennwortschutz verwenden** und speichern Sie die Änderungen. Der Kennwortschutz wird deaktiviert und die alte Prüfsumme des Kennworts entfernt. Wiederholen Sie den Kennworterstellungsprozess mit einem neuen Kennwort.

Echtzeitschutz für Dateien

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

Über die Aufgabe zum Echtzeitschutz für Dateien

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

- Dateien
- Alternative NTFS-Datenströme
- Master Boot Records und Bootsektoren von lokalen Festplatten und externen Geräten

Wenn ein Programm eine Datei auf dem geschützten Gerät speichert oder eine Datei vom Gerät abruft, fängt Kaspersky Embedded Systems Security die 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. Vor der Desinfektion oder dem Löschen speichert Kaspersky Embedded Systems Security eine verschlüsselte Kopie der Quelldatei im Backup-Ordner.

Kaspersky Embedded Systems Security erkennt außerdem Schadsoftware für Prozesse, die unter Windows Subsystem for Linux® laufen. Bei solchen Prozessen wendet die Aufgabe zum Echtzeitschutz für Dateien die von der aktuellen Konfiguration festgelegte Aktion an.

Über den Schutzbereich von Aufgaben und Sicherheitseinstellungen

Standardmäßig schützt die Aufgabe für den Echtzeitschutz für Dateien alle Objekte im Dateisystem des Geräts. Verlangen die Sicherheitsanforderungen keinen Schutz für alle Objekte des Dateisystems, oder wenn Sie einige Objekte aus dem Gültigkeitsbereich der Aufgabe zum Echtzeitschutz ausschließen möchten, können Sie den Schutzbereich beschränken.

In der Programmkonsole wird der Schutzbereich als Struktur oder Liste jener Dateiressourcen des Geräts dargestellt, die von Kaspersky Embedded Systems Security überwacht werden können. Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Geräts als Liste angezeigt.

Im Verwaltungs-Plug-in steht nur die Listenansicht zur Verfügung.

Um freigegebene Netzwerkordner in der Programmkonsole in der Baumstruktur anzuzeigen, gehen Sie wie folgt vor:

Wählen Sie im linken unteren Teil des Fensters **Schutzbereichseinstellungen** aus der Dropdown-Liste den Punkt **Als Baumstruktur anzeigen**.

Wenn die Dateistruktur des geschützten Geräts als Liste oder Baumstruktur angezeigt werden, haben die Symbole für die Knoten folgende Bedeutung:

☑ Der Knoten ist im Schutzbereich.

☐ Der Knoten ist nicht im Schutzbereich.

Mindestens ein diesem Knoten untergeordneter Knoten gehört nicht zum Schutzbereich oder die Sicherheitseinstellungen des oder der untergeordneten Knoten unterscheiden sich von den Sicherheitseinstellungen des übergeordneten Knotens (nur für die Baumstruktur-Ansicht).

Das Symbol wird angezeigt, wenn alle untergeordneten Knoten ausgewählt sind, nicht jedoch der übergeordnete Knoten. In diesem Fall werden Änderungen der Dateien und Ordner des übergeordneten Knotens bei der Einrichtung eines Schutzbereichs für den ausgewählten untergeordneten Knoten nicht automatisch berücksichtigt.

Mithilfe der Programmkonsole können Sie auch virtuelle Festplatten zum Schutzbereich hinzufügen. Die Namen von virtuellen Nodes werden blau dargestellt.

Parameter für Sicherheit

Die Sicherheitseinstellungen für Aufgaben können als allgemeine Einstellungen für alle Knoten oder Elemente im Schutzbereich, oder als unterschiedliche Einstellungen für jeden Knoten bzw. jedes Element in der Baumstruktur oder Liste der Dateiressourcen des Geräts konfiguriert werden.

Die Sicherheitseinstellungen, die für den ausgewählten übergeordneten Knoten konfiguriert wurden, werden automatisch für alle untergeordneten Node übernommen. Die Sicherheitseinstellungen des übergeordneten Knotens werden für untergeordnete Knoten, die gesondert konfiguriert werden, nicht übernommen.

Sie können die Parameter eines ausgewählten Schutzbereichs auf eine der folgenden Weisen anpassen:

- Wählen Sie eine der vordefinierten Sicherheitsstufen aus.
- Konfigurieren Sie die Sicherheitseinstellungen manuell für die ausgewählten Knoten oder Elemente in der Struktur oder Liste der Dateiressourcen (die Sicherheitsstufe wechselt zu **Benutzerdefiniert**).

Sie können einen Einstellungssatz für einen Knoten oder ein Element in einer Vorlage speichern, um diese Vorlage später für andere Nodes oder Elemente zu übernehmen.

Über virtuelle Schutzbereiche

Kaspersky Embedded Systems Security kann nicht nur vorhandene Ordner und Dateien auf Festplatten und Wechseldatenträgern untersuchen, sondern auch Datenträger, die von verschiedenen Anwendungen und Diensten dynamisch auf dem geschützten Gerät angelegt werden.

Wenn Sie alle Objekte des Geräts in den Schutzbereich aufgenommen haben, gehören automatisch auch diese dynamischen Knoten zum Schutzbereich. Wenn Sie allerdings spezielle Werte für die Sicherheitsparameter dieser dynamischen Knoten festlegen möchten oder den Schutz nur für einzelne Bereiche des Geräts aktiviert haben, dann muss, um virtuelle Laufwerke, Ordner oder Dateien in den Schutzbereich aufzunehmen, zuvor in der Programmkonsole ein virtueller Schutzbereich angelegt werden. Die von Ihnen angelegten Laufwerke, Ordner und Dateien existieren nur in der Programmkonsole, nicht aber in der Dateisystemstruktur des geschützten Geräts.

Wenn Sie einen Schutzbereich anlegen und alle untergeordneten Ordner oder Dateien auswählen, nicht aber den übergeordneten Ordner, dann werden die virtuellen Ordner oder Dateien, die sich darin befinden, nicht automatisch in den Schutzbereich aufgenommen. Es ist erforderlich, in der Programmkonsole "virtuelle Kopien" davon anzulegen und zum Schutzbereich hinzuzufügen.

Vordefinierte Schutzbereiche

Die Dateistruktur oder Liste der Dateiressourcen zeigt die Knoten an, für die Sie nach den Sicherheitseinstellungen in Microsoft Windows über Leserechte verfügen.

Kaspersky Embedded Systems Security deckt die folgenden vordefinierten Schutzbereiche ab:

- **Lokale Festplatten**. Kaspersky Embedded Systems Security schützt Dateien auf den Festplatten des Geräts.
- **Wechseldatenträger**. Kaspersky Embedded Systems Security schützt Dateien auf externen Geräten, z. B. auf CDs oder Wechseldatenträger. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Schutzbereich aufnehmen oder aus diesem ausschließen.
- **Netzwerkumgebung**. Kaspersky Embedded Systems Security schützt die Dateien, die in Netzwerkordnern gespeichert sind oder aus diesen von auf dem Gerät laufenden Programmen abgefragt werden. Kaspersky Embedded Systems Security schützt Dateien in Netzwerkordnern nicht, wenn Programme von anderen geschützten Geräten aus darauf zugreifen.
- **Virtuelle Festplatten**. Sie können in den Schutzbereich virtuelle Ordner und Dateien sowie Laufwerke aufnehmen, die vorübergehend auf dem Gerät 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 Schutzbereichseinstellungen verfügbar.

Standardmäßig sind alle vordefinierten Bereiche mit Ausnahme von virtuellen Festplatten in den Schutzbereich eingeschlossen.

Virtuelle Festplatten, die mit dem Befehl SUBST erzeugt wurden, werden in der Dateistruktur des geschützten Geräts in der Programmkonsole nicht angezeigt. Um Objekte auf einer virtuellen Festplatte in den Schutzbereich aufzunehmen, schließen Sie den Ordner auf dem Gerät, mit dem diese virtuelle Festplatte verbunden ist, in den Schutzbereich ein.

Verbundene Netzlaufwerke werden ebenfalls nicht in der Dateiressourcenliste des geschützten Geräts angezeigt. Um Objekte auf einem Netzwerk-Datenträger in den Schutzbereich aufzunehmen, geben Sie den Pfad des Ordners an, der diesem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

Über vordefinierte Sicherheitsstufen

Für in der Struktur oder Liste der Dateiressourcen des geschützten Geräts ausgewählte Knoten können Sie eine der folgenden vordefinierten Sicherheitsstufen festlegen: **Maximale Leistung**, **Empfohlen** oder **Maximale Sicherheit**. Jede dieser Ebenen besitzt eine eigene Auswahl von Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird empfohlen, wenn Ihr Netzwerk über zusätzliche Sicherheitsmaßnahmen verfügt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien, die über die Verwendung von Kaspersky Embedded Systems Security auf geschützten Geräten hinausgehen.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Geräte. Die Experten von Kaspersky empfehlen diese Stufe als ausreichenden Schutz von Geräten in den meisten Unternehmensnetzwerken. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximale Sicherheit

Die Sicherheitsstufe **Maximale Sicherheit** wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Gerätesicherheit hat.

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	Nur informieren	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte	Zugriff verweigern und in die Quarantäne verschieben	Nur informieren	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
Schutz von zusammengesetzten Objekten	• Gepackte Objekte* *Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-

		Objekte* *Nur neue und veränderte	Objekte* *Alle Objekte
Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann	Nein	Nein	Ja

Die Einstellungen **Schutz von Objekten**, **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden** und **Heuristische Analyse verwenden** sind nicht in den vordefinierten Sicherheitsstufen enthalten. Wenn Sie nach der Auswahl einer der vordefinierten Sicherheitsstufen die Sicherheitseinstellungen für **Schutz von Objekten**, **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden**, **Heuristische Analyse verwenden** verändern, wird dadurch die gewählte voreingestellte Sicherheitsstufe nicht geändert.

Dateierweiterungen, die in der Aufgabe zum Echtzeitschutz für Dateien standardmäßig untersucht werden

In der Grundeinstellung untersucht Kaspersky Embedded Systems Security Dateien mit den folgenden Erweiterungen:

- *386*
- *acm*
- *ade, adp*
- *asp*
- *asx*
- *ax*
- *bas*
- *bat*
- *bin*
- *chm*
- *cla, clas**
- *cmd*
- *com*
- *cpl*
- *crt*

- *dll*
- *dpl*
- *drv*
- *dvb*
- *dwg*
- *efi*
- *emf*
- *eml*
- *exe*
- *fon*
- *fpm*
- *hlp*
- *hta*
- *htm, html**
- *htt*
- *ico*
- *inf*
- *ini*
- *ins*
- *isp*
- *jpg, jpe*
- *js, jse*
- *lnk*
- *mbx*
- *msc*
- *msg*
- *msi*
- *msp*

- *mst*
- *nws*
- *ocx*
- *oft*
- *otm*
- *pcd*
- *pdf*
- *php*
- *pht*
- *phtm**
- *pif*
- *plg*
- *png*
- *pot*
- *prf*
- *prg*
- *reg*
- *rsc*
- *rtf*
- *scf*
- *scr*
- *sct*
- *shb*
- *shs*
- *sht*
- *shtm**
- *swf*
- *sys*

- *the*
- *them**
- *tsp*
- *url*
- *vb*
- *vbe*
- *vbs*
- *vxd*
- *wma*
- *wmf*
- *wmv*
- *wsc*
- *wsf*
- *wsh*
- *do?*
- *md?*
- *mp?*
- *ov?*
- *pp?*
- *vs?*
- *xl?*

Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien

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

Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien

Einstellung	Standardwert	Beschreibung
Schutzbereich	Gesamtes geschütztes Gerät ohne virtuelle Festplatten.	Sie können den Schutzbereich ändern.

Parameter für Sicherheit	Einheitlich für den gesamten Schutzbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Sie können für die ausgewählten Knoten in der Struktur oder Liste der Dateiressourcen des geschützten Geräts folgende Aktionen ausführen: • eine andere vordefinierte Sicherheitsstufe auswählen • Sicherheitseinstellungen manuell ändern. Sie können eine Gruppe von Sicherheitsparametern für den ausgewählten Knoten in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen.
Schutzmodus für Objekte	**Intelligenter Modus**	Sie können den Schutzmodus für Objekte festlegen, also die Art der Zugriffsversuche, bei denen Objekte von Kaspersky Embedded Systems Security überprüft werden.
Heuristische Analyse	Es wird die Sicherheitsstufe **Mittel** angewendet.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
Vertrauenswürdige Zone anwenden	Wird verwendet	Einheitliche Liste mit Ausnahmen, die Sie in bestimmten Aufgaben verwenden können.
KSN zum Schutz verwenden	Wird verwendet	Sie können Ihr Gerät durch die Nutzung des Cloud-Dienstes von Kaspersky Security Network effektiver schützen (nur verfügbar, wenn die KSN-Erklärung akzeptiert wurde).
Zeitplan für den Aufgabenstart	Bei Programmstart.	Sie können die Ausführung einer Aufgabe nach Zeitplan konfigurieren.
Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen	Wird nicht verwendet.	Sie können Computer, die schädliche Aktivitäten zeigen, zur Liste der blockierten Hosts hinzufügen.
Untersuchung wichtiger Bereiche starten, wenn aktive Infektion erkannt wird	Wird verwendet	Wenn eine aktive Infektion erkannt wird, erstellt Kaspersky Embedded Systems Security eine temporäre Aufgabe zur Untersuchung wichtiger Bereiche und startet sie.

Aufgabe zum Echtzeitschutz für Dateien über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Aufgabeneinstellungen für einen oder alle geschützten Geräte im Netzwerk konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Richtlinieneinstellungen für die Aufgabe zum Echtzeitschutz für Dateien öffnen

Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien über die Richtlinie für Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Echtzeit-Computerschutz** aus.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Echtzeitschutz für Dateien**.

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

Wenn ein geschütztes Gerät durch eine aktive Richtlinie von Kaspersky Security Center verwaltet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht über die Programmkonsole geändert werden.

Aufgabeneigenschaften für den Echtzeitschutz für Dateien öffnen

Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien für ein einzelnes Netzwerkgerät zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Name des geschützten Geräts>** zu öffnen:

   - Doppelklicken Sie auf den Namen des geschützten Geräts.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Geräts aus.

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.
5. Wählen Sie im Abschnitt **Aufgaben** die Aufgabe **Echtzeitschutz für Dateien** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

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

Aufgabe zum Echtzeitschutz für Dateien anpassen

Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Echtzeitschutz für Dateien**.
2. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Auf der Registerkarte **Allgemein**:
     - **Interception-Parameter**
     - **Heuristische Analyse**
     - **Integration mit anderen Komponenten**
   - Auf der Registerkarte **Aufgabenverwaltung**:
     - Einstellungen für den Start der Aufgabe nach Zeitplan.
3. Wählen Sie die Registerkarte **Schutzbereich** aus und gehen Sie wie folgt vor:
   - Klicken Sie auf die Schaltfläche **Hinzufügen** oder **Ändern**, um den Schutzbereich zu ändern.
     - 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 oder passen Sie den Schutz manuell an.
4. Klicken Sie im Fenster **Echtzeitschutz für Dateien** auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in einer ausgeführten Aufgabe. Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Schutzmodus auswählen

Sie können den Schutzmodus in der Aufgabe Echtzeitschutz für Dateien auswählen. Im Abschnitt **Schutzmodus für Objekte** können Sie die Art der Zugriffsversuche festlegen, die Kaspersky Embedded Systems Security bei einer Untersuchung von Objekten ausführt.

Der Wert der Einstellung **Schutzmodus für Objekte** wird für den gesamten in der Aufgabe angegebenen Schutzbereich angewendet. Für diese Einstellung können keine unterschiedlichen Werte für einzelne Knoten des Schutzbereichs festgelegt werden.

Um den Schutzmodus auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Echtzeitschutz für Dateien**.
2. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** den Schutzmodus aus, den Sie festlegen möchten:
   - **Intelligenter Modus**
   - **Beim Öffnen und Ändern**
   - **Beim Öffnen**
   - **Beim Ausführen**
   - **Tiefere Analyse startender Prozesse (Blockiert den Start eines Prozesses, bis die Analyse abgeschlossen ist)**
3. Klicken Sie auf **OK**.

Der ausgewählte Schutzmodus für die Objekte wird eingestellt.

Heuristische Analyse und Integration mit anderen Programmkomponenten

Die Aufgabe "Verwendung von KSN" kann nur gestartet werden, wenn die Erklärung zu Kaspersky Security Network akzeptiert wurde.

Um die heuristische Analyse und Integration mit anderen Programmkomponenten zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Echtzeitschutz für Dateien**.
2. Deaktivieren oder aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Heuristische Analyse verwenden**.
3. Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.
4. Konfigurieren Sie im Abschnitt **Integration mit anderen Komponenten** die folgenden Einstellungen:
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **KSN zum Schutz verwenden**.

     Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Daten über untersuchte Dateien senden** in den Aufgabeneinstellungen für die Verwendung von KSN aktiviert ist.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen**.

- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Untersuchung wichtiger Bereiche starten, wenn aktive Infektion erkannt wird**.

5. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe werden unverzüglich während der Ausführung einer Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Aufgaben planen

In der Programmkonsole können Sie lokale Systemaufgaben und benutzerdefinierte Aufgaben planen. Gruppenaufgaben können nicht über die Programmkonsole geplant werden.

So planen Sie Gruppenaufgaben mithilfe des Verwaltungs-Plug-in:

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

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

7. Passen Sie die Zeitplaneinstellungen entsprechend Ihren Anforderungen an. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie in der Liste **Startintervall** einen der folgenden Werte aus:
      - **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 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 die Startzeit, das Datum und die Häufigkeit der Aufgabe festgelegt haben, wird die geschätzte Zeit für den nächsten Start angezeigt.

Gehen Sie zur Registerkarte **Zeitplan** und öffnen Sie das Fenster **Aufgabeneinstellungen**. Im oberen Bereich des Fensters wird im Feld **Nächster Start**, die geschätzte Startzeit angezeigt. Jedes Mal, wenn Sie das Fenster öffnen, wird diese geschätzte Startzeit aktualisiert und angezeigt.

Im Feld **Nächster Start** wird der Wert **Durch Richtlinie verboten** angezeigt, wenn die Richtlinieneinstellungen von Kaspersky Security Center den Start geplanter lokaler Systemaufgaben verhindern.

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

- Im Abschnitt **Einstellungen für das Anhalten der Aufgabe**:

  a. Aktivieren Sie das Kontrollkästchen **Dauer** und geben Sie in den Feldern auf der rechten Seite die maximale Anzahl der Stunden und Minuten für die Ausführung der Aufgabe ein.

  b. Aktivieren Sie das Kontrollkästchen **Anhalten von** und geben Sie in den Feldern auf der rechten Seite den Start- und Endwert eines Zeitintervalls für 24 Stunden ein, in dem die Ausführung der Aufgabe angehalten wird.

- Im Abschnitt **Erweiterte Einstellungen**:

  a. Aktivieren Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.

  b. Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.

  c. Aktivieren Sie das Kontrollkästchen **Aufgabenstart zufällig wählen innerhalb von** und geben Sie einen Wert in Minuten ein.

9. Klicken Sie auf **OK**.

10. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen für den Aufgabenstart zu speichern.

Wenn Sie Programmeinstellungen für eine einzelne Aufgabe mithilfe von Kaspersky Security Center konfigurieren möchten, siehe Abschnitt "Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen".

Schutzbereich von Aufgaben erstellen und konfigurieren

Um den Schutzbereich von Aufgaben über das Kaspersky Security Center zu erstellen und zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Echtzeitschutz für Dateien**.
2. Wählen Sie die Registerkarte **Schutzbereich** aus.

   Alle bereits durch die Aufgabe geschützten Elemente sind in der Tabelle **Schutzbereich** aufgelistet.
3. Klicken Sie auf die Schaltfläche **Hinzufügen**, um ein neues Element zur Liste hinzuzufügen.

   Das Fenster **Zum Schutzbereich hinzufügen** wird geöffnet.
4. Wählen Sie einen Objekttyp aus, um ihm zu einem Schutzbereich hinzuzufügen:

   - **Vordefinierter Bereich**, wenn Sie in den Schutzbereich einen der vordefinierten Bereiche auf dem Gerät aufnehmen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Schutzbereich aus.
   - **Laufwerk, Ordner oder Netzwerkobjekt**, wenn Sie in den Schutzbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Schutzbereich über die Schaltfläche **Durchsuchen** aus.
   - **Datei**, wenn Sie in den Schutzbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Schutzbereich über die Schaltfläche **Durchsuchen** aus.

   Sie können ein Objekt nicht zum Schutzbereich hinzufügen, wenn es bereits als Ausnahme aus dem Schutzbereich hinzugefügt wurde.
5. Um einzelne Elemente aus dem Schutzbereich auszuschließen, deaktivieren Sie die Kontrollkästchen neben den Namen dieser Elemente, oder führen Sie die folgenden Schritte durch:

   a. Öffnen Sie das Kontextmenü des Schutzbereichs mit der rechten Maustaste.

   b. Wählen Sie im Kontextmenü den Punkt **Ausnahme hinzufügen**.

   c. Wählen Sie im geöffneten Fenster **Ausnahme hinzufügen** den Typ des Objektes aus, das Sie als Ausnahme aus dem Schutzbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Schutzbereich.
6. Um den Schutzbereich einer vorhandenen Ausnahme zu ändern, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option **Bereich ändern**.
7. Um die Anzeige eines zuvor hinzugefügten Schutzbereiches bzw. einer Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option **Bereich löschen** aus.

   Der Schutzbereich wird aus dem Gültigkeitsbereich der Aufgabe zum Echtzeitschutz für Dateien bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner entfernt.
8. Klicken Sie auf **OK**.

Das Fenster Schutzbereichseinstellungen wird geschlossen. Ihre neu konfigurierten Einstellungen werden gespeichert.

Die Aufgabe **Echtzeitschutz für Dateien** kann gestartet werden, wenn mindestens ein Knoten der Struktur der Dateiressourcen des Geräts in einen Schutzbereich aufgenommen wurde.

Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen

Sie können eine der folgenden drei vordefinierten Sicherheitsstufen für einen in der Liste der Dateiressourcen des Geräts ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen** und **Maximale Sicherheit**.

Um eine der vordefinierten Sicherheitsstufen auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Echtzeitschutz für Dateien**.
2. Wählen Sie die Registerkarte **Schutzbereich** aus.
3. Wählen Sie in der Liste des geschützten Geräts ein Element aus dem Schutzbereich aus, um eine vordefinierte Sicherheitsstufe festzulegen.
4. Klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Einstellungen für den Echtzeitschutz für Dateien anpassen** wird geöffnet.
5. Wählen Sie auf der Registerkarte **Sicherheitsstufe** die Sicherheitsstufe aus, die Sie übernehmen möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Eigenschaften: Echtzeitschutz für Dateien** auf **OK**.

   Die Einstellungen der Aufgabe werden gespeichert und unverzüglich auf eine ausgeführte Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

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**.

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für einzelne Elemente in der Liste der Dateiressourcen des Geräts oder den Nodes in der Struktur festlegen.

So passen Sie die Sicherheitsparameter eines bestimmten Knotens manuell an:

1. Öffnen Sie das Fenster **Echtzeitschutz für Dateien**.

2. Wählen Sie auf der Registerkarte **Schutzbereich** den Knoten aus, dessen Sicherheitseinstellungen Sie anpassen möchten, und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Einstellungen für den Echtzeitschutz für Dateien anpassen** wird geöffnet.

3. Klicken Sie auf der Registerkarte **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**, um eine benutzerdefinierte Konfiguration einzurichten.

4. Sie können benutzerdefinierte Sicherheitseinstellungen für den ausgewählten Knoten gemäß Ihren Bedürfnissen anpassen:

   - Allgemeine Parameter
   - Aktionen
   - Optimierung

5. Klicken Sie im Fenster **Echtzeitschutz für Dateien** auf **OK**.

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 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
   - **Objekte, die nach Format untersucht werden**
   - **Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden**
   - **Objekte, die nach der angegebenen Erweiterungsliste untersucht werden**
   - **Bootsektoren und MBR**
   - **Alternative NTFS-Ströme**

4. Aktivieren oder deaktivieren Sie im Gruppenfeld **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien schützen**.

   Um bei deaktiviertem Kontrollkästchen zwischen den verfügbaren Optionen hin- und her zu wechseln, 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**
- Alle / **Nur neue SFX-Archive**
- Alle / **Nur neue E-Mail-Datenbanken**
- Alle / **Nur neue gepackte Objekte**
- Alle / **Nur neue E-Mails im Nur-Text-Format**
- Alle / **Nur neue eingebettete OLE-Objekte**

6. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

So passen Sie die Aktionen für infizierte und andere gefundene Objekte während der Aufgabe zum Echtzeitschutz für Dateien an:

1. Öffnen Sie das Fenster **Einstellungen für den Echtzeitschutz für Dateien anpassen**.
2. Wählen Sie die Registerkarte **Aktionen** aus.
3. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
   - **Nur informieren**.
   - **Zugriff verweigern**.
   - **Zusätzliche Aktion ausführen**.
     Wählen Sie in der Dropdown-Liste die Aktion:
     - **Desinfizieren**.
     - **Desinfizieren. Löschen, falls Desinfektion fehlschlägt**.
     - **Löschen**.
     - **Empfohlen**.
4. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - **Nur informieren**.
   - **Zugriff verweigern**.
   - **Zusätzliche Aktion ausführen**.
     Wählen Sie in der Dropdown-Liste die Aktion:
     - **In Quarantäne verschieben**.
     - **Löschen**.

- **Empfohlen**.

5. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:

   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktionen je nach Typ des erkannten Objekts ausführen**.

   b. Klicken Sie auf die Schaltfläche **Einstellungen**.

   c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts eine primäre und eine sekundäre Aktion aus (die auszuführen ist, falls die primäre Aktion nicht durchgeführt werden kann).

   d. Klicken Sie auf **OK**.

6. Wählen Sie Aktion für nicht veränderbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann**.

7. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

So optimieren Sie die Leistungseinstellungen der Aufgabe zum Echtzeitschutz für Dateien:

1. Öffnen Sie das Fenster **Einstellungen für den Echtzeitschutz für Dateien anpassen**.

2. Wählen Sie die Registerkarte **Optimierung** aus.

3. Im Abschnitt **Ausnahmen**:

   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Nicht erkennen**.
   - Klicken Sie für jede Einstellung auf die Schaltfläche **Ändern**, um Ausnahmen hinzuzufügen.

4. Im Abschnitt **Erweiterte Einstellungen**:

   - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
   - **Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)**
   - **iSwift-Technologie verwenden**
   - **iChecker-Technologie verwenden**

Aufgabe zum Echtzeitschutz für Dateien über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem geschützten Gerät konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Aufgabeneinstellungen für den Echtzeitschutz für Dateien öffnen

Um das Fenster für die allgemeinen Aufgabeneinstellungen zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien** aus.
3. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.
   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

Einstellungen für den Schutzbereich der Aufgabe zum Echtzeitschutz für Dateien öffnen

Um das Einstellungsfenster des Schutzbereiches für die Aufgabe zum Echtzeitschutz für Dateien zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien** aus.
3. Klicken Sie im Ergebnisbereich auf den Link **Schutzbereich anpassen**.
   Das Fenster **Schutzbereichseinstellungen** wird geöffnet.

Aufgabe zum Echtzeitschutz für Dateien anpassen

Um die Aufgabeneinstellungen für den Echtzeitschutz für Dateien anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:
   - Schutzmodus für Objekte
   - **Heuristische Analyse**

- Integration mit anderen Komponenten

3. Geben Sie auf den Registerkarten **Zeitplan** und **Erweitert** die geplanten Starteinstellungen an.

4. Klicken Sie im Fenster **Aufgabeneinstellungen** auf OK.

   Die Änderung der Einstellungen wird gespeichert.

5. Klicken Sie im Ergebnisfenster des Knotens **Echtzeitschutz für Dateien** auf den Link **Schutzbereich anpassen**.

6. Führen Sie folgende Aktionen aus:

   - Wählen Sie in der Dateistruktur oder Liste der Dateiressourcen des Geräts die Knoten oder Elemente aus, die Sie in den Schutzbereich der Aufgabe aufnehmen möchten.

   - Wählen Sie eine der voreingestellten Sicherheitsstufen aus oder passen Sie die Sicherheitseinstellungen der Objekte manuell an.

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

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in einer ausgeführten Aufgabe. Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Schutzmodus auswählen

Sie können den Schutzmodus in der Aufgabe Echtzeitschutz für Dateien auswählen. Im Abschnitt **Schutzmodus für Objekte** können Sie die Art der Zugriffsversuche festlegen, die Kaspersky Embedded Systems Security bei einer Untersuchung von Objekten ausführt.

Der Wert der Einstellung **Schutzmodus für Objekte** wird für den gesamten in der Aufgabe angegebenen Schutzbereich angewendet. Für diese Einstellung können keine unterschiedlichen Werte für einzelne Knoten des Schutzbereichs festgelegt werden.

Um den Schutzmodus auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.

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

   - **Intelligenter Modus**
   - **Beim Öffnen und Ändern**
   - **Beim Öffnen**
   - **Beim Ausführen**
   - **Tiefere Analyse startender Prozesse (Blockiert den Start eines Prozesses, bis die Analyse abgeschlossen ist)**

3. Klicken Sie auf **OK**.

Der ausgewählte Schutzmodus für die Objekte wird eingestellt.

Heuristische Analyse und Integration mit anderen Programmkomponenten

Die Aufgabe "Verwendung von KSN" kann nur gestartet werden, wenn die Erklärung zu Kaspersky Security Network akzeptiert wurde.

Um die heuristische Analyse und Integration mit anderen Programmkomponenten zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Heuristische Analyse verwenden**.
3. Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.
4. Konfigurieren Sie im Abschnitt **Integration mit anderen Komponenten** die folgenden Einstellungen:
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**.

     Klicken Sie auf den Link **Vertrauenswürdige Zone**, um die Einstellungen der vertrauenswürdigen Zone zu öffnen.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **KSN zum Schutz verwenden**.

     Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Daten über untersuchte Dateien senden** in den Aufgabeneinstellungen für die Verwendung von KSN aktiviert ist.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen**.
   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Untersuchung wichtiger Bereiche starten, wenn aktive Infektion erkannt wird**.
5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden angewandt.

Einstellungen für den Aufgabenzeitplan anpassen

In der Programmkonsole können Sie planen, wann lokale System- und benutzerdefinierte Aufgaben gestartet werden sollen. Sie können jedoch nicht planen, wann Gruppenaufgaben gestartet werden sollen.

So planen Sie eine Aufgabe:

1. Öffnen Sie das Kontextmenü der Aufgabe, die Sie planen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Zeitplan** das Kontrollkästchen **Aufgabe nach Zeitplan ausführen**.

4. Führen Sie die folgenden Schritte aus, um Zeitplan-Einstellungen festzulegen:

   a. Wählen Sie im Dropdown-Menü **Startintervall** eines der Folgenden aus:

   - **Alle n Stunden**: Um die Aufgabe in stündlichen Abständen auszuführen, geben Sie die Anzahl der Stunden im Feld **Alle** <Anzahl> **Stunden** ein.
   - **Alle n Tage**: Um die Aufgabe in täglichen Intervallen auszuführen; geben Sie die Anzahl der Tage im Feld **Alle** <Anzahl> **Tage** ein.
   - **Wöchentlich**: Um die Aufgabe in wöchentlichen Intervallen auszuführen; geben Sie die Anzahl der Wochen im Feld **Alle** <Anzahl> **Wochen am** ein. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (standardmäßig werden Aufgaben montags gestartet).
   - **Bei Programmstart**: Um die Aufgabe bei jedem Start von Kaspersky Embedded Systems Security auszuführen.
   - **Nach dem Update der Programm-Datenbanken**: Um die Aufgabe nach jedem Update der Programm-Datenbanken auszuführen.

   b. Geben Sie im Feld **Startzeit** den Zeitpunkt an, zu dem die Aufgabe zum ersten Mal gestartet werden soll.

   c. Geben Sie im Feld **Beginnen am** das Datum an, zu dem die Aufgabe zum ersten Mal gestartet werden soll.

   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 geschätzte Zeitpunkt des nächsten Aufgabenstarts angezeigt. Die geschätzte Zeit, die bis zum nächsten Aufgabenstart verbleibt, wird jedes Mal angezeigt, wenn Sie das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Zeitplan** öffnen.

   Im Feld **Nächster Start** wird der Wert **Durch Richtlinie verboten** angezeigt, wenn die Einstellungen der geltenden Richtlinie von Kaspersky Security Center den Start einer geplanten lokalen Systemaufgabe verhindern.

5. Verwenden Sie die Registerkarte **Erweitert**, um die folgenden Zeitplan-Einstellungen festzulegen:

   - Im Abschnitt **Einstellungen für das Anhalten der Aufgabe**:

     a. Wählen Sie das Kontrollkästchen **Dauer**. Geben Sie in die Felder rechts die maximale Aufgabendauer in Stunden und Minuten ein.

     b. Wählen Sie das Kontrollkästchen **Anhalten von**. Geben Sie in die Felder rechts ein, wann die Aufgabe angehalten und fortgesetzt werden soll (unter 24 Stunden).

   - Im Abschnitt **Erweiterte Einstellungen**:

     a. Wählen Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und geben das Enddatum des Aufgabenzeitplans an.

     b. Wählen Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, um übersprungene Aufgaben zu starten.

c. Aktivieren Sie das Kontrollkästchen **Aufgabenstart zufällig wählen innerhalb von** und geben Sie einen Wert in Minuten ein.

6. Klicken Sie auf **OK**.

Die Zeitplan-Einstellungen werden gespeichert.

Schutzbereich erstellen

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

Einstellungen für die Anzeige der freigegebenen Netzwerkordner anpassen

So wählen Sie die Art der Anzeige der freigegebenen Netzwerkordner beim Anpassen von Einstellungen für den Untersuchungsbereich aus:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Öffnen Sie die Dropdown-Liste im oberen linken Abschnitt des Fensters und wählen Sie eine der folgenden Optionen aus:

   - Wählen Sie den Punkt **Als Baumstruktur anzeigen**, wenn Sie möchten, dass die freigegebenen Netzwerkordner als Baumstruktur angezeigt werden.

   - Wählen Sie den Punkt **Als Liste anzeigen**, wenn Sie möchten, dass die freigegebenen Netzwerkordner des geschützten Computers in Form einer Liste angezeigt werden.

   Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Geräts als Liste angezeigt.

3. Klicken Sie auf die Schaltfläche **Speichern**.

Schutzbereich erstellen

Die Vorgehensweise beim Erstellen des Schutzbereichs in der Aufgabe zum Echtzeitschutz für Dateien hängt von der ausgewählten Anzeige der freigegebenen Netzwerkordner ab. Sie können die freigegebenen Netzwerkordner als Baumstruktur oder Liste (standardmäßig aktiviert) anzeigen.

Um auf die Aufgabe neue Schutzbereichseinstellungen anzuwenden, muss die Aufgabe zum Echtzeitschutz für Dateien neu gestartet werden.

Um mithilfe der Struktur der freigegebenen Netzwerkordner einen Schutzbereich zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Öffnen Sie im linken Teil des geöffneten Fensters die Struktur mit den freigegebenen Netzwerkordnern des Computers, um alle Knoten und untergeordneten Knoten anzuzeigen.

3. Führen Sie folgende Aktionen aus:

   - Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Schutzbereich ausschließen möchten.

   - Deaktivieren Sie das Kontrollkästchen **Arbeitsplatz**, um einzelne Knoten in den Schutzbereich einzuschließen, und gehen Sie wie folgt vor:

     - Um alle Laufwerke eines bestimmten Typs in den Schutzbereich aufzunehmen, aktivieren Sie das Kontrollkästchen neben dem Namen des entsprechenden Laufwerkstyps (z. B. um alle Wechseldatenträger auf dem Gerät einzuschließen, aktivieren Sie das Kontrollkästchen **Wechseldatenträger**).

     - Um ein einzelnes Laufwerk eines bestimmten Typs in den Schutzbereich aufzunehmen, öffnen Sie den Knoten, der die Liste dieses Laufwerkstyps enthält, und aktivieren Sie das Kontrollkästchen für das entsprechende Laufwerk. Um beispielsweise den Wechseldatenträger F: auszuwählen, öffnen Sie den Knoten **Wechseldatenträger** und aktivieren Sie das Kontrollkästchen für Laufwerk **F:**.

     - Wenn Sie nur einen einzelnen Ordner oder eine einzelne Datei auf dem Laufwerk in den Schutzbereich einschließen möchten, aktivieren Sie das Kontrollkästchen neben dem Namen dieses Ordners bzw. dieser Datei.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Das Fenster **Schutzbereichseinstellungen** wird geschlossen. Ihre neu konfigurierten Einstellungen werden gespeichert.

Um mithilfe der Liste der freigegebenen Netzwerkordner einen Schutzbereich zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Deaktivieren Sie das Kontrollkästchen **Arbeitsplatz**, um einzelne Knoten in den Schutzbereich einzuschließen, und gehen Sie wie folgt vor:

   a. Öffnen Sie das Kontextmenü des Schutzbereichs mit der rechten Maustaste.

   b. Wählen Sie im Kontextmenü der Tabelle den Punkt **Schutzbereich hinzufügen** aus.

   c. Wählen Sie im geöffneten Fenster **Schutzbereich hinzufügen** den Typ des Objektes aus, das Sie zum Schutzbereich hinzufügen möchten:

      - **Vordefinierter Bereich**, wenn Sie in den Schutzbereich einen der vordefinierten Bereiche auf dem Gerät aufnehmen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Schutzbereich aus.

      - **Laufwerk, Ordner oder Netzwerkobjekt**, wenn Sie in den Schutzbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Bereich über die Schaltfläche **Durchsuchen** aus.

      - **Datei**, wenn Sie in den Schutzbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Bereich über die Schaltfläche **Durchsuchen** aus.

Sie können ein Objekt nicht zum Schutzbereich hinzufügen, wenn es bereits als Ausnahme aus dem Schutzbereich hinzugefügt wurde.

3. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Schutzbereich ausschließen möchten, oder gehen Sie wie folgt vor:

   a. Öffnen Sie das Kontextmenü des Schutzbereichs mit der rechten Maustaste.

   b. Wählen Sie im Kontextmenü den Punkt **Ausnahme hinzufügen**.

   c. Wählen Sie im geöffneten Fenster **Ausnahme hinzufügen** den Typ des Objektes aus, das Sie als Ausnahme aus dem Schutzbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Schutzbereich.

4. Um den Schutzbereich einer vorhandenen Ausnahme zu ändern, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option **Bereich ändern**.

5. Um die Anzeige eines zuvor hinzugefügten Schutzbereiches bzw. einer Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des gewünschten Schutzbereichs die Option **Aus Liste löschen** aus.

   Der Schutzbereich wird aus dem Gültigkeitsbereich der Aufgabe zum Echtzeitschutz für Dateien bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner entfernt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Das Fenster **Schutzbereichseinstellungen** wird geschlossen. Ihre neu konfigurierten Einstellungen werden gespeichert.

Die Aufgabe Echtzeitschutz für Dateien kann gestartet werden, wenn mindestens ein Knoten der Struktur der Dateiressourcen des Geräts in einen Schutzbereich aufgenommen wurde.

Wenn Sie einen ungültigen Schutzbereich angeben, Sie beispielsweise verschiedene Sicherheitsparameterwerte für viele einzelne Knoten in der Dateistruktur des Geräts setzen, so kann dadurch die Untersuchung der Objekte bei Zugriff verlangsamt werden.

Netzwerkobjekte in den Schutzbereich aufnehmen

Sie können Netzlaufwerke, Ordner und Dateien in den Schutzbereich aufnehmen. Geben Sie dazu die Netzwerkpfade im UNC-Format (Universal Naming Convention) an.

Sie können keine Netzwerkordner untersuchen, wenn Sie unter dem Systemkonto arbeiten.

So fügen Sie ein Netzwerkobjekt zum Schutzbereich hinzu:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Öffnen Sie die Dropdown-Liste im oberen linken Bereich des Fensters und wählen Sie **Als Baumstruktur anzeigen** aus.

3. Gehen Sie im Kontextmenü des Knotens **Netzwerkumgebung** wie folgt vor:

   - Wählen Sie den Punkt **Netzwerkordner hinzufügen** aus, wenn Sie einen Netzwerkordner zum Schutzbereich hinzufügen möchten.

   - Wählen Sie den Punkt **Netzwerkdatei hinzufügen** aus, wenn Sie eine Netzwerkdatei zum Schutzbereich hinzufügen möchten.

4. Geben Sie den Pfad zum Netzwerkordner oder zur Datei im UNC-Format ein.

5. Drücken Sie die Taste **EINGABE**.

6. Aktivieren Sie das Kontrollkästchen neben dem Namen des hinzugefügten Netzwerkobjekts, um es in den Schutzbereich aufzunehmen.

7. Ändern Sie, falls erforderlich, die Sicherheitseinstellungen für das hinzugefügte Netzwerkobjekt.

8. Klicken Sie auf die Schaltfläche **Speichern**.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Virtuellen Schutzbereich erstellen

Sie können separate virtuelle Festplatten, Ordner oder Dateien nur dann zum Schutzbereich bzw. Untersuchungsbereich hinzufügen, wenn der Schutzbereich bzw. Untersuchungsbereich in Form einer Struktur der Dateiressourcen angezeigt wird.

Um eine virtuelle Festplatte zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Wählen Sie im linken unteren Teil des Fensters aus der Dropdown-Liste den Punkt **Als Baumstruktur anzeigen**.

3. Öffnen Sie das Kontextmenü des Knotens **Virtuelle Festplatten**.

4. Wählen Sie die Option **Virtuelle Festplatte hinzufügen** aus.

5. Wählen Sie in der Liste der verfügbaren Namen den Namen der gerade entstehenden virtuellen Festplatte aus.

6. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Datenträger, um diesen Datenträger in den Schutzbereich zu übernehmen.

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

Ihre neu konfigurierten Einstellungen werden gespeichert.

Um einen virtuellen Ordner oder eine virtuelle Datei zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Öffnen Sie die Dropdown-Liste im oberen linken Bereich des Fensters und wählen Sie **Als Baumstruktur anzeigen** aus.

3. Öffnen Sie das Kontextmenü der virtuellen Festplatte, der Sie den Ordner oder die Datei hinzufügen möchten, und wählen Sie einen der folgenden Punkte aus:

   - **Virtuellen Ordner hinzufügen**, wenn Sie einen virtuellen Ordner zum Schutzbereich hinzufügen möchten.
   - **Virtuelle Datei hinzufügen**, wenn Sie eine virtuelle Datei zum Schutzbereich hinzufügen möchten.

4. Tragen Sie im Eingabefeld den Namen für den Ordner bzw. die Datei ein.

5. In der Zeile mit dem Namen des erstellten Ordners bzw. der erstellten Datei aktivieren Sie das Kontrollkästchen, um den Ordner bzw. die Datei in den Schutzbereich zu übernehmen.

6. Klicken Sie im Fenster **Schutzbereichseinstellungen** auf die Schaltfläche **Speichern**.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Sicherheitseinstellungen manuell anpassen

Standardmäßig werden in den Aufgaben zum Echtzeit-Computerschutz die gleichen Sicherheitseinstellungen verwendet wie für den gesamten Schutzbereich. Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**.

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für einzelne Elemente in der Liste der Dateiressourcen des Geräts oder den Nodes in der Struktur festlegen.

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

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

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.

2. Wählen Sie im linken Bereich des Fensters den Knoten, dessen Sicherheitsanstellungen Sie konfigurieren möchten.

   Für einen ausgewählten Knoten oder ein Element im Schutzbereich kann eine vordefinierte Vorlage mit Sicherheitseinstellungen übernommen werden.

   Links im Fenster können Sie die Anzeige der freigegebenen Netzwerkordner auswählen, einen Schutzbereich erstellen oder einen virtuellen Schutzbereich erstellen.

3. Führen Sie im rechten Teil des Fensters eine der folgenden Aktionen aus:

   - Wählen Sie auf der Registerkarte **Sicherheitsstufe** die Sicherheitsstufe aus, die Sie übernehmen möchten.
   - Passen Sie die Sicherheitseinstellungen des ausgewählten Knotens oder Elements entsprechend ihren Anforderungen auf den folgenden Registerkarten an:
     - **Allgemein**
     - **Aktionen**

- Optimierung

4. Klicken Sie im Fenster **Schutzbereichseinstellungen** auf die Schaltfläche **Speichern**.

Die neuen Einstellungen des Schutzbereichs werden gespeichert.

Auswahl von vordefinierten Sicherheitsstufen für die Aufgabe Echtzeitschutz für Dateien

Sie können eine der folgenden drei vordefinierten Sicherheitsstufen für einen in der Baumstruktur oder Liste der Dateiressourcen des geschützten Geräts ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen** und **Maximale Sicherheit**.

Um eine der vordefinierten Sicherheitsstufen auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.
2. Wählen Sie in der Baumstruktur oder Liste der freigegebenen Netzwerkordner einen Knoten oder ein Element aus, um die vordefinierte Sicherheitsstufe festzulegen.
3. Vergewissern Sie sich, dass der ausgewählte Knoten bzw. das Element zum Schutzbereich gehört.
4. Wählen Sie im rechten Teil des Fensters auf der Registerkarte **Sicherheitsstufe** die Sicherheitsstufe aus, die Sie anwenden möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
5. Klicken Sie auf die Schaltfläche **Speichern**.

   Die Einstellungen der Aufgabe werden gespeichert und unverzüglich während der Ausführung der Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Allgemeine Aufgabeneinstellungen anpassen

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

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.
2. Wählen Sie die Registerkarte **Allgemein** aus.
3. Geben Sie im Abschnitt **Schutz von Objekten** die Objekte an, die Sie in den Schutzbereich einschließen möchten:
   - **Alle Objekte**
   - **Objekte, die nach Format untersucht werden**
   - **Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden**

- **Objekte, die nach der angegebenen Erweiterungsliste untersucht werden**
- **Bootsektoren und MBR**
- **Alternative NTFS-Ströme**

4. Aktivieren oder deaktivieren Sie im Gruppenfeld **Optimierung** das Kontrollkästchen **Nur neue und veränderte Dateien schützen**.

   Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

5. Geben Sie im Abschnitt **Schutz von zusammengesetzten Objekten** die zusammengesetzten Objekte an, die Sie in den Schutzbereich einschließen möchten:

   - **Alle**/**Nur neue Archive**
   - **Alle**/**Nur neue SFX-Archive**
   - **Alle**/**Nur neue E-Mail-Datenbanken**
   - **Alle**/**Nur neue gepackte Objekte**
   - **Alle**/**Nur neue E-Mails im Nur-Text-Format**
   - **Alle**/**Nur neue eingebettete OLE-Objekte**

6. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

So passen Sie Aktionen für infizierte und andere gefundene Objekte für die Aufgabe zum Echtzeitschutz für Dateien an:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.
2. Wählen Sie die Registerkarte **Aktionen** aus.
3. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:

   - **Nur informieren**.
   - **Zugriff verweigern**.
   - **Zusätzliche Aktion ausführen**.

     Wählen Sie in der Dropdown-Liste die Aktion:

     - **Desinfizieren**.
     - **Desinfizieren. Löschen, falls Desinfektion fehlschlägt**.

- **Löschen**.
- **Empfohlen**.

4. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - **Nur informieren**.
   - **Zugriff verweigern**.
   - **Zusätzliche Aktion ausführen**.

     Wählen Sie in der Dropdown-Liste die Aktion:
     - **In Quarantäne verschieben**.
     - **Löschen**.
     - **Empfohlen**.
5. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktionen je nach Typ des erkannten Objekts ausführen**.
   b. Klicken Sie auf die Schaltfläche **Einstellungen**.
   c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts eine primäre und eine sekundäre Aktion aus (die auszuführen ist, falls die primäre Aktion nicht durchgeführt werden kann).
   d. Klicken Sie auf **OK**.
6. Wählen Sie Aktion für nicht veränderbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann**.
7. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

So optimieren Sie die Leistungseinstellungen der Aufgabe zum Echtzeitschutz für Dateien:

1. Öffnen Sie das Fenster **Schutzbereichseinstellungen**.
2. Wählen Sie die Registerkarte **Optimierung** aus.
3. Im Abschnitt **Ausnahmen**:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Nicht erkennen**.
   - Klicken Sie für jede Einstellung auf die Schaltfläche **Ändern**, um Ausnahmen hinzuzufügen.

4. Im Abschnitt **Erweiterte Einstellungen**:

- Untersuchung beenden, wenn sie länger dauert als (Sek.)
- Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)
- iSwift-Technologie verwenden
- iChecker-Technologie verwenden

Statistik für die Aufgabe zum Echtzeitschutz für Dateien

Wenn die Aufgabe zum Echtzeitschutz für Dateien ausgeführt wird, können Sie in Echtzeit Informationen über die Anzahl der Objekte, die Kaspersky Embedded Systems Security seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen lassen.

So zeigen Sie die Aufgabenstatistiken für den Echtzeitschutz für Dateien an:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien** aus.

   Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Sie können Informationen über Objekte anzeigen, die Kaspersky Embedded Systems Security seit dem Aufgabenstart verarbeitet hat (siehe Tabelle unten).

Statistik für die Aufgabe zum Echtzeitschutz für Dateien

Feld	Beschreibung
Gefunden	Anzahl der Objekte, die von Kaspersky Embedded Systems Security gefunden wurden. Findet Kaspersky Embedded Systems Security beispielsweise in fünf Dateien ein und dasselbe schädliche Objekt, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Infizierte und andere gefundene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security als infiziert eingestuft hat, oder gefundene legale Software, die von Eindringlingen verwendet werden kann, um Ihr Gerät oder persönliche Daten zu beschädigen.
Möglicherweise infizierte Objekte gefunden	Anzahl der von Kaspersky Embedded Systems Security erkannten Objekte, die als möglicherweise infiziert eingestuft wurden.
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security aus folgenden Gründen nicht desinfiziert wurden: • Das erkannte Objekt ist von einem Typ, der nicht desinfiziert werden kann. • Bei der Desinfektion ist eine Störung aufgetreten.
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos versucht hat, in die Quarantäne zu verschieben, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Nicht gelöschte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos zu

Objekte	entfernen versucht hat, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht untersuchte Objekte	Anzahl der zum Schutzbereich gehörenden Objekte, die Kaspersky Embedded Systems Security nicht untersuchen konnte, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu kopieren versucht hat, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Verarbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden.
In Quarantäne verschoben	Anzahl der Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Embedded Systems Security im Backup gespeichert wurden.
Gelöschte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security entfernt wurden.
Kennwortgeschützte Objekte	Anzahl der Objekte (z. B. Archive), die von Kaspersky Embedded Systems Security übersprungen wurden, weil sie kennwortgeschützt sind.
Beschädigte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security übersprungen wurden, da ihr Format beschädigt war.
Verarbeitete Objekte	Objekte insgesamt, die von Kaspersky Embedded Systems Security verarbeitet wurden.

Sie können auch eine Statistik über die Ausführung der Aufgabe zum Echtzeitschutz für Dateien im Protokoll der Aufgabenausführung über den Link **Protokoll der Aufgabenausführung öffnen** im Abschnitt **Verwaltung** des Detailbereichs anzeigen.

Wenn der Wert im Feld **Ereignisse insgesamt** im Fenster des Protokolls der Aufgabenausführung zum Echtzeitschutz für Dateien größer als 0 ist, wird empfohlen, die Ereignisse im Protokoll der Aufgabenausführung auf der Registerkarte **Ereignisse** manuell zu bearbeiten.

Aufgabe zum Echtzeitschutz für Dateien über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe "Echtzeitschutz für Dateien" über die Benutzeroberfläche des Web-Plug-ins verwalten.

Konfigurieren der Aufgabe zum Echtzeitschutz für Dateien

Vordefinierte Sicherheitsstufe kann für die Aufgabe "Echtzeitschutz für Dateien" über das Web-Plug-in nicht geändert werden.

So konfigurieren Sie die Aufgabe "Echtzeitschutz für Dateien" über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen der Aufgabe zum Echtzeitschutz für Dateien

Einstellung	Beschreibung
Intelligenter Modus	Kaspersky Embedded Systems Security wählt die Objekte für die Untersuchung selbstständig aus. Ein Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn durch den Prozess mehrere Male auf das Objekt zugegriffen und von ihm verändert wird, untersucht Kaspersky Embedded Systems Security das Objekt nur nachdem das Objekt zum letzten Mal von dem Prozess gespeichert wurde.
Beim Öffnen	Kaspersky Embedded Systems Security untersucht alle Objekte, wenn diese zum Lesen, Ausführen oder Ändern geöffnet werden.
Beim Öffnen und Ändern	Kaspersky Embedded Systems Security untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern. Diese Variante gilt als Standard.
Beim Ausführen	Kaspersky Embedded Systems Security untersucht eine Datei nur beim Öffnen zum Ausführen.
Tiefere Analyse startender Prozesse (Blockiert den Start eines Prozesses, bis die Analyse abgeschlossen ist)	Kaspersky Embedded Systems Security führt eine längerdauernde Analyse startender Prozesse durch. Dies erhöht die Wahrscheinlichkeit, eine Bedrohung zu entdecken. Der Start des Prozesses wird bis zum Ende der Analyse blockiert.
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.
Ebene der heuristischen Analyse	Die Stufe der heuristischen Analyse 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 geringere Anzahl der Anweisungen 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-Experten. Diese Stufe gilt als Standard. • **Tief**. Bei der heuristischen Analyse wird eine höhere Anzahl der Anweisungen 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 zu einer erhöhten Anzahl an Fehlalarmen führen. Die Einstellung ist aktiv, wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist.
Vertrauenswürdige Zone anwenden	Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert. Ist das Kontrollkästchen aktiviert, fügt Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu. Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Embedded Systems Security die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs für die Aufgabe. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
KSN zum Schutz verwenden	Mit diesem Kontrollkästchen wird die Verwendung der KSN-Dienste aktiviert und deaktiviert. Wenn das Kontrollkästchen aktiviert ist, verwendet das Programm die Daten von Kaspersky Security Network um sicherzustellen, dass das Programm schneller auf neue Bedrohungen reagiert und die Wahrscheinlichkeit von Fehlalarmen verringert wird. Ist das Kontrollkästchen deaktiviert, werden die KSN-Dienste von der Aufgabe nicht verwendet. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Zugriff auf geteilte Netzwerkressourcen für die Hosts blockieren, von denen schädliche Aktivitäten ausgehen	Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, von denen eine bösartige Aktivität ausgeht, zur Liste der blockierten Hosts. Wenn das Kontrollkästchen aktiviert ist, fügt Kaspersky Embedded Systems Security die Hosts, von denen eine bösartige Aktivität ausgeht, zur Liste der blockierten Hosts hinzu. Ist das Kontrollkästchen nicht aktiviert, so fügt Kaspersky Embedded Systems Security die Hosts, von denen eine bösartige Aktivität ausgeht, nicht zur Liste der blockierten Hosts hinzu. Das Kontrollkästchen ist standardmäßig deaktiviert. Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen. Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

Untersuchung wichtiger Bereiche starten, wenn aktive Infektion erkannt wird	Wenn das Kontrollkästchen aktiviert ist und eine aktive Infektion erkannt wird, erstellt Kaspersky Embedded Systems Security eine temporäre Aufgabe zur Untersuchung wichtiger Bereiche und startet sie. Wenn die temporäre Aufgabe zur Untersuchung wichtiger Bereiche abgeschlossen ist, entfernt Kaspersky Embedded Systems Security die Aufgabe. Wenn das Kontrollkästchen deaktiviert ist und eine aktive Infektion erkannt wird, erstellt Kaspersky Embedded Systems Security keine temporäre Aufgabe zur Untersuchung wichtiger Bereiche und startet sie nicht. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Schutzbereich	Sie können die Sicherheitseinstellungen für den Schutzbereich anpassen.

Schutzbereich der Aufgabe anpassen

So konfigurieren Sie den Schutzbereich der Aufgabe zum Echtzeitschutz für Dateien:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Echtzeitschutz für Dateien** auf **Einstellungen**.
6. Wählen Sie den Abschnitt **Schutzbereich** aus.
7. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel hinzuzufügen.
   - Wählen Sie eine bestehende Regel aus und klicken Sie auf die Schaltfläche **Bearbeiten**.

   Das Fenster **Bereich ändern** wird geöffnet.
8. Stellen Sie die Umschaltfläche auf **Aktiv** wählen Sie einen Objekttyp aus.
9. Passen Sie im Abschnitt **Schutz von Objekten** folgende Einstellungen an:
   - **Schutzmodus für Objekte**:
     - Alle Objekte
     - Objekte, die nach Format untersucht werden
     - Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden
     - Objekte, die nach der angegebenen Erweiterungsliste untersucht werden
   - Bootsektoren und MBR untersuchen

- Alternative NTFS-Ströme untersuchen

10. Aktivieren oder deaktivieren Sie im Abschnitt **Schutz von Objekten** das Kontrollkästchen Nur neue und veränderte Dateien schützen.

11. Geben Sie im Abschnitt **Schutz von zusammengesetzten Objekten** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

    - Archive
    - SFX-Archive
    - Gepackte Objekte
    - E-Mail-Datenbanken
    - E-Mails im Nur-Text-Format
    - Eingebettete OLE-Objekte
    - Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann

12. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:

    - Nur informieren.
    - Zugriff verweigern.
    - **Zusätzliche Aktion ausführen**.

      Wählen Sie in der Dropdown-Liste die Aktion:

      - **Desinfizieren**.
      - **Desinfizieren. Löschen, falls Desinfektion fehlschlägt**.
      - Löschen.
      - Empfohlen.

13. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:

    - Nur informieren.
    - Zugriff verweigern.
    - **Zusätzliche Aktion ausführen**.

      Wählen Sie in der Dropdown-Liste die Aktion:

      - **In Quarantäne verschieben**.
      - Löschen.
      - Empfohlen.

14. 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**.

    b. Klicken Sie auf die Schaltfläche **Einstellungen**.

    c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts eine primäre und eine sekundäre Aktion aus (die auszuführen ist, falls die primäre Aktion nicht durchgeführt werden kann).

    d. Klicken Sie auf **OK**.

15. Konfigurieren Sie im Abschnitt **Ausnahmen** die folgenden Einstellungen:

    - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
    - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Nicht erkennen**.

16. Konfigurieren Sie im Abschnitt **Optimierung** die folgenden Einstellungen:

    - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
    - **Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)**
    - **iSwift-Technologie verwenden**
    - **iChecker-Technologie verwenden**

17. Klicken Sie auf die Schaltfläche **OK**.

Verwendung von KSN

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

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

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-Wissensdatenbank über die Reputation von Dateien, Web-Ressourcen und Programmen gewährleistet. Die Nutzung der Daten des Kaspersky Security Network gewährleistet eine schnellere Reaktion von Kaspersky Embedded Systems Security auf neue Bedrohungen, erhöht die Effektivität der Arbeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

Die Aufgabe "Verwendung von KSN" kann nur gestartet werden, wenn die Erklärung zu Kaspersky Security Network akzeptiert wurde.

Kaspersky Embedded Systems Security erhält von Kaspersky Security Network ausschließlich Informationen über die Reputation von Programmen.

Die Teilnahme von Benutzern an KSN ermöglicht es Kaspersky, schnell Informationen über Typen und Quellen neuer Bedrohungen zu erhalten, Neutralisierungsmethoden zu entwickeln und die Anzahl an Fehlalarmen der Programmkomponenten zu reduzieren.

Ausführliche Informationen über die Übertragung, Verarbeitung, Speicherung und Vernichtung von Daten über die Programmnutzung finden Sie im Fenster **Datenverarbeitung** der Aufgabe "Verwendung von KSN" sowie in der Datenschutzrichtlinie auf der Website von Kaspersky.

Die Teilnahme an Kaspersky Security Network ist freiwillig. Sie können nach der Installation von Kaspersky Embedded Systems Security entscheiden, ob Sie an Kaspersky Security Network teilnehmen möchten. Sie können Ihre Entscheidung über die Teilnahme an Kaspersky Security Network jederzeit ändern.

Das Kaspersky Security Network kann in den folgenden Aufgaben von Kaspersky Embedded Systems Security verwendet werden:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Kontrolle des Programmstarts

Kaspersky Private Security Network

Ausführliche Informationen über die Konfiguration von Kaspersky Private Security Network (im Weiteren "Private KSN") finden Sie im *Hilfesystem von Kaspersky Security Center*.

Wenn Sie Private KSN auf dem Gerät verwenden, können Sie im Fenster **Datenverarbeitung** der Aufgabe zur Verwendung von KSN die KSN-Erklärung lesen und die Aufgabe mithilfe des Kontrollkästchens **Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network** aktivieren. Indem Sie die Bedingungen akzeptieren, erklären Sie sich damit einverstanden, dass alle Datentypen, die in der KSN-Erklärung genannt werden (Sicherheitsanfragen, Statistikdaten), an den KSN-Dienst gesendet werden.

Nach der Annahme der Private-KSN-Bedingungen sind die Kontrollkästchen für die Verwendung von Global KSN nicht mehr verfügbar.

Wenn Sie Private KSN deaktivieren, während die Aufgabe "Verwendung von KSN" läuft, wird der Fehler *Lizenzverletzung* angezeigt und die Aufgabe beendet. Um das Gerät 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 an Kaspersky Security Network senden**: Das Programm stellt die Aufbereitung von Daten mit zusätzlichen KSN-Statistiken ein.
- Deaktivieren des Kontrollkästchens **Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network**: Das Programm stellt jegliche KSN-bezogene Datenverarbeitung ein und die Aufgabe "Verwendung von KSN" wird gestoppt.
- Deinstallation der Komponente "Verwendung von KSN": Jegliche Verarbeitung KSN-bezogener Daten wird gestoppt.
- Deinstallation von Kaspersky Embedded Systems Security: Jegliche Verarbeitung KSN-bezogener Daten wird gestoppt.
- Deinstallation eines Lizenzschlüssels für Kaspersky Embedded Systems Security oder Aussetzen der Lizenz: Jegliche Verarbeitung KSN-bezogener Daten wird gestoppt.

Standardeinstellungen der Aufgabe "Verwendung von KSN"

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

Standardeinstellungen der Aufgabe "Verwendung von KSN"

Einstellung	Standardwert	Beschreibung
Aktion für Objekte, die in KSN nicht	Löschen	Sie können die Aktionen festlegen, die Kaspersky Embedded Systems Security in Bezug auf Objekte ausführen soll, die laut KSN als nicht vertrauenswürdig eingestuft sind.

vertrauenswürdig sind		
Versand von Daten	Die Prüfsumme der Datei (MD5-Hash) wird für Dateien berechnet, deren Größe nicht mehr als 2 MB beträgt.	Sie können die maximale Dateigröße angeben, bis zu der die Prüfsumme nach dem Algorithmus MD5 für den Versand an KSN berechnet werden soll. Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security den MD5-Hash für Dateien beliebiger Größe.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.
Kaspersky Security Center als KSN-Proxyserver verwenden	Ausgewählt	Die Daten werden standardmäßig über das Kaspersky Security Center an KSN gesendet. Sie können diese Einstellung nur über das Verwaltungs-Plug-in ändern
Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network	Deaktiviert	Wenn diese Option ausgewählt ist, wird die Teilnahme an KSN nach der Installation gewährt. Sie können Ihre Entscheidung jederzeit ändern.
Statistiken an 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.

Verwendung von KSN über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe zur Verwendung von KSN und die Datenverwaltung über das Verwaltungs-Plug-in konfigurieren.

Konfiguration der Aufgabe Verwendung von KSN

So konfigurieren Sie die Aufgabe "Verwendung von KSN":

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.

- Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **Echtzeit-Computerschutz** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Verwendung von KSN**.

   Das Fenster **Verwendung von KSN** wird geöffnet.

5. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:

   - Geben Sie im Abschnitt **Aktion für Objekte, die in KSN nicht vertrauenswürdig sind** die Aktion an, die Kaspersky Embedded Systems Security ausführen soll, wenn ein Objekt gefunden wird, das laut KSN als nicht vertrauenswürdig eingestuft ist:

     - **Löschen**
     - **Informationen protokollieren**

   - Begrenzen Sie im Abschnitt **Versand von Daten** die Größe der Dateien, für die eine Prüfsumme berechnet werden soll:

     - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Keine Prüfsumme für den Versand an KSN berechnen für Dateien, die größer sind als (MB)**.
     - Ändern Sie bei Bedarf im Feld rechts die maximale Dateigröße, bis zu der Kaspersky Embedded Systems Security die Prüfsumme berechnen soll.

   - Aktivieren oder deaktivieren Sie im Abschnitt **KSN-Proxyserver** das Kontrollkästchen **Kaspersky Security Center als KSN-Proxyserver verwenden**.

     Der KSN-Proxyserver kann nur aktiviert werden, wenn die KSN-Erklärung akzeptiert wurde und Kaspersky Security Center ordnungsgemäß konfiguriert ist. Weitere Informationen finden Sie im *Hilfesystem von Kaspersky Security Center*.

6. Passen Sie bei Bedarf den Zeitplan für den Aufgabenstart auf der Registerkarte **Aufgabenverwaltung** an. Sie können beispielsweise die Aufgabe nach Zeitplan starten und als Intervall **Bei Programmstart** angeben, wenn Sie möchten, dass die Aufgabe nach dem Neustart des geschützten Geräts automatisch gestartet wird.

   Das Programm startet die Aufgabe Verwendung von KSN zukünftig nach Zeitplan.

7. Konfigurieren Sie die Datenverarbeitung, bevor Sie die Aufgabe starten.

8. Klicken Sie auf **OK**.

Die vorgenommenen Änderungen der Aufgabe werden übernommen. Datum und Uhrzeit der Änderung sowie Informationen über die Einstellungen der Aufgabe vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

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 den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Echtzeit-Computerschutz** auf die Schaltfläche **Datenverarbeitung** im Unterabschnitt **Verwendung von KSN**.

   Das Fenster **KSN-Datenverarbeitung** wird geöffnet.
5. Lesen Sie auf der Registerkarte **Statistiken und Dienste** die Erklärung und wählen Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network**.
6. Um die Schutzstufe zu erhöhen, werden die folgenden Kontrollkästchen automatisch aktiviert:
   - **Daten über untersuchte Dateien senden**.
   - **Statistiken an Kaspersky Security Network senden**.

   Sie können diese Kontrollkästchen deaktivieren und das Senden zusätzlicher Daten jederzeit unterbinden.
7. Das Kontrollkästchen **Statistiken an Kaspersky Security Network senden** ist standardmäßig aktiviert. Sie können dieses Kontrollkästchen jederzeit deaktivieren, wenn Sie nicht möchten, dass Kaspersky Embedded Systems Security zusätzliche Statistikdaten an Kaspersky sendet.
8. Klicken Sie auf **OK**.

   Die vorgenommenen Einstellungen der Datenverarbeitung werden gespeichert.

Verwendung von KSN über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe zur Verwendung von KSN und die Datenverwaltung über die Programmkonsole konfigurieren.

Konfiguration der Aufgabe Verwendung von KSN

So konfigurieren Sie die Aufgabe "Verwendung von KSN":

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Verwendung von KSN**.
3. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** wird geöffnet.
4. Passen Sie die Aufgabeneinstellungen an:
   - Geben Sie im Abschnitt **Aktion für Objekte, die in KSN nicht vertrauenswürdig sind** die Aktion an, die Kaspersky Embedded Systems Security ausführen soll, wenn ein Objekt gefunden wird, das laut KSN als nicht vertrauenswürdig eingestuft ist:
     - **Löschen**
     - **Informationen protokollieren**
   - Begrenzen Sie im Abschnitt **Versand von Daten** die Größe der Dateien, für die eine Prüfsumme berechnet werden soll:
     - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Keine Prüfsumme für den Versand an KSN berechnen für Dateien, die größer sind als (MB)**.
     - Ändern Sie bei Bedarf im Feld rechts die maximale Dateigröße, bis zu der Kaspersky Embedded Systems Security die Prüfsumme berechnen soll.
5. Passen Sie bei Bedarf den Zeitplan für den Aufgabenstart auf den Registerkarten **Zeitplan** und **Erweitert** an. Sie können beispielsweise den Aufgabenstart nach Zeitplan aktivieren und als Intervall für den Aufgabenstart **Bei Programmstart** angeben, wenn Sie möchten, dass die Aufgabe nach dem Neustart des geschützten Geräts automatisch gestartet wird.

   Das Programm startet die Aufgabe Verwendung von KSN zukünftig nach Zeitplan.
6. Konfigurieren Sie die Datenverarbeitung, bevor Sie die Aufgabe starten.
7. Klicken Sie auf **OK**.

Die vorgenommenen Änderungen der Aufgabe werden übernommen. Datum und Uhrzeit der Änderung sowie Informationen über die Einstellungen der Aufgabe vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

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. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.

2. Wählen Sie den untergeordneten Knoten **Verwendung von KSN**.
3. Klicken Sie im Ergebnisbereich auf den Link **Datenverarbeitung**.

   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 zur Teilnahme an Kaspersky Security Network**.
5. Um die Schutzstufe zu erhöhen, werden die folgenden Kontrollkästchen automatisch aktiviert:

   - Daten über untersuchte Dateien senden.
   - Statistiken an Kaspersky Security Network senden.

   Sie können diese Kontrollkästchen deaktivieren und das Senden zusätzlicher Daten jederzeit unterbinden.
6. Das Kontrollkästchen Statistiken an Kaspersky Security Network senden ist standardmäßig aktiviert. Sie können dieses Kontrollkästchen jederzeit deaktivieren, wenn Sie nicht möchten, dass Kaspersky Embedded Systems Security zusätzliche Statistikdaten an Kaspersky sendet.
7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen der Datenverarbeitung werden gespeichert.

Verwendung von KSN über das Web-Plug-in verwalten

So konfigurieren Sie die Aufgabe zur Verwendung von KSN und die Datenverwaltung über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Unterabschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Verwendung von KSN** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen für die Aufgabe zur Verwendung von KSN und Datenverwaltung über das Verwaltungs-Plug-in

Einstellung	Beschreibung
Löschen	Kaspersky Embedded Systems Security löscht das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, und verschiebt eine Kopie davon ins Backup. Diese Variante gilt als Standard.
Informationen protokollieren	Kaspersky Embedded Systems Security nimmt Informationen über das Objekt, das von KSN als nicht vertrauenswürdig angesehen wird, in das Protokoll der Aufgabenausführung auf. Das nicht vertrauenswürdige Objekt wird von Kaspersky Embedded Systems Security nicht gelöscht.
Keine Prüfsumme für den Versand an	Über dieses Kontrollkästchen lässt sich die Ermittlung der Prüfsumme von Dateien ab einer bestimmten Größe für den Versand dieser Informationen an die

KSN berechnen für Dateien, die größer sind als	KSN-Dienste aktivieren bzw. deaktivieren. Wie viel Zeit die Ermittlung der Prüfsumme beansprucht, hängt von der Dateigröße ab. Ist das Kontrollkästchen aktiviert, wird die Prüfsumme für Dateien, deren Größe den in MB festgelegten Wert übersteigt, von Kaspersky Embedded Systems Security nicht ermittelt. Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Embedded Systems Security die Prüfsumme für Dateien beliebiger Größe. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Ich bestätige, dass ich alle Bedingungen zur Teilnahme an Kaspersky Security Network vollständig gelesen habe, und sie verstehe und akzeptiere	Mit der Aktivierung dieses Kontrollkästchens bestätigen Sie, dass Sie die Bedingungen der Erklärung zu Kaspersky Security Network gelesen und akzeptiert haben.
Daten über untersuchte Dateien senden	Ist dieses Kontrollkästchen aktiviert, sendet Kaspersky Embedded Systems Security die Prüfsumme der untersuchten Dateien an Kaspersky. Die Einstufung der Sicherheit jeder Datei basiert auf der von KSN bereitgestellten Reputation. Ist dieses Kontrollkästchen deaktiviert, sendet Kaspersky Embedded Systems Security die Prüfsumme der Dateien nicht an KSN. Beachten Sie, dass die Anfragen bezüglich der Reputation von Dateien möglicherweise in einem eingeschränkten Modus gesendet werden. Die Einschränkungen werden zum Schutz der Reputationsserver von Kaspersky 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 festgelegten Regeln und Methoden definiert und können nicht von einem Benutzer eines geschützten Geräts konfiguriert werden. Aktualisierungen dieser Regeln und Methoden erfolgen zusammen mit den Datenbank-Updates des Programms. Wenn die Einschränkungen angewendet werden, wird der Status *aktiviert von Kaspersky zum Schutz von KSN-Servern vor DDoS* in den Statistiken der Aufgabe "Verwendung von KSN" angezeigt. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Der Verarbeitung von Daten als Teil der Statistik für Kaspersky Security Network zustimmen	Wenn dieses Kontrollkästchen aktiviert ist, sendet Kaspersky Embedded Systems Security zusätzliche Statistikdaten, zu denen auch persönliche Daten gehören können. Die Liste mit allen Datenarten, die als KSN-Statistiken gesendet werden, ist in der KSN-Erklärung enthalten. Die von Kaspersky erhaltenen Daten werden dazu verwendet, um die Qualität der Programme und das Niveau des Erkennens von Bedrohungen zu steigern. Ist das Kontrollkästchen deaktiviert, versendet Kaspersky Embedded Systems Security keine zusätzlichen Statistikdaten. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Aufgabenverwaltung	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Konfiguration des zusätzlichen Versands von Daten

Kaspersky Embedded Systems Security kann konfiguriert werden, um die folgenden Daten an Kaspersky zu senden:

- Prüfsummen untersuchter Dateien (Kontrollkästchen **Daten über untersuchte Dateien senden**).
- Zusätzliche Statistiken, einschließlich persönlicher Daten (Kontrollkästchen **Statistiken an Kaspersky Security Network senden**).

Genauere Informationen zu Daten, die an Kaspersky gesendet werden, finden Sie im Abschnitt "Lokale Datenverarbeitung" dieses Handbuchs.

Die entsprechenden Kontrollkästchen können nur dann aktiviert bzw. deaktiviert werden, wenn das Kontrollkästchen **Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network** aktiviert ist.

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

Das Kontrollkästchen **Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network** ist nur dann nicht editierbar, wenn die Richtlinie des Kaspersky Security Center Änderungen der Einstellungen für die Datenverarbeitung blockiert.

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 an Kaspersky Security Network senden	Bedingungen für den Status des Kontrollkästchens Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Security Network
☑	• Anfragen bezüglich der Reputation werden gesendet • Kontrollkästchen ist editierbar	• Zusätzliche Statistiken werden gesendet • Kontrollkästchen ist editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network werden akzeptiert • Kontrollkästchen ist editierbar
☑	• Anfragen bezüglich der Reputation werden gesendet • Kontrollkästchen ist nicht editierbar	• Zusätzliche Statistiken werden gesendet • Kontrollkästchen ist nicht editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network werden akzeptiert • Kontrollkästchen ist nicht editierbar
☐	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network werden nicht akzeptiert • Kontrollkästchen ist editierbar

☐	• Anfragen bezüglich der Reputation werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Zusätzliche Statistiken werden nicht gesendet • Kontrollkästchen ist nicht editierbar	• Die Bedingungen der Erklärung zu Kaspersky Security Network werden nicht akzeptiert • Kontrollkästchen ist nicht editierbar

Statistik für die Aufgabe Verwendung von KSN

Während die Aufgabe zur Verwendung von KSN ausgeführt wird, können Sie in Echtzeit Informationen über die Anzahl der Objekte, die Kaspersky Embedded Systems Security seit seinem Start bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen lassen. Informationen über alle Ereignisse, die während der Aufgabenausführung eintreten, werden in das Protokoll der Aufgabenausführung aufgenommen.

So zeigen Sie die Statistik für die Aufgabe "Verwendung von KSN" an:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Verwendung von KSN**.

Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Sie können Informationen über Objekte aufrufen, die Kaspersky Embedded Systems Security während der Ausführung der Aufgabe verarbeitet hat (siehe Tabelle unten).

Statistik für die Aufgabe Verwendung von KSN

Feld	Beschreibung
Fehler beim Versand von Anfragen	Anzahl der Anfragen an KSN, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Statistiken erstellt	Anzahl der erstellten Statistikpakete, die an KSN gesendet wurden.
Gelöschte Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security während der Ausführung der Aufgabe zur Verwendung von KSN entfernt hat.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Embedded Systems Security im Backup gespeichert wurden.
Nicht gelöschte Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos zu entfernen versucht hat, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war. Die Informationen über diese Objekte werden in das Protokoll der Aufgabenausführung aufgenommen.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu kopieren versucht hat, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war. Dateien, die nicht in den Backup verschoben werden konnten, werden durch das Programm weder desinfiziert noch gelöscht. Die Informationen über diese Objekte werden in das Protokoll der Aufgabenausführung aufgenommen.
Begrenzter Modus	Der Status gibt an, ob die Anwendung Datei-Reputationsanforderungen in einem begrenzten Modus sendet. Im begrenzten Modus sendet Kaspersky Embedded Systems

	Security gemäß den Empfehlungen der Spezialisten von Kaspersky nur einen Teil der Datei-Reputationsanforderungen.

Schutz vor Netzwerkbedrohungen

Dieser Abschnitt informiert über die Aufgabe "Schutz vor Netzwerkbedrohungen" und erläutert die Konfiguration dieser Aufgabe.

Informationen zur Aufgabe "Schutz vor Netzwerkbedrohungen"

"Schutz vor Netzwerkbedrohungen" kann nur auf einem Gerät installiert werden, dass unter Microsoft Windows 7 oder höher oder unter Windows Server 2008 R2 oder höher ausgeführt wird.

Die Aufgabe "Schutz vor Netzwerkbedrohungen" untersucht eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind. Wird ein versuchter Netzwerkangriff erkannt, der auf den Computer abzielt, blockiert Kaspersky Embedded Systems Security die Netzwerkaktivitäten vom angreifenden Computer. Auf Ihrem Bildschirm wird eine Warnung angezeigt, die besagt, dass ein Netzwerkangriff versucht wurde. Zudem werden Informationen zum angreifenden Computer angezeigt.

Standardmäßig wird die Aufgabe zum Schutz vor Netzwerkbedrohungen im Modus **Verbindungen bei erkanntem Angriff blockieren** ausgeführt. In diesem Modus fügt Kaspersky Embedded Systems Security der Liste der blockierten Hosts die IP-Adressen von Hosts hinzu, welche die für Netzwerkangriffe typischen Aktivitäten anzeigen.

Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

Die IP-Adressen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, werden in den folgenden Fällen aus der Liste der blockierten Hosts gelöscht:

- Kaspersky Embedded Systems Security wird deinstalliert.
- Die IP-Adresse wurde manuell aus der Liste der blockierten Hosts gelöscht.
- Die Blockierdauer des Hosts ist abgelaufen.
- Die Aufgabe zum Schutz vor Netzwerkbedrohungen wurde angehalten und das Kontrollkästchen **Datenverkehrsanalyse nicht stoppen, wenn die Aufgabe nicht ausgeführt wird** ist deaktiviert.
- Der Modus **Verbindungen bei erkanntem Angriff blockieren** wurde deaktiviert.

Standardeinstellungen der Aufgabe "Schutz vor Netzwerkbedrohungen"

Die Aufgabe "Schutz vor Netzwerkbedrohungen" verwendet die in der Tabelle unten beschriebenen Standardeinstellungen. Sie können die Werte dieser Parameter ändern.

Standardeinstellungen der Aufgabe "Schutz vor Netzwerkbedrohungen"

Einstellung	Standardwert	Beschreibung
Verarbeitungsmodus	**Verbindungen bei**	Die Aufgabe "Schutz vor Netzwerkbedrohungen" kann in

	erkanntem Angriff blockieren	den Modi **Pass-Through** gestartet werden, und **Über Netzwerkangriffe nur informieren** oder **Verbindungen bei erkanntem Angriff blockieren**. Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, zur Liste der blockierten Hosts. Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten und fügt die IP-Adressen von Hosts, welche die für Netzwerkangriffe typischen Aktivitäten zeigen, der Liste der blockierten Hosts hinzu. Dieser Modus ist standardmäßig eingestellt. Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen. Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen. Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten, aber blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen. Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, aber protokolliert keine erkannten Aktivitäten und blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen. Sie können diesen Modus beispielsweise verwenden, wenn die Leistung des geschützten Geräts abnimmt.
Ausnahmen	Die Ausnahmeliste wird nicht angewendet.	Wählen Sie Bereiche aus, die Sie vom Schutzbereich der Aufgabe ausschließen wollen.
Zeitplan-Einstellungen	Die Aufgabe zum Schutz vor Netzwerkbedrohungen wird automatisch zeitgleich mit dem	Sie können den Zeitplan anpassen.

	Start von Kaspersky Embedded Systems Security gestartet.	

Aufgabe "Schutz vor Netzwerkbedrohungen" über die Programmkonsole konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe "Schutz vor Netzwerkbedrohungen" über die Benutzeroberfläche der Programmkonsole verwalten.

Allgemeine Aufgabeneinstellungen

Um den Zeitplan einer allgemeinen Aufgabe anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Schutz vor Netzwerkbedrohungen** aus.
3. Klicken Sie im Detailbereich des Knotens **Eigenschaften** auf den Link **Schutz vor Netzwerkbedrohungen**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Öffnen Sie die Registerkarte **Allgemein**.
5. Wählen Sie im Abschnitt **Verarbeitungsmodus** den Verarbeitungsmodus aus:

   - **Pass-Through**.

     Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, aber protokolliert keine erkannten Aktivitäten und blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

     Sie können diesen Modus beispielsweise verwenden, wenn die Leistung des geschützten Geräts abnimmt.

   - **Über Netzwerkangriffe nur informieren**.

     Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten, aber blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

   - **Verbindungen bei erkanntem Angriff blockieren**.

Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, zur Liste der blockierten Hosts.

Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten und fügt die IP-Adressen von Hosts, welche die für Netzwerkangriffe typischen Aktivitäten zeigen, der Liste der blockierten Hosts hinzu.

Dieser Modus ist standardmäßig eingestellt.

Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

6. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datenverkehrsanalyse nicht stoppen, wenn die Aufgabe nicht ausgeführt wird**.

   Ist dieses Kontrollkästchen aktiviert, wenn die Aufgabe zum Schutz vor Netzwerkbedrohungen angehalten wird, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert Netzwerkaktivitäten vom angreifenden Computer abhängig vom ausgewählten Verarbeitungsmodus.

   Ist dieses Kontrollkästchen deaktiviert, wenn die Aufgabe "Schutz vor Netzwerkbedrohungen" angehalten wird, untersucht Kaspersky Security für Windows Server den eingehenden Netzwerkverkehr nicht auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

7. Klicken Sie auf **OK**.

Ausnahmen hinzufügen

Gehen Sie wie folgt vor, um Ausnahmen der Aufgabe "Schutz vor Netzwerkbedrohungen" hinzuzufügen:

1. Öffnen Sie in der Programmkonsolenstruktur den Knoten **Echtzeit-Computerschutz**.
2. Wählen Sie den untergeordneten Knoten **Schutz vor Netzwerkbedrohungen** aus.
3. Klicken Sie im Detailbereich des Knotens **Eigenschaften** auf den Link **Schutz vor Netzwerkbedrohungen**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Ausnahmen** das Kontrollkästchen **Ausgenommene IP-Adressen nicht kontrollieren**.

   Ist dieses Kontrollkästchen aktiviert, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr nicht auf ausgenommene IP-Adressen.

   Ist dieses Kontrollkästchen deaktiviert, wendet Kaspersky Embedded Systems Security die Ausnahmeliste nicht an.

5. Geben Sie die IP-Adresse an, und klicken Sie auf **Hinzufügen**.

6. Klicken Sie auf **OK**.

Aufgabe "Schutz vor Netzwerkbedrohungen" über das Verwaltungs-Plug-in konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe "Schutz vor Netzwerkbedrohungen" über die Benutzeroberfläche des Verwaltungs-Plug-ins verwalten.

Allgemeine Aufgabeneinstellungen

Um den Zeitplan einer allgemeinen Aufgabe anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Echtzeit-Computerschutz** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

   Das Fenster **Schutz vor Netzwerkbedrohungen** wird geöffnet.
5. Öffnen Sie die Registerkarte **Allgemein**.
6. Wählen Sie im Abschnitt **Verarbeitungsmodus** den Verarbeitungsmodus aus:
   - **Pass-Through**.

     Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, aber protokolliert keine erkannten Aktivitäten und blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

     Sie können diesen Modus beispielsweise verwenden, wenn die Leistung des geschützten Geräts abnimmt.
   - **Über Netzwerkangriffe nur informieren**.

Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten, aber blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

- **Verbindungen bei erkanntem Angriff blockieren**.

  Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, zur Liste der blockierten Hosts.

  Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten und fügt die IP-Adressen von Hosts, welche die für Netzwerkangriffe typischen Aktivitäten zeigen, der Liste der blockierten Hosts hinzu.

  Dieser Modus ist standardmäßig eingestellt.

  Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

  Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

7. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datenverkehrsanalyse nicht stoppen, wenn die Aufgabe nicht ausgeführt wird**.

   Ist dieses Kontrollkästchen aktiviert, wenn die Aufgabe zum Schutz vor Netzwerkbedrohungen angehalten wird, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert Netzwerkaktivitäten vom angreifenden Computer abhängig vom ausgewählten Verarbeitungsmodus.

   Ist dieses Kontrollkästchen deaktiviert, wenn die Aufgabe "Schutz vor Netzwerkbedrohungen" angehalten wird, untersucht Kaspersky Security für Windows Server den eingehenden Netzwerkverkehr nicht auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

8. Klicken Sie auf **OK**.

Ausnahmen hinzufügen

Gehen Sie wie folgt vor, um Ausnahmen der Aufgabe "Schutz vor Netzwerkbedrohungen" hinzuzufügen:

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

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

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

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

- Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **Echtzeit-Computerschutz** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Schutz vor Netzwerkbedrohungen**.

   Das Fenster **Schutz vor Netzwerkbedrohungen** wird geöffnet.

5. Aktivieren Sie auf der Registerkarte **Ausnahmen** das Kontrollkästchen **Ausgenommene IP-Adressen nicht kontrollieren**.

   Ist dieses Kontrollkästchen aktiviert, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr nicht auf ausgenommene IP-Adressen.

   Ist dieses Kontrollkästchen deaktiviert, wendet Kaspersky Embedded Systems Security die Ausnahmeliste nicht an.

6. Geben Sie die IP-Adresse an, und klicken Sie auf **Hinzufügen**.

7. Klicken Sie auf **OK**.

Aufgabe "Schutz vor Netzwerkbedrohungen" über das Web-Plug-in konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die Aufgabe "Schutz vor Netzwerkbedrohungen" über die Benutzeroberfläche des Web-Plug-ins verwalten.

Allgemeine Aufgabeneinstellungen

Um den Zeitplan einer allgemeinen Aufgabe anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.

4. Wählen Sie den Abschnitt **Echtzeitschutz für Computer** aus.

5. Klicken Sie im Unterabschnitt **Schutz vor Netzwerkbedrohungen** auf **Einstellungen**.

6. Öffnen Sie die Registerkarte **Allgemein**.

7. Wählen Sie im Abschnitt **Verarbeitungsmodus** den Verarbeitungsmodus aus:

- **Pass-Through**.

  Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, aber protokolliert keine erkannten Aktivitäten und blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

  Sie können diesen Modus beispielsweise verwenden, wenn die Leistung des geschützten Geräts abnimmt.

- **Über Netzwerkangriffe nur informieren**.

  Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten, aber blockierte keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

- **Verbindungen bei erkanntem Angriff blockieren**.

  Mit diesem Kontrollkästchen aktivieren oder deaktivieren Sie das Hinzufügen von Hosts, die für Netzwerkangriffe typische Aktivitäten zeigen, zur Liste der blockierten Hosts.

  Wurde dieser Modus ausgewählt, untersucht Kaspersky Embedded Systems Security eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, protokolliert Ereignisse über erkannte Aktivitäten und fügt die IP-Adressen von Hosts, welche die für Netzwerkangriffe typischen Aktivitäten zeigen, der Liste der blockierten Hosts hinzu.

  Dieser Modus ist standardmäßig eingestellt.

  Sie können die Liste der blockierten Hosts im Speicher der blockierten Hosts einsehen.

  Sie können den Zugriff auf blockierte Hosts wiederherstellen, indem Sie in den Einstellungen für den Speicher der blockierten Hosts die Anzahl der Tage, Stunden und Minuten angeben, nach deren Ablauf blockierte Hosts wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.

8. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datenverkehrsanalyse nicht stoppen, wenn die Aufgabe nicht ausgeführt wird**.

   Ist dieses Kontrollkästchen aktiviert, wenn die Aufgabe zum Schutz vor Netzwerkbedrohungen angehalten wird, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert Netzwerkaktivitäten vom angreifenden Computer abhängig vom ausgewählten Verarbeitungsmodus.

   Ist dieses Kontrollkästchen deaktiviert, wenn die Aufgabe "Schutz vor Netzwerkbedrohungen" angehalten wird, untersucht Kaspersky Security für Windows Server den eingehenden Netzwerkverkehr nicht auf Aktivitäten, die typisch für Netzwerkangriffe sind, und blockiert keine Netzwerkaktivitäten, die vom angreifenden Computer ausgehen.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

9. Klicken Sie auf **OK**.

Ausnahmen hinzufügen

Gehen Sie wie folgt vor, um Ausnahmen der Aufgabe "Schutz vor Netzwerkbedrohungen" hinzuzufügen:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Schutz vor Netzwerkbedrohungen** auf **Einstellungen**.
6. Aktivieren Sie auf der Registerkarte **Ausnahmen** das Kontrollkästchen **Ausgenommene IP-Adressen nicht kontrollieren**.

   Ist dieses Kontrollkästchen aktiviert, untersucht Kaspersky Embedded Systems Security den eingehenden Netzwerkverkehr nicht auf ausgenommene IP-Adressen.

   Ist dieses Kontrollkästchen deaktiviert, wendet Kaspersky Embedded Systems Security die Ausnahmeliste nicht an.
7. Geben Sie die IP-Adresse an, und klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **OK**.

Kontrolle des Programmstarts

Dieser Abschnitt informiert über die Aufgabe zur Kontrolle des Programmstarts und erläutert die Konfiguration dieser Aufgabe.

Über die Aufgabe zur Kontrolle des Programmstarts

Wenn die Aufgabe zur Kontrolle des Programmstarts ausgeführt wird, überwacht Kaspersky Embedded Systems Security die versuchten Programmstarts des Benutzers und erlaubt oder verbietet den Start dieser Programme. Die Aufgabe zur Kontrolle des Programmstarts baut auf dem "Prinzip des standardmäßigen Verbots" (Default Deny) auf, was bedeutet, dass alle Programme, die in den Aufgabeneinstellungen nicht erlaubt sind, automatisch blockiert werden.

Sie können den Programmstart auf eine der folgenden Weisen erlauben:

- Anhand von Erlaubnisregeln für vertrauenswürdige Programme
- Prüfung der Reputation vertrauenswürdiger Programme in KSN beim Start

Die Aufgabe verleiht dem Startverbot von Programmen oberste Priorität. Wenn ein Programm beispielsweise durch eine der Verbotsregeln am Start gehindert wird, wird der Programmstart unabhängig von der Einstufung von KSN als "vertrauenswürdig" verboten. Wenn ein Programm also von den KSN-Diensten als nicht vertrauenswürdig eingestuft wird, aber in den Gültigkeitsbereich einer Erlaubnisregel fällt, wird der Programmstart verboten.

Alle Versuche, Programme zu starten, werden im Protokoll der Aufgabenausführung festgehalten.

Aufgabe zur Kontrolle des Programmstarts kann in einem von zwei Modi betrieben werden:

- **Aktiv**. Die Kontrolle durch Kaspersky Embedded Systems Security erfolgt mithilfe eines Regelsatzes zur Kontrolle des Starts von Programmen, die unter den Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts fallen. Der Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts ist in den Einstellungen der Aufgabe angegeben. Fällt ein Programm unter den Gültigkeitsbereich der Regeln zur Kontrolle des Programmstarts und entsprechen die Aufgabeneinstellungen keiner der angegebenen Regeln, ist der Programmstart verboten.

  Starts von Programmen, die sich außerhalb des Gültigkeitsbereichs der Regeln befinden, wie er in den Eigenschaften der Aufgabe zur Kontrolle des Programmstarts festgelegt ist, werden unabhängig von den Einstellungen der Regeln für die Kontrolle des Programmstarts verweigert.

  Die Aufgabe zur **Kontrolle des Programmstarts** kann nicht im aktiven Modus gestartet werden, wenn keine Regeln erstellt wurden oder wenn es mehr als 65.535 Regeln für ein geschütztes Gerät gibt.

- **Nur Statistik**. Kaspersky Embedded Systems Security verwendet keine Regel für die Kontrolle des Programmstarts, um den Start von Programmen zu erlauben oder zu verbieten. Stattdessen werden nur Informationen über Programmstarts, Regeln, die von laufenden Programmen erfüllt werden, und Aktionen, die ausgeführt worden wären, wenn die Aufgabe im Modus **Aktiv** ausgeführt würde, aufgezeichnet. Allen Programmen wird der Start erlaubt. Dieser Modus ist standardmäßig eingestellt.

  Sie können diesen Modus anwenden, um auf der Grundlage der im Protokoll der Aufgabenausführung aufgezeichneten Informationen die Regeln zur Kontrolle des Programmstarts zu erstellen.

Sie können die Aufgabe zur Kontrolle des Programmstarts nach einem der folgenden Szenarien gestalten:

- Erweiterte Konfiguration von Regeln und Verwendung für die Kontrolle des Programmstarts.
- Minimale Konfiguration der Regeln und die Verwendung von KSN für die Kontrolle des Programmstarts.

Wenn Dateien des Betriebssystems in den Gültigkeitsbereich der Aufgabe zur Kontrolle des Programmstarts fallen, wird empfohlen, beim Erstellen von Regeln für die Kontrolle des Programmstarts sicherzustellen, dass solche Programme von den neu erstellten Regeln erlaubt werden. Andernfalls kann das Betriebssystem möglicherweise nicht mehr starten.

Kaspersky Embedded Systems Security fängt außerdem Prozesse ab, die unter dem Windows Subsystem for Linux gestartet werden (außer Skripten, die von der UNIX™-Shell oder aus dem Kommandozeileninterpreter gestartet werden). Bei solchen Prozessen wendet die Aufgabe zur Kontrolle des Programmstarts die von der aktuellen Konfiguration festgelegte Aktion an. Die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" erkennt den Start von Programmen und erstellt entsprechende Regeln für Programme, die unter Windows Subsystem for Linux laufen.

Über die Regeln für die Kontrolle des Programmstarts

So funktionieren Regeln für die Kontrolle des Programmstarts

Die Funktion der Regeln für die Kontrolle des Programmstarts basiert auf folgenden Elementen:

- Regeltyp.

  Regeln für die Kontrolle des Programmstarts können den Start eines Programms erlauben oder verbieten. Demgemäß werden sie als *Erlaubnisregeln* oder *Verbotsregeln* bezeichnet. Zum Erstellen einer Liste von Erlaubnisregeln für die Kontrolle des Programmstarts können Sie die Aufgabe zur Erstellung von Erlaubnisregeln oder den Modus **Nur Statistik** in der Aufgabe zur Kontrolle des Programmstarts verwenden. Sie können ferner Erlaubnisregeln manuell hinzufügen.

- Benutzer und / oder Benutzergruppe.

  Regeln für die Kontrolle des Programmstarts können den Start von festgelegten Programmen durch einen Benutzer und/oder eine Benutzergruppe kontrollieren.

- Gültigkeitsbereich der Regel.

  Regeln für die Kontrolle des Programmstarts können auf *ausführbare Dateien*, *Skripts* und *MSI-Pakete* angewendet werden.

- Auslösekriterium für die Regel.

  Die Regeln für die Kontrolle des Programmstarts kontrollieren den Start derjenigen Dateien, die eines der in den Regeleinstellungen festgelegten Kriterien erfüllen: Sie sind mit dem angegebenen *digitalen Zertifikat* signiert, weisen den angegebenen *SHA256-Hash* auf oder sind unter dem angegebenen *Pfad* gespeichert.

  Ist die Einstellung **Digitales Zertifikat** als Auslösekriterium für die Regel festgelegt, kontrolliert die erstellte Regel den Start aller vertrauenswürdigen Programme im Betriebssystem. Sie können strengere Bedingungen für dieses Kriterium festlegen, indem Sie die folgenden Kontrollkästchen aktivieren:

  - **Header verwenden**
  - **Fingerabdruck verwenden**

Fingerabdrücke ermöglichen die strengste Einschränkung für das Auslösen der Regeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles Identifikationsmerkmal eines digitalen Zertifikats handelt, welches im Gegensatz zum Header eines digitalen Zertifikats fälschungssicher ist.

Sie können Ausnahmen von der Regel für die Kontrolle des Programmstarts festlegen. Ausnahmen von der Regel für die Kontrolle des Programmstarts basieren auf denselben Kriterien, die für das Auslösen der Regel gelten: digitales Zertifikat, SHA256-Hash und Dateipfad. Ausnahmen von den Regeln für die Kontrolle des Programmstarts können für bestimmten Erlaubnisregeln erforderlich werden: z. B., wenn Sie Benutzern den Start von Programmen aus dem Pfad C:\Windows erlauben möchten, den Start der Datei Regedit.exe jedoch verbieten wollen.

Wenn Dateien des Betriebssystems in den Gültigkeitsbereich der Aufgabe zur Kontrolle des Programmstarts fallen, wird empfohlen, beim Erstellen von Regeln für die Kontrolle des Programmstarts sicherzustellen, dass solche Programme von den neu erstellten Regeln erlaubt werden. Andernfalls kann das Betriebssystem möglicherweise nicht mehr starten.

Verwaltung der Regeln für die Kontrolle des Programmstarts

Für die Regel für die Kontrolle des Programmstarts stehen Ihnen die folgenden Aktionen zur Verfügung:

- Regeln manuell hinzufügen
- Regeln automatisch erstellen und hinzufügen
- Regeln löschen
- Regeln in eine Konfigurationsdatei exportieren
- Ausgewählte Dateien auf das Vorhandensein von Regeln prüfen, die den Start dieser Dateien erlauben
- Die Liste der Regeln nach einem festgelegten Kriterium filtern

Über die Kontrolle für Installationspakete

Das Erzeugen von Regeln für die Kontrolle des Programmstarts kann kompliziert sein, wenn Sie auch Installationspakete auf einem geschützten Gerät überwachen müssen, beispielsweise auf geschützten Geräten, auf denen installierte Software regelmäßig automatisch aktualisiert wird. In diesem Fall muss die Liste der Erlaubnisregeln nach jedem Software-Update aktualisiert werden, damit neu erstellte Dateien in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts berücksichtigt werden. Um die Startkontrolle bei Installationspakete-Szenarien zu vereinfachen, können Sie das Untersystem "Kontrolle für Installationspakete" verwenden.

Ein *Installationspaket* (im Weiteren "Paket") stellt eine Software-Anwendung dar, die auf einem geschützten Gerät installiert werden soll. Jedes Paket enthält mindestens eine Anwendung und kann darüber hinaus einzelne Dateien, Updates oder auch einen bestimmten Befehl enthalten, vor allem, wenn Sie eine Software-Anwendung oder ein Update installieren.

Das Untersystem "Kontrolle für Installationspakete" wird als zusätzliche Liste von Ausnahmen implementiert. Wenn Sie ein Installationspaket zu dieser Liste hinzufügen, erlaubt das Programm, dass diese vertrauenswürdigen Pakete dekomprimiert werden und erlaubt, dass Software, die von einem vertrauenswürdigen Paket installiert oder verändert wurde, automatisch gestartet wird. Die extrahierten Dateien können das Merkmal für die Vertrauenswürdigkeit von einem Hauptprogrammpaket erben. Ein *Hauptprogrammpaket* ist ein Paket, das vom Benutzer zur Liste der Ausnahmen von der Kontrolle der Installationspakete hinzugefügt wurde und nun als vertrauenswürdiges Paket gilt.

Kaspersky Embedded Systems Security kontrolliert nur vollständige Zyklen von Installationspaketen. Das Programm kann den Start von Dateien, die von einem vertrauenswürdigen Paket modifiziert wurden, nicht korrekt verarbeiten, wenn das Paket das erste Mal ausgeführt wird, wenn die Kontrolle für Installationspakete deaktiviert ist oder wenn die Komponente "Kontrolle des Programmstarts" nicht installiert ist.

Die Kontrolle für Installationspakete ist nicht verfügbar, wenn das Kontrollkästchen **Regeln für ausführbare Dateien verwenden** in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts deaktiviert ist.

Cache für Softwareverteilung

Kaspersky Embedded Systems Security verwendet einen dynamisch erzeugten Cache für Softwareverteilung (Installations-Cache), um die Beziehung zwischen vertrauenswürdigen Paketen und Dateien herzustellen, die während der Softwareverteilung erstellt wurden. Wenn ein Paket erstmals gestartet wird, erkennt Kaspersky Embedded Systems Security alle Dateien, die von dem Paket während des Softwareverteilungsprozesses erstellt werden, und speichert die Prüfsummen und Pfade der Dateien im Installations-Cache. Anschließend dürfen alle Dateien im Installations-Cache standardmäßig gestartet werden.

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

Sie können den Installations-Cache in eine Konfigurationsdatei exportieren (xml-Format) und den Cache außerdem mithilfe von Befehlszeilenoptionen löschen.

Um den Installations-Cache in eine Konfigurationsdatei zu exportieren, führen Sie den folgenden Befehl aus:

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

Um den Installations-Cache zu löschen, führen Sie den folgenden Befehl aus:

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

Kaspersky Embedded Systems Security aktualisiert den Installations-Cache alle 24 Stunden. Wenn die Prüfsumme einer zuvor erlaubten Datei geändert wird, löscht das Programm den Datensatz für diese Datei aus dem Installations-Cache. Wenn die Aufgabe zur Kontrolle des Programmstarts im aktiven Modus gestartet wurde, werden weitere Ausführungsversuche dieser Datei unterbunden. Wenn der vollständige Pfad einer zuvor erlaubten Datei geändert wird, werden weitere Ausführungsversuche dieser Datei unterbunden, da die Prüfsumme im Installations-Cache gespeichert ist.

Verarbeiten der extrahierten Dateien

Alle aus einem vertrauenswürdigen Paket extrahierten Dateien erben beim ersten Start des Pakets das Merkmal für die Vertrauenswürdigkeit. Wenn Sie das Kontrollkästchen nach dem ersten Start deaktivieren, behalten alle aus dem Paket extrahierten Dateien das geerbte Attribut. Um das geerbte Attribut für alle extrahierten Dateien zurückzusetzen, müssen Sie den Installations-Cache löschen und das Kontrollkästchen **Weitere Verteilung von aus diesem Installationspaket erstellten Programmen erlauben** deaktivieren, bevor Sie das vertrauenswürdige Installationspaket erneut starten.

Extrahierte Dateien und Pakete, die von einem vertrauenswürdigen Hauptprogrammpaket erstellt wurden, erben das Merkmal für die Vertrauenswürdigkeit, indem ihre Prüfsummen beim ersten Start des Installationspakets in der Liste mit Ausnahmen zum Installations-Cache hinzugefügt werden. Als Folge gelten sowohl das Installationspaket selbst als auch alle extrahierten Dateien des Pakets als vertrauenswürdig. Standardmäßig ist die Anzahl der Ebenen von Vererbung des Merkmals für die Vertrauenswürdigkeit unbegrenzt.

Extrahierte Dateien behalten das Merkmal für die Vertrauenswürdigkeit nachdem das Betriebssystem neu gestartet wurde.

Die Verarbeitung von Dateien wird in den Einstellungen der Kontrolle für Installationspakete angepasst. Aktivieren oder deaktivieren Sie dazu das Kontrollkästchen **Weitere Verteilung von aus diesem Installationspaket erstellten Programmen erlauben**.

Angenommen, Sie fügen beispielsweise das Paket test.msi, das einige andere Pakete und Programme enthält, zur Ausnahmeliste hinzu und aktivieren das Kontrollkästchen. In diesem Fall wird allen Paketen und Programmen im Paket test.msi erlaubt, zu starten oder ihren Inhalt zu extrahieren, wenn sie andere Dateien enthalten. Dieses Szenario gilt für extrahierte Dateien auf allen Verschachtelungsebenen.

Wenn Sie das Paket test.msi zur Ausnahmeliste hinzufügen und das Kontrollkästchen **Weitere Verteilung von aus diesem Installationspaket erstellten Programmen erlauben** deaktivieren, weist das Programm das Merkmal für die Vertrauenswürdigkeit nur solchen Paketen und ausführbaren Dateien zu, die direkt aus dem primären vertrauenswürdigen Paket extrahiert werden (auf der ersten Verschachtelungsebene). Die Prüfsummen dieser Dateien werden im Installations-Cache gespeichert. Alle Dateien, die sich auf der zweiten Verschachtelungsebene und tiefer befinden, werden nach dem Prinzip des standardmäßigen Verbots (Default Deny) blockiert.

Arbeiten mit der Regelliste für die Kontrolle des Programmstarts

Die Liste vertrauenswürdiger Pakete des Untersystems "Kontrolle für Installationspakete" ist eine Liste bestehend aus Ausnahmen. Diese Liste erweitert die allgemeine Liste mit Regeln für die Kontrolle des Programmstarts, ersetzt sie jedoch nicht.

Verbotsregeln der Kontrolle des Programmstarts haben die höchste Priorität: Das Dekomprimieren vertrauenswürdiger Pakete und das Ausführen neuer oder modifizierter Dateien wird blockiert, wenn diese Pakete und Dateien von den Verbotsregeln zur Kontrolle des Programmstarts betroffen sind.

Ausnahmen für die Kontrolle für Installationspakete werden sowohl auf vertrauenswürdige Pakete als auch auf Dateien angewendet, die von diesen Paketen erstellt oder modifiziert wurden, wenn keine Verbotsregeln in der Liste der Kontrolle des Programmstarts auf diese Pakete und Dateien angewendet werden.

Verwendung der KSN-Einstufungen

KSN-Einstufungen, dass eine Datei nicht vertrauenswürdig ist, haben eine höhere Priorität als die Ausnahmen der Kontrolle für Installationspakete: Dekomprimierung von vertrauenswürdigen Paketen und Start von Dateien, die von diesen Paketen erstellt oder geändert werden, werden blockiert, wenn KSN meldet, dass diese Dateien nicht vertrauenswürdig sind.

Danach und nach dem Entpacken eines vertrauenswürdigen Pakets dürfen alle untergeordneten Dateien ausgeführt werden, unabhängig von der Verwendung von KSN innerhalb des Bereichs "Kontrolle des Programmstarts". Die Status der Kontrollkästchen **Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten** und **Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben** haben daher keine Auswirkung auf das Kontrollkästchen **Weitere Verteilung von aus diesem Installationspaket erstellten Programmen erlauben**.

Über die Verwendung von KSN mit der Aufgabe Kontrolle des Programmstarts

Die Aufgabe Verwendung von KSN kann nur gestartet werden, wenn die KSN-Erklärung akzeptiert wurde.

Wenn KSN-Daten über die Reputation von der Aufgabe zur Kontrolle des Programmstarts verwendet werden, wird die Programmreputation von KSN als Kriterium für das Erlauben oder Blockieren des Starts dieses Programms betrachtet. Wenn KSN an Kaspersky Embedded Systems Security meldet, dass ein Programm nicht vertrauenswürdig ist, wenn der Benutzer versucht, das Programm zu starten, wird der Start des Programms verboten. Wenn KSN an Kaspersky Embedded Systems Security meldet, dass das Programm vertrauenswürdig ist, wenn der Benutzer versucht, das Programm zu starten, wird der Start des Programms erlaubt. Sie können KSN zusammen mit Regeln für die Kontrolle des Programmstarts oder als unabhängiges Kriterium für das Verbot des Starts von Programmen verwenden.

Einstufungen von KSN als unabhängiges Kriterium für die Blockierung des Programmstarts übernehmen

Dieses Szenario ermöglicht es, den Programmstart auf einem geschützten Gerät auf sichere Weise zu kontrollieren, ohne erweiterte Einstellungen der Regelliste zu erfordern.

Sie können die KSN-Einstufungen für Kaspersky Embedded Systems Security gemeinsam mit der einzigen angegebenen Regel übernehmen. Das Programm erlaubt nur den Start von Programmen, die von KSN als vertrauenswürdig eingestuft wurden oder durch eine angegebene Regel erlaubt werden.

> Für ein solches Szenario wird empfohlen, eine Erlaubnisregel für den Programmstart anhand des digitalen Zertifikats festzulegen.

Alle übrigen Programme werden nach dem Prinzip des standardmäßigen Verbots (Default Deny) verboten. Wenn keine Regeln festgelegt wurden, hilft die Verwendung von KSN dabei, das Gerät vor Programmen zu schützen, die laut KSN eine Gefahr darstellen.

Einstufungen von KSN zusammen mit Regeln für die Kontrolle des Programmstarts übernehmen

Für die Verwendung von KSN zusammen mit Regeln für die Kontrolle des Programmstarts gelten die folgenden Bedingungen:

- Kaspersky Embedded Systems Security verbietet immer den Start eines Programms aus dem Gültigkeitsbereich von zumindest einer Verbotsregel. Wenn das Programm von den KSN-Diensten als vertrauenswürdig eingestuft wurde, wird der entsprechenden Einstufung eine niedrigere Priorität zugewiesen, und der Programmstart wird dennoch verboten. Dadurch können Sie die Liste blockierter Programme manuell erweitern.

- Kaspersky Embedded Systems Security verbietet den Start eines Programms immer, wenn der Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verboten ist und das Programm in KSN als nicht

vertrauenswürdig eingestuft wurde. Wenn für das Programm eine Erlaubnisregel festgelegt wurde, wird dieser Regel eine niedrigere Priorität zugewiesen, und der Programmstart wird dennoch verboten. Auf diese Weise kann das Gerät vor Programmen geschützt werden, die laut KSN eine Gefahr darstellen, aber bei der Erstkonfiguration der Regeln nicht berücksichtigt wurden.

Über das Erstellen von Regeln für die Kontrolle des Programmstarts

Sie können mithilfe der Aufgaben und Richtlinien von Kaspersky Security Center für alle Geräte und Gruppen von geschützten Geräten im Netzwerk des Unternehmens gleichzeitig Listen mit Regeln für die Kontrolle des Programmstarts erstellen. Die unten angeführten Szenarien werden empfohlen, wenn sich im Unternehmensnetzwerk keine Referenzcomputer befinden und Sie keine Möglichkeit haben, eine Liste von Erlaubnisregeln anhand der auf einem solchen Vorlagencomputer installierten Programme zu erstellen.

Sie können die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" lokal über die Programmkonsole ausführen, um eine Liste von Regeln zu erstellen, die auf den Anwendungen basieren, die auf einem einzelnen geschützten Gerät ausgeführt werden.

Die Komponente zur Kontrolle des Programmstarts wird mit zwei voreingestellten Erlaubnisregeln installiert:

- Erlaubnisregel für Skripts und Windows Installer-Paketen mit einem Zertifikat, das vom Betriebssystem als vertrauenswürdig betrachtet wird.
- Erlaubnisregel für ausführbare Dateien mit einem Zertifikat, das vom Betriebssystem als vertrauenswürdig betrachtet wird.

Sie können Listen mit Regeln für die Kontrolle des Programmstarts in der Konsole von Kaspersky Security Center auf eine der folgenden Arten erstellen:

- Mithilfe einer Gruppenaufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts".

  In diesem Szenario erstellt die Gruppenaufgabe für jedes geschützte Gerät im Netzwerk eine eigene Liste der Regeln für die Kontrolle des Programmstarts und speichert diese Listen im angegebenen freigegebenen Ordner in Form einer XML-Datei. Die XML-Datei, die von der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" erzeugt wurde, enthält die Erlaubnisregel, die in Aufgabeneinstellungen angegeben sind, bevor die Aufgabe gestartet wird. Es werden keine Regeln für Programme erstellt, die in den angegebenen Aufgabeneinstellungen nicht gestartet werden dürfen. Der Start solcher Programme ist standardmäßig verboten. Danach können Sie die erstellten Listen mit Regeln manuell in die Aufgabe Kontrolle des Programmstarts für die Richtlinie von Kaspersky Security Center importieren.

  Sie können die erstellten Regeln so konfigurieren, dass sie automatisch in die Liste der Regeln für die Aufgabe zur Kontrolle des Programmstarts importiert werden.

  Es wird empfohlen, diese Option zu verwenden, wenn die rasche Erstellung von Listen mit Regeln für die Kontrolle des Programmstarts erforderlich ist. Es wird empfohlen, den geplanten Start der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" nur dann einzurichten, wenn die übernommenen Erlaubnisregeln Ordner und Dateien enthalten, von denen Sie wissen, dass sie sicher sind.

  Stellen Sie vor der Verwendung der Aufgabe Kontrolle des Programmstarts im Netzwerk sicher, dass alle geschützten Geräte Zugriff auf einen freigegebenen Ordner haben. Falls die Verwendung eines freigegebenen Ordners im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" auf einem geschützten Gerät in der Testgruppe der geschützten Geräte oder auf einem Referenzcomputer zu starten.

- Auf Grundlage eines Berichts über Aufgabenereignisse, der in Kaspersky Security Center anhand der Ausführung der Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** erstellt wird.

  In diesem Szenario verbietet Kaspersky Embedded Systems Security den Start von Programmen nicht. Stattdessen werden bei Ausführung der Kontrolle des Programmstarts im Modus **Nur Statistik** alle erlaubten und verbotenen Programmstarts für alle geschützten Geräte im Netzwerk im Abschnitt **Ereignisse** im Arbeitsbereich des Knotens Administrationsserver von Kaspersky Security Center gemeldet. Kaspersky Security Center verwendet die Berichte, um eine einzelne Liste von Ereignissen zu erstellen, bei denen Programmstarts verboten wurden.

  Sie müssen den Zeitraum für die Ausführung der Aufgabe so konfigurieren, dass alle möglichen Szenarien, in denen die geschützten Geräte und Gruppen von geschützten Geräten beteiligt sind und mindestens ein Server-Neustart während der angegebenen Zeitspanne ausgeführt werden. Nachdem Ende des Aufgabenausführungszeitraums können Sie Daten über Programmstarts aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (TXT-Format) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle des Programmstarts für solche Programme erstellen.

  Dieses Szenario wird empfohlen, wenn das Netzwerk des Unternehmens eine große Anzahl an geschützten Geräten verschiedener Typen (mit unterschiedlicher Software) enthält.

- Auf Grundlage der Ereignisse über den verbotenen Start von Programmen, die über Kaspersky Security Center erhalten wurden, ohne Erstellen und Importieren der Konfigurationsdatei.

  Um die vorliegende Möglichkeit zu nutzen, muss sich die Aufgabe zur Kontrolle des Programmstarts auf dem geschützten Gerät unter der Verwaltung der aktiven Richtlinie für Kaspersky Security Center befinden. Alle Ereignisse auf dem geschützten Gerät werden dabei an den Administrationsserver übergeben.

Es wird empfohlen, die Regelliste bei Änderungen an der Zusammensetzung der auf den geschützten Geräten des Netzwerks installierten Programme zu aktualisieren (beispielsweise bei der Installation von Updates oder nach einer Neuinstallation des Betriebssystems). Es wird empfohlen, eine aktualisierte Liste von Regeln zu erstellen, in dem Sie auf geschützten Geräten in der Test-Administrationsgruppe die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" oder die Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** ausführen. Die Test-Administrationsgruppe beinhaltet die geschützten Geräte, die für den Test des Starts von neuen Programmen vor deren Installation auf den geschützten Geräten des Netzwerks erforderlich sind.

XML-Dateien mit Listen von Erlaubnisregeln werden auf Grundlage einer Analyse der gestarteten Aufgaben auf dem geschützten Gerät erstellt. Es wird empfohlen, die Aufgaben "Erstellen von Regeln für die Kontrolle des Programmstarts" und "Kontrolle des Programmstarts" im Modus **Nur Statistik** für die Erstellung von Regellisten auf einem Referenzcomputer zu starten, damit alle im Netzwerk verwendeten Programme berücksichtigt werden.

Überzeugen Sie sich vor dem Erstellen der Liste der Erlaubnisregeln nach Programmen, die auf dem Referenzcomputer des Unternehmens gestartet werden, dass der Vorlagencomputer sicher ist und es darauf keine Schadsoftware gibt.

Bevor Sie Erlaubnisregeln hinzufügen, wählen Sie einen der verfügbaren Modi zur Anwendung der Regeln aus. In der Regelliste der Richtlinie für Kaspersky Security Center werden nur Regeln angezeigt, die in dieser Richtlinie festgelegt sind, unabhängig vom Modus der Regelanwendung. Die Regelliste des lokalen Computers enthält alle angewendeten Regeln – sowohl lokale als auch durch eine Richtlinie hinzugefügte.

Standardeinstellungen der Aufgabe "Kontrolle des Programmstarts"

Die Aufgabe Kontrolle des Programmstarts weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Standardeinstellungen der Aufgabe "Kontrolle des Programmstarts"

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	**Nur Statistik**. Die Datensätze der Aufgabe haben auf der Grundlage der festgelegten Regeln Startereignisse verboten und Startereignisse erlaubt. Der Programmstart wird nicht explizit verboten.	Sie können den Modus **Aktiv** auswählen, nachdem die endgültige Liste der Regeln erstellt wurde.
Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten	Wird nicht verwendet	Sie können bei weiteren Starts dieser Datei Aktionen wiederholen, die Sie beim ersten Start der Datei angewendet haben.
Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten	Wird nicht verwendet.	Sie können den Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten.
Regelverwaltung	**Richtlinienregeln zu lokalen Regeln hinzufügen**	Sie können den Modus der gemeinsamen Anwendung der in der Richtlinie festgelegten Regeln und der Regeln auf dem geschützten Gerät auswählen.
Gültigkeitsbereich der Regel	Die Aufgabe überwacht den Start von ausführbaren Dateien, Skripten und MSI-Paketen. Zudem überwacht die Aufgabe das Laden von DLL-Modulen.	Sie können die Dateitypen angeben, deren Start durch die Regeln kontrolliert werden soll.
Verwendung von KSN	Daten der KSN-Programmreputation werden nicht verwendet.	Sie können die Daten über die Reputation von Programmen in KSN bei der Ausführung der Aufgabe zur Kontrolle des Programmstarts verwenden.
Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben	Wird nicht verwendet.	Sie können die Softwareverteilung mithilfe der in den Einstellungen angegebenen Installationspakete und Programme erlauben. Standardmäßig ist die Verteilung der Programme nur mithilfe des Dienstes Windows Installer erlaubt.
Verteilung von Programmen mithilfe von Windows Installer immer erlauben	Übernommen (kann nur geändert werden, wenn die Einstellung **Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben** aktiviert ist).	Sie können die Installation oder das Update einer beliebigen Software erlauben, wenn der entsprechende Vorgang über Windows Installer ausgeführt wird.
Verteilung von Programmen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben	Übernommen (kann nur geändert werden, wenn die Einstellung **Verteilung von Software mittels aufgelisteter Programme und**	Sie können die automatische Verteilung von Installationspaketen mithilfe der Softwarelösung System Center Configuration Manager aktivieren bzw. deaktivieren.

	Installationspakete automatisch erlauben aktiviert ist).	
Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Kontrolle des Programmstarts wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Standardeinstellungen der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts"

Einstellung	Standardwert	Beschreibung
Präfix für Namen von Erlaubnisregeln	Entspricht dem Namen des geschützten Geräts, auf dem Kaspersky Embedded Systems Security installiert ist.	Sie können das Präfix für die Namen von Erlaubnisregeln ändern.
Gültigkeitsbereich der Erlaubnisregeln	Unter den Gültigkeitsbereich der Erlaubnisregeln fallen standardmäßig die folgenden Kategorien von Dateien: • Dateien mit der Erweiterung EXE, die sich in den Ordnern C:\Windows, C:\Program Files (x86) und C:\Program Files befinden • MSI-Pakete im Ordner C:\Windows • Skripte im Ordner C:\Windows Außerdem erstellt die Aufgabe Regeln für alle bereits gestarteten Programme, unabhängig von deren Speicherort und Format.	Sie können den Schutzbereich ändern, indem Sie Ordnerpfade hinzufügen oder entfernen und Typen von Dateien festlegen, deren Start durch die automatisch generierten Regeln erlaubt wird. Sie können bei der Erstellung von Erlaubnisregeln auch bereits gestartete Programme ignorieren.
Kriterien für die Erstellung von Erlaubnisregeln.	Der Header des digitalen Zertifikats und der Fingerabdrucks werden verwendet, Regeln werden für alle Benutzer und Benutzergruppen erstellt.	Sie können den SHA256-Hash bei der Erstellung von Erlaubnisregeln verwenden. Sie können einen Benutzer und eine Benutzergruppe auswählen, für die automatisch Erlaubnisregeln erstellt werden sollen.
Aktionen nach Abschluss der Aufgabe	Die Erlaubnisregeln werden der Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt; neue Regeln werden mit bestehenden Regeln zusammengeführt; doppelte Regeln werden gelöscht.	Sie können die Regeln zu den bereits existierenden Regeln hinzufügen, ohne sie zusammenzuführen und ohne doppelte Regeln zu löschen, oder bestehende Regeln durch die neuen Erlaubnisregeln ersetzen, sowie den Export der Erlaubnisregeln in eine Datei konfigurieren.
Einstellungen für den Aufgabenstart mit Rechten	Die Aufgabe wird mit den Rechten des Systemkontos gestartet.	Sie können den Start der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" unter einem Systemkontos erlauben oder die Rechte eines angegebenen Benutzers verwenden.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts wird beim Start von

		Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Kontrolle des Programmstarts über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Aufgabeneinstellungen für einen oder alle geschützten Geräte im Netzwerk konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Richtlinieneinstellungen für die Aufgabe zur Kontrolle des Programmstarts öffnen

Um die Aufgabeneinstellungen für die Kontrolle des Programmstarts über die Richtlinie von Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Überwachung der Desktop-Aktivitäten**.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Kontrolle des Programmstarts**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.

Konfigurieren Sie die Richtlinie nach Bedarf.

Regelliste für die Kontrolle des Programmstarts öffnen

Um die Regelliste für die Kontrolle des Programmstarts über das Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

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

2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Überwachung der Desktop-Aktivitäten**.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Kontrolle des Programmstarts**.

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.
7. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.

Konfigurieren Sie die Regelliste nach Bedarf.

Assistent und Eigenschaften für die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen

Um mit dem Erstellen einer Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu beginnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.
5. Wählen Sie den untergeordneten Knoten **Erstellen von Regeln für die Kontrolle des Programmstarts**.
6. Klicken Sie auf **Weiter**.

   Das Fenster **Einstellungen** wird geöffnet.

Um der bestehenden Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben von Kaspersky Security Center.

   Das Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.

Informationen darüber, wie Sie die Aufgabe konfigurieren, finden Sie im Abschnitt Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren.

Aufgabe Kontrolle des Programmstarts konfigurieren

Um die allgemeinen Aufgabeneinstellungen für die Kontrolle des Programmstarts zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Kontrolle des Programmstarts**.
2. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Aufgabenmodus** folgende Einstellungen:
   - Geben Sie in der Dropdown-Liste **Aufgabenmodus** den Aufgabenmodus an.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten**.
3. Passen Sie im Abschnitt **Regelverwaltung** 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 erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie den Backslash ("\"), um den Pfad korrekt einzutragen.

   b. Wählen Sie den Modus für die Anwendung der Regeln aus:
      - **Lokale Regeln durch Richtlinienregeln ersetzen**.

        Das Programm wendet die in der Richtlinie festgelegte Regelliste für die zentralisierte Kontrolle des Programmstarts auf der Gruppe von geschützten Geräten 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 "Erstellen von Regeln für die Kontrolle des Programmstarts" bearbeiten.
4. Nehmen Sie im Abschnitt **Gültigkeitsbereich der Regel** die folgenden Einstellungen vor:
   - **Regeln für ausführbare Dateien verwenden**.
   - **Laden von DLL-Modulen überwachen**.

     Das Überwachen des Ladens von DLL-Modulen kann sich auf die Leistung des Betriebssystems auswirken.
   - **Regeln für Skripte und MSI-Pakete verwenden**.

5. Passen Sie in der Gruppe **Verwendung von KSN** die folgenden Einstellungen des Programmstarts an:

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

6. Passen Sie auf der Registerkarte **Überwachung von Installationspaketen** die Einstellungen für die Kontrolle für Installationspakete an.

7. Passen Sie auf der Registerkarte **Aufgabenverwaltung** die geplanten Einstellungen für den Aufgabenstart an.

8. Klicken Sie im Fenster **Kontrolle des Programmstarts** auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Konfiguration der Kontrolle für Installationspakete

Um ein vertrauenswürdiges Installationspaket hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Kontrolle des Programmstarts**.

2. Aktivieren Sie auf der Registerkarte **Überwachung von Installationspaketen** das Kontrollkästchen Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben.

   Sie können das Kontrollkästchen **Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben** aktivieren, wenn das Kontrollkästchen **Regeln für ausführbare Dateien verwenden** auf der Registerkarte **Allgemein** in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts aktiviert ist.

3. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Verteilung von Programmen mithilfe von Windows Installer immer erlauben**.

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

4. Aktivieren Sie bei Bedarf das Kontrollkästchen **Verteilung von Programmen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben**.

   Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an das geschützte Gerät bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation des Systems auf dem geschützten Gerät ausgeführt wurde.

5. Um die Liste der vertrauenswürdigen Installationspakete zu bearbeiten, klicken Sie auf die Schaltfläche **Liste der Pakete bearbeiten** und wählen Sie im nächsten Fenster eine der verfügbaren Methoden aus:

   - **Ein Installationspaket hinzufügen**.

     a. Klicken Sie auf die Schaltfläche **Durchsuchen**.

     b. Wählen Sie die ausführbare Datei oder das Installationspaket aus.

     Im Abschnitt **Kriterien für Vertrauenswürdigkeit** werden die Daten zur ausgewählten Datei automatisch angezeigt.

     c. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Weitere Verteilung von aus diesem Installationspaket erstellten Programmen erlauben**.

     d. Wählen Sie eine der beiden verfügbaren Varianten der Kriterien für die Vertrauenswürdigkeit aus, auf deren Grundlage die Datei oder das Installationspaket als vertrauenswürdig gelten:

     - **Digitales Zertifikat verwenden**
     - **SHA256-Hash verwenden**

   - **Mehrere Pakete anhand von Hash hinzufügen**.

     Sie können eine unbegrenzte Anzahl an ausführbaren Dateien und Installationspaketen auswählen und gleichzeitig zur Liste hinzufügen. Kaspersky Embedded Systems Security untersucht den Hash und erlaubt dem Betriebssystem den Start der angegebenen Dateien.

   - **Ausgewähltes Paket bearbeiten**.

     Verwenden Sie diese Variante, um eine andere ausführbare Datei oder ein anderes Installationspaket auszuwählen sowie die Kriterien für die Vertrauenswürdigkeit zu ändern.

   - Liste mit Paketen aus Datei importieren.

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

6. Wenn Sie ein früher hinzugefügtes Programm oder Installationspaket aus der Liste der vertrauenswürdigen Installationspakete löschen möchten, klicken Sie auf die Schaltfläche **Installationspakete löschen**. Der Start extrahierter Dateien wird erlaubt.

   Um den Start extrahierter Dateien zu verbieten, deinstallieren Sie das Programm vollständig vom geschützten Gerät oder erstellen Sie eine Verbotsregel in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts.

7. Klicken Sie auf OK.

Ihre neu konfigurierten Einstellungen werden gespeichert.

Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren

Um die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts**.

2. Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.

   Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

3. Im Abschnitt **Einstellungen** können Sie die folgenden Einstellungen konfigurieren:

   - Fügen Sie ein Präfix für Regelnamen hinzu.
   - Geben Sie an, wie Erlaubnisregeln erstellt werden:
     - **Erlaubnisregeln auf Grundlage gestarteter Programme erstellen**
     - **Erlaubnisregeln für Programme aus folgenden Ordnern erstellen**

4. Im Abschnitt **Einstellungen** können Sie Aktionen festlegen, die bei der Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen:

   - **Digitales Zertifikat verwenden**
   - **Header und Fingerabdruck des digitalen Zertifikats verwenden**
   - **Falls kein Zertifikat vorhanden, Folgendes verwenden**
     - **SHA256-Hash**. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.
     - **Dateipfad**. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm keinen Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle **Erlaubnisregeln für Programme aus folgenden Ordnern erstellen** im Abschnitt **Einstellungen** angegeben wurden.
   - **SHA256-Hash verwenden**
   - **Regeln für Benutzer oder Benutzergruppe erstellen**.

   Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.

5. 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).

6. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird.

7. Geben Sie bei Bedarf im Abschnitt **Ausnahmen vom Gültigkeitsbereich** der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

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

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Konfiguration von Regeln für die Kontrolle des Programmstarts über das Kaspersky Security Center

Erfahren Sie, wie Sie auf der Grundlage von verschiedenen Kriterien eine Liste von Regeln erzeugen oder mithilfe der Aufgabe zur Kontrolle des Programmstarts manuell Erlaubnis- oder Verbotsregeln erstellen können.

Regel für die Kontrolle des Programmstarts hinzufügen

Um eine Regel für die Kontrolle des Programmstarts hinzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Eine Regel hinzufügen** aus.

   Das Fenster **Einstellungen der Regel** wird geöffnet.
4. Geben Sie die folgenden Einstellungen an:

   a. Geben Sie im Feld **Name** den Namen der Regel an.

   b. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Regel:

   - **Erlaubnis**, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien erlaubt.
   - **Verbot**, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien verbietet.

   c. Wählen Sie in der Dropdown-Liste **Gültigkeitsbereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

   - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Dateien kontrolliert.
   - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.

   d. Geben Sie im Feld **Benutzer und/oder Benutzergruppe** die Benutzer an, denen der Programmstart in Übereinstimmung mit dem Regeltyp erlaubt oder verboten werden soll. Gehen Sie hierzu wie folgt vor:

      1. Klicken Sie auf die Schaltfläche **Durchsuchen**.

2. Das Microsoft Windows-Standardfenster Benutzer oder Gruppen auswählen wird geöffnet.

3. Geben Sie die Liste der Benutzer und/oder Benutzergruppen an.

4. Klicken Sie auf OK.

e. Gehen Sie wie folgt vor, wenn Sie die Werte für die im Abschnitt **Auslösekriterien für Regeln** genannten Auslösekriterien der Regel aus einer Datei entnehmen möchten:

1. Klicken Sie auf die Schaltfläche **Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben**.

   Es öffnet sich das Microsoft-Windows-Standardfenster Öffnen.

2. Wählen Sie die Datei aus.

3. Klicken Sie auf Öffnen.

   Die Werte der Kriterien in den Dateien werden in den Feldern im Gruppenfeld **Auslösekriterien für Regeln** angezeigt. Standardmäßig wird das erste Kriterium der Liste ausgewählt, dessen Daten in den Dateieigenschaften enthalten sind.

f. Wählen Sie im Gruppenfeld **Auslösekriterien für Regeln** eine der folgenden Optionen aus:

- **Digitales Zertifikat**, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, welche mit einem digitalen Zertifikat signiert sind:

  - Aktivieren Sie das Kontrollkästchen **Header verwenden**, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit einem ganz bestimmten Header signiert sind.

  - Aktivieren Sie das Kontrollkästchen **Fingerabdruck verwenden**, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.

- **SHA256-Hash**, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, deren Prüfsumme dem angegebenen Wert entspricht.

- **Dateipfad**, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, die sich unter dem angegebenen Dateipfad befinden.

  Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie den Backslash ("\"), um den Pfad korrekt einzutragen.

  Bei der Angabe der Objekte können Sie neben Dateimasken (mittels der Zeichen ? und *) die folgenden Arten von Umgebungsvariablen verwenden: %WINDIR%, %SYSTEM32%, %OSDRIVE%, %PROGRAMFILES%.

g. Gehen Sie wie folgt vor, wenn Sie Ausnahmen von den Regeln hinzufügen möchten:

1. Klicken Sie im Abschnitt **Ausnahmen von der Regel** auf Hinzufügen.

   Das Fenster **Ausnahme von der Regel** wird geöffnet.

2. Geben Sie im Feld **Name** den Namen der Ausnahme ein.

3. Geben Sie die Einstellungen für die Ausnahme von Programmdateien von den Regeln für die Kontrolle des Programmstarts an. Sie können die Felder mit den Parametern aus den Dateieigenschaften über die Schaltfläche **Ausnahme auf Grundlage der Dateieigenschaften festlegen** ausfüllen.

   - Digitales Zertifikat
   - **Header verwenden**
   - **Fingerabdruck verwenden**
   - **SHA256-Hash**
   - **Dateipfad**

4. Klicken Sie auf **OK**.

5. Wiederholen Sie die Schritte (i)-(iv), wenn Sie zusätzliche Ausnahmen hinzufügen möchten.

5. Klicken Sie im Fenster **Einstellungen der Regel** auf **OK**.

Die erstellte Regel wird in der Liste im Fenster **Regeln für die Kontrolle des Programmstarts** angezeigt.

Standarderlaubnismodus aktivieren

Der Standarderlaubnismodus erlaubt den Start aller Programme, sofern diese nicht durch Regeln, oder durch eine KSN-Einstufung als "nicht vertrauenswürdig", blockiert sind. Der Standarderlaubnismodus kann durch Hinzufügen bestimmter Erlaubnisregeln aktiviert werden. Sie können den Standarderlaubnismodus nur für Skripte oder für alle ausführbaren Dateien aktivieren.

Um eine Standarderlaubnisregel hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie aus dem Kontextmenü der Schaltfläche die Option **Eine Regel hinzufügen**.

   Das Fenster **Einstellungen der Regel** wird geöffnet.

3. Geben Sie im Feld **Name** den Namen der Regel an.

4. Wählen Sie in der Dropdown-Liste **Typ** den Regel-Typ **Erlaubnis** aus.

5. Wählen Sie in der Dropdown-Liste **Gültigkeitsbereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

   - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Programmdateien kontrolliert.
   - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.

6. Wählen Sie im Gruppenfeld **Auslösekriterien für Regeln** die Option **Dateipfad** aus.

7. Geben Sie die folgende Maske ein: `?:\`

8. Klicken Sie im Fenster **Einstellungen der Regel** auf **OK**.

Kaspersky Embedded Systems Security übernimmt den Standarderlaubnismodus.

Erlaubnisregeln aus Ereignissen in Kaspersky Security Center erstellen

Um Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center in der Kontrolle des Programmstarts zu erzeugen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche die Option **Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center erstellen**.

3. Wählen Sie das Prinzip aus, nach dem Regeln zur Liste der bereits festgelegten Regeln für die Kontrolle des Programmstarts hinzugefügt werden sollen:

   - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.

   - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.

   - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   Das Fenster **Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.

4. Wählen Sie den Typ von Ereignissen aus, die von der Aufgabe zum Erstellen von Regeln verwendet werden sollen:

   - **Nur Statistik: Programmstart verboten**

   - **Programmstart verboten**

5. Wählen Sie den Zeitraum aus der Dropdown-Liste **Ereignisse anfordern, die in diesem Zeitraum erstellt wurden**.

6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Nutzung des Hashs beim Generieren von Regeln priorisieren**.

   Wenn das Kontrollkästchen aktiviert ist, verwendet Kaspersky Embedded Systems Security die Prüfsumme der Datei, um die Regel zu generieren, wenn sowohl die Prüfsumme als auch das Zertifikat der Datei verfügbar sind.

   Wenn das Kontrollkästchen deaktiviert ist, verwendet Kaspersky Embedded Systems Security das digitale Zertifikat der Datei, um die Regel zu generieren, wenn sowohl die Prüfsumme als auch das Zertifikat der Datei verfügbar sind.

7. Klicken Sie auf die Schaltfläche **Regeln erstellen**.

8. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Kontrolle des Programmstarts**.

Die Regelliste in der Aufgabe zur Kontrolle des Programmstarts wird mit neuen Regeln geladen, basierend auf den Systemdaten des geschützten Geräts mit der installierten Verwaltungskonsole von Kaspersky Security Center.

Wenn die Liste der Regeln für die Kontrolle des Programmstarts bereits in der Richtlinie festgelegt ist, fügt Kaspersky Embedded Systems Security die ausgewählten Regeln aus den Blockierungsereignissen zu den schon angegebenen Regeln hinzu. Regeln mit demselben Hash werden nicht hinzugefügt, da alle Regeln in der Liste eindeutig sein müssen.

Regeln aus einem Bericht von Kaspersky Security Center über blockierte Programme importieren

Sie können Daten über blockierte Programmstarts aus einem Bericht importieren, der in Kaspersky Security Center nach der Ausführung der Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** erstellt wurde, und diese Daten zur Erstellung einer Liste von Erlaubnisregeln für die Kontrolle des Programmstarts in der konfigurierten Richtlinie verwenden.

Bei der Berichterstellung über Ereignisse, die während der Ausführung der Aufgabe zur Kontrolle des Programmstarts eintreten, können Sie verfolgen, für welche Programme der Start blockiert wird.

Vergewissern Sie sich beim Import von Daten aus einem Bericht über blockierte Programme in die Richtlinieneinstellungen davon, dass die verwendete Liste nur diejenigen Programme beinhaltet, deren Start Sie erlauben möchten.

Um für eine Gruppe von geschützten Geräten Erlaubnisregeln zur Kontrolle des Programmstarts auf der Grundlage eines Berichts über blockierte Programme aus Kaspersky Security Center festzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Kontrolle des Programmstarts**.
2. Wählen Sie im Abschnitt **Aufgabenmodus** den Modus **Nur Statistik** aus.
3. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisbenachrichtigungen**, dass:
   - Für **Kritische Ereignisse** die Speicherdauer des Protokolls der Aufgabenausführung für **Programmstart verboten**-Ereignisse die geplante Zeitspanne für die Ausführung der Aufgabe im Modus **Nur Statistik** übersteigt (der Standardwert beträgt 30 Tage).
   - Für Ereignisse mit einer Prioritätsstufe von **Warnung** die Speicherdauer des Protokolls der Aufgabenausführung für **Nur Statistik: Programmstart verboten**-Ereignisse die geplante Zeitspanne für die Ausführung der Aufgabe im Modus **Nur Statistik** übersteigt (der Standardwert beträgt 30 Tage).

     Nach Ablauf der Speicherdauer für Ereignisse werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in der Berichtsdatei aufgeführt. Vergewissern Sie sich vor dem Start der Aufgabe Kontrolle des Programmstarts im Modus **Nur Statistik**, dass die Ausführungsdauer der Aufgabe die festgelegte Zeitspanne für die angegebenen Ereignisse nicht überschreitet.
4. Exportieren Sie nach Abschluss der Aufgabe die protokollierten Ereignisse in eine TXT-Datei:
   a. Wählen Sie im Arbeitsbereich des Knotens **Administrationsserver** in Kaspersky Security Center die Registerkarte **Ereignisse** aus.

b. Erstellen Sie im untergeordneten Knoten **Auswahl erstellen** eine Auswahl von Ereignissen anhand der Eigenschaft Blockiert, um zu sehen, welche Programmstarts durch die Aufgabe zur Kontrolle des Programmstarts blockiert werden.

c. Klicken Sie im Ergebnisfenster der Auswahl auf **Ereignisse in Datei exportieren**, um einen Bericht über die blockierten Programmstarts in einer TXT-Datei zu speichern.

Vergewissern Sie sich vor dem Import und der Verwendung des erstellten Berichts in einer Richtlinie, dass der Bericht nur Daten derjenigen Programme enthält, deren Start Sie erlauben möchten.

5. Importieren Sie die Daten über blockierte Programmstarts in die Aufgabe zur Kontrolle des Programmstarts. Gehen Sie dazu in den Eigenschaften der Richtlinie in den Einstellungen der Aufgabe Kontrolle des Programmstarts wie folgt vor:

a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.

b. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Importieren der Daten über blockierte Programme aus dem Bericht von Kaspersky Security Center**.

c. Wählen Sie das Prinzip aus, nach dem die Regeln aus der auf Grundlage des Berichts von Kaspersky Security Center erstellten Liste zur Liste der bereits bestehenden Regeln für die Kontrolle des Programmstarts hinzugefügt werden:

- **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
- **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
- **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

d. Wählen Sie folgenden Windows-Standardfenster die txt-Datei aus, in die Ereignisse aus dem Bericht über den gesperrten Programmstart exportiert wurden.

e. Klicken Sie auf **Speichern** im Fenster **Regeln für die Kontrolle des Programmstarts**.

Die auf Grundlage des Berichts von Kaspersky Security Center über die blockierten Programme erstellten Regeln werden zur Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt.

Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren

Sie können Berichte, die von der Gruppenaufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" erstellt wurden, importieren und als Liste mit Erlaubnisregeln in der konfigurierten Richtlinie verwenden.

Nach Abschluss der Gruppenaufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" exportiert das Programm die erstellten Erlaubnisregeln in Form von XML-Dateien in den freigegebenen Ordner. Jede Datei mit einer Regelliste wird durch eine Analyse des Starts der Dateien und Programme auf jedem einzelnen geschützten Gerät des Unternehmensnetzwerks erstellt. Die Listen enthalten Erlaubnisregeln für den Start von Dateien und Programmen, deren Typ den in den Einstellungen der Gruppenaufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" gemachten Angaben entspricht.

Um Erlaubnisregeln zur Kontrolle des Programmstarts für eine Gruppe von geschützten Geräten auf der Grundlage automatisch erstellter Liste von Erlaubnisregeln festzulegen, gehen Sie wie folgt vor:

1. Erstellen Sie auf der Registerkarte **Aufgaben** im Detailbereich der Gruppe geschützter Geräte, die Sie konfigurieren, eine Gruppenaufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" oder wählen Sie eine bestehende Aufgabe aus.

2. Konfigurieren Sie in den Eigenschaften der erstellten Gruppenaufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" oder im Assistenten für neue Aufgaben die folgenden Einstellungen:

   - Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für die Speicherung des Berichts über die Aufgabenausführung.

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

   - Legen Sie im Abschnitt **Einstellungen** die Programmtypen fest, deren Start durch die erstellten Regeln erlaubt werden soll. Sie können auch die Zusammensetzung der Ordner ändern, aus denen ein Programmstart erlaubt ist: Standard-Ordner aus dem Gültigkeitsbereich der Aufgabe ausschließen und neue Ordner manuell hinzufügen.

   - Legen Sie im Abschnitt **Einstellungen** die Vorgänge fest, die von der Aufgabe während ihrer Ausführung und nach ihrem Abschluss durchgeführt werden sollen. Legen Sie das Regelerzeugungskriterium und den Namen der Datei fest, in welche die erzeugten Regeln exportiert werden.

   - Passen Sie im Abschnitt **Zeitplan** die Zeitplan-Einstellungen für den Aufgabenstart.

   - Geben Sie im Abschnitt **Benutzerkonto** das Benutzerkonto an, mit dessen Rechten die Aufgabe ausgeführt werden soll.

   - Geben Sie im Abschnitt **Ausnahmen vom Gültigkeitsbereich der Aufgabe** diejenigen Gruppen von geschützten Geräten an, die aus dem Gültigkeitsbereich der Aufgabe ausgeschlossen werden sollen.

     Kaspersky Embedded Systems Security erstellt keine Erlaubnisregeln für Programme, die auf ausgeschlossenen geschützten Geräten gestartet werden.

3. Wählen Sie auf der Registerkarte **Aufgaben** im Detailbereich der konfigurierten Gruppe von geschützten Geräten in der Liste der Gruppenaufgaben die erstellte Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" aus und klicken Sie auf die Schaltfläche **Starten**, um die Aufgabe zu starten.

   Wenn die Aufgabe abgeschlossen ist, werden die automatisch generierten Listen von Erlaubnisregeln in XML-Dateien in einem freigegebenen Ordner gespeichert.

Stellen Sie vor der Verwendung der Aufgabe Kontrolle des Programmstarts im Netzwerk sicher, dass alle geschützten Geräte Zugriff auf einen freigegebenen Ordner haben. Falls die Verwendung eines freigegebenen Ordners im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" auf einem geschützten Gerät in der Testgruppe der geschützten Geräte oder auf einem Referenzcomputer zu starten.

4. Um die erstellten Listen mit Erlaubnisregeln zur Aufgabe zur Kontrolle des Programmstarts hinzuzufügen, gehen Sie wie folgt vor:

   a. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.

   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 "Erstellen von Regeln für die Kontrolle des Programmstarts" erstellt wurden.

   e. Klicken Sie auf **Speichern** im Fenster **Regeln für die Kontrolle des Programmstarts**.

5. Wenn Sie die erstellten Kontrollregeln für den Start von Programmen übernehmen möchten, wählen Sie in den Eigenschaften der Aufgabe "Kontrolle des Programmstarts" in der Richtlinie den Modus **Aktiv** für die Aufgabe aus.

Automatisch auf Grundlage der Aufgabenstarts auf jedem einzelnen geschützten Gerät erstellte Erlaubnisregeln werden für alle geschützten Geräte im Netzwerk, auf denen die konfigurierte Richtlinie übernommen wird, übernommen. Auf diesen geschützten Geräten erlaubt das Programm nur den Start derjenigen Programme, für die Erlaubnisregeln erstellt wurden.

Programmstarts testen

Bevor Sie die konfigurierten Regeln für die Kontrolle des Programmstarts übernehmen, können Sie ein beliebiges Programm testen, um zu bestimmen, welche Regeln für die Kontrolle des Programmstarts durch dieses Programm ausgelöst werden.

Standardmäßig verbietet Kaspersky Embedded Systems Security den Start von Programmen, deren Start nicht durch eine einzelne Regel erlaubt wird. Um das Verbot des Starts wichtiger Programme zu vermeiden, müssen Sie entsprechende Erlaubnisregeln für solche Programme erstellen.

Wenn der Start eines Programms durch mehrere Regeln verschiedener Typen kontrolliert wird, erhalten Verbotsregeln Priorität: Der Start eines Programms wird verboten, wenn es auch nur unter eine Verbotsregel fällt.

Um Regeln für die Kontrolle des Programmstarts zu testen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.
2. Klicken Sie im nächsten Fenster auf **Regeln für die Datei anzeigen**.

   Das Microsoft-Windows-Standardfenster wird geöffnet.
3. Wählen Sie die Datei aus, für die Sie die Kontrolle des Starts testen möchten.

In der Suchzeile wird der Pfad zur angegebenen Datei angezeigt. Die Liste enthält alle Regeln, die ausgelöst werden, wenn die ausgewählte Datei gestartet wird.

Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" erstellen

Um die Einstellungen der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu erstellen und zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Einstellungen** im Assistenten für neue Aufgaben.
2. Passen Sie Folgendes an:
   - Geben Sie ein Präfix für Regelnamen an.
   - Gültigkeitsbereich der Erlaubnisregeln konfigurieren.
3. Klicken Sie auf Weiter.
4. Geben Sie die Aktionen an, die Kaspersky Embedded Systems Security ausführen soll:
   - Bei der Erstellung von Erlaubnisregeln.
   - Nach Abschluss der Aufgabe.
5. Legen Sie im Fenster **Zeitplan** die Einstellungen für den Zeitplan für den Aufgabenstart fest.
6. Klicken Sie auf Weiter.
7. Legen Sie im Fenster Konto für das Ausführen der Aufgabe auswählen das Konto fest, das Sie verwenden möchten.
8. Klicken Sie auf Weiter.
9. Geben Sie einen Aufgabennamen an.
10. Klicken Sie auf Weiter.

    Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

    Das Fenster Erstellung der Aufgabe fertig stellen wird geöffnet.

11. Sie können die Aufgabe optional ausführen, nachdem der Assistent abgeschlossen wurde, indem Sie das Kontrollkästchen Aufgabe nach Abschluss des Assistenten starten aktivieren.

12. Klicken Sie auf Fertig stellen, um die Erstellung der Aufgabe abzuschließen.

Um eine bestehende Regel in Kaspersky Security Center zu konfigurieren, gehen Sie wie folgt vor:

Öffnen Sie das Fenster Eigenschaften: **Erstellen von Regeln für die Kontrolle des Programmstarts** und passen Sie die oben beschriebenen Einstellungen an.

Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Gültigkeitsbereich der Aufgabe einschränken

Um den Gültigkeitsbereich der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu beschränken, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts**.

2. Geben Sie an, wie Erlaubnisregeln erstellt werden:

   - **Erlaubnisregeln auf Grundlage gestarteter Programme erstellen**
   - **Erlaubnisregeln für Programme aus folgenden Ordnern erstellen**

3. Klicken Sie auf OK.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln

Um die Aktionen anzupassen, die Kaspersky Embedded Systems Security ausführen soll, während Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts ausgeführt wird, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts**.

2. Öffnen Sie die Registerkarte **Einstellungen**.

3. Konfigurieren Sie im Abschnitt **Bei der Erstellung von Erlaubnisregeln** die folgenden Parameter:

   - **Digitales Zertifikat verwenden**
   - **Header und Fingerabdruck des digitalen Zertifikats verwenden**
   - **Falls kein Zertifikat vorhanden, Folgendes verwenden**

     - **SHA256-Hash**. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.

- **Dateipfad**. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm keinen Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle **Erlaubnisregeln für Programme aus folgenden Ordnern erstellen** im Abschnitt **Einstellungen** angegeben wurden.

- **SHA256-Hash verwenden**.

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

4. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln

Gehen Sie wie folgt vor, um festzulegen, wie sich Kaspersky Embedded Systems Security nach Abschluss der Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts verhalten soll:

1. Öffnen Sie das Fenster **Eigenschaften: Erstellen von Regeln für die Kontrolle des Programmstarts**.

2. Öffnen Sie die Registerkarte **Einstellungen**.

3. Konfigurieren Sie im Abschnitt **Nach Abschluss der Aufgabe** die folgenden Einstellungen:

   - **Erlaubnisregeln in die Liste der Regeln für die Kontrolle des Programmstarts aufnehmen**.

   - **Prinzip für das Hinzufügen**.

   - **Erlaubnisregeln in Datei exportieren**.

   - **Informationen über das geschützte Gerät zum Dateinamen hinzufügen**.

4. Klicken Sie auf OK.

Die vorgenommenen Einstellungen werden gespeichert.

Kontrolle des Programmstarts über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem geschützten Gerät konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Einstellungen der Aufgabe zur Kontrolle des Programmstarts öffnen

Um die allgemeinen Einstellungen der Aufgabe zur Kontrolle des Programmstarts über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Kontrolle des Programmstarts** aus.
3. Klicken Sie im Detailbereich des untergeordneten Knotens **Kontrolle des Programmstarts** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

Fenster "Regeln für die Kontrolle des Programmstarts" öffnen

Um die Regelliste für die Kontrolle des Programmstarts über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Kontrolle des Programmstarts** aus.
3. Klicken Sie im Ergebnisfenster des Knotens **Kontrolle des Programmstarts** auf den Link **Regeln für die Kontrolle des Programmstarts**.

   Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.
4. Konfigurieren Sie die Regelliste nach Bedarf.

Einstellungen der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" öffnen

Um die Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Automatisches Erstellen von Regeln**.
2. Wählen Sie den untergeordneten Knoten **Erstellen von Regeln für die Kontrolle des Programmstarts**.
3. Klicken Sie im Ergebnisbereich des untergeordneten Knotens **Erstellen von Regeln für die Kontrolle des Programmstarts** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Konfigurieren Sie die Aufgabe nach Bedarf.

Aufgabe Kontrolle des Programmstarts konfigurieren

Um die allgemeinen Aufgabeneinstellungen für die Kontrolle des Programmstarts zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Auf der Registerkarte **Allgemein**:
     - Modus der Aufgabe zur Kontrolle des Programmstarts.
     - Gültigkeitsbereich der Regeln in der Aufgabe.
     - Verwendung von KSN.
   - Einstellungen der Kontrolle für Installationspakete auf der Registerkarte **Überwachung von Installationspaketen**.
   - Einstellungen für den Zeitplan für den Aufgabenstart auf den Registerkarten **Zeitplan** und **Erweitert**.
3. Klicken Sie im Fenster **Aufgabeneinstellungen** auf OK.

   Die Änderung der Einstellungen wird gespeichert.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Modus der Aufgabe zur Kontrolle des Programmstarts auswählen

Gehen Sie wie folgt vor, um den Modus der Aufgabe zur Kontrolle des Programmstarts zu konfigurieren:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Geben Sie auf der Registerkarte **Aufgabenmodus** in der Dropdown-Liste **Allgemein** den Modus der Aufgabe an.
3. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten**.

   Kaspersky Embedded Systems Security legt bei jeder Änderung der Einstellungen der Aufgabe zur Kontrolle des Programmstarts eine neue Liste mit Ereignissen im Cache an. Das bedeutet, dass die Kontrolle des Programmstarts gemäß den aktuellen Sicherheitseinstellungen ausgeführt wird.
4. Deaktivieren oder aktivieren Sie **Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten**.
5. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Alle Versuche, Programme zu starten, werden im Protokoll der Aufgabenausführung festgehalten.

Modus der Aufgabe zur Kontrolle des Programmstarts konfigurieren

Gehen Sie wie folgt vor, um den Modus der Aufgabe zur Kontrolle des Programmstarts zu definieren:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Geben Sie auf der Registerkarte **Allgemein** im Abschnitt **Gültigkeitsbereich der Regel** die folgenden Einstellungen an:
   - **Regeln für ausführbare Dateien verwenden**
   - **Laden von DLL-Modulen überwachen**

     Das Überwachen des Ladens von DLL-Modulen kann sich auf die Leistung des Betriebssystems auswirken.

   - **Regeln für Skripte und MSI-Pakete verwenden**
3. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Verwendung von KSN konfigurieren

Gehen Sie wie folgt vor, um die Verwendung der KSN-Dienste für die Aufgabe zur Kontrolle des Programmstarts einzurichten:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Geben Sie auf der Registerkarte **Allgemein** im Abschnitt **Verwendung von KSN** die Einstellungen für die Verwendung von KSN-Diensten an.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten**.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben**.
   - Wenn das Kontrollkästchen **Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben** aktiviert ist, geben Sie die Benutzer und/oder Benutzergruppen an, denen der Start von laut KSN vertrauenswürdigen Programmen erlaubt ist. Gehen Sie hierzu wie folgt vor:

     a. Klicken Sie auf die Schaltfläche **Ändern**.

     Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** wird geöffnet.

Standardmäßig ist allen Nutzen der Zugriff auf Programme, die laut KSN vertrauenswürdige sind, erlaubt.

b. Geben Sie die Liste der Benutzer und/oder Benutzergruppen an.

c. Klicken Sie auf **OK**.

3. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Kontrolle für Installationspakete

Um ein vertrauenswürdiges Installationspaket hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Aktivieren Sie auf der Registerkarte **Überwachung von Installationspaketen** das Kontrollkästchen **Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben**.

Sie können das Kontrollkästchen **Verteilung von Software mittels aufgelisteter Programme und Installationspakete automatisch erlauben** aktivieren, wenn das Kontrollkästchen **Regeln für ausführbare Dateien verwenden** auf der Registerkarte **Allgemein** in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts aktiviert ist.

3. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Verteilung von Programmen mithilfe von Windows Installer immer erlauben**.

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

4. Aktivieren Sie bei Bedarf das Kontrollkästchen **Verteilung von Programmen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben**.

Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an das geschützte Gerät bis zu der Installation bzw. dem Update. Das Programm überwacht die Prozesse nicht, wenn einer der Schritte der Softwareverteilung bereits vor der Installation des Systems auf dem geschützten Gerät ausgeführt wurde.

5. Um die Liste der vertrauenswürdigen Installationspakete zu bearbeiten, klicken Sie auf die Schaltfläche **Liste der Pakete bearbeiten** und wählen Sie im nächsten Fenster eine der verfügbaren Methoden aus:

- **Ein Installationspaket hinzufügen**.

a. Klicken Sie auf die Schaltfläche **Durchsuchen**.

b. Wählen Sie die ausführbare Datei oder das Installationspaket aus.

Im Abschnitt **Kriterien für Vertrauenswürdigkeit** werden die Daten zur ausgewählten Datei automatisch angezeigt.

c. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Weitere Verteilung von aus diesem Installationspaket erstellten Programmen erlauben**.

d. Wählen Sie eine der beiden verfügbaren Varianten der Kriterien für die Vertrauenswürdigkeit aus, auf deren Grundlage die Datei oder das Installationspaket als vertrauenswürdig gelten:

- **Digitales Zertifikat verwenden**
- **SHA256-Hash verwenden**

- **Mehrere Pakete anhand von Hash hinzufügen**.

  Sie können eine unbegrenzte Anzahl an ausführbaren Dateien und Installationspaketen auswählen und gleichzeitig zur Liste hinzufügen. Kaspersky Embedded Systems Security untersucht den Hash und erlaubt dem Betriebssystem den Start der angegebenen Dateien.

- **Ausgewähltes Paket bearbeiten**.

  Verwenden Sie diese Variante, um eine andere ausführbare Datei oder ein anderes Installationspaket auszuwählen sowie die Kriterien für die Vertrauenswürdigkeit zu ändern.

- Liste mit Paketen aus Datei importieren.

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

6. Wenn Sie ein früher hinzugefügtes Programm oder Installationspaket aus der Liste der vertrauenswürdigen Installationspakete löschen möchten, klicken Sie auf die Schaltfläche **Installationspakete löschen**. Der Start extrahierter Dateien wird erlaubt.

   Um den Start extrahierter Dateien zu verbieten, deinstallieren Sie das Programm vollständig vom geschützten Gerät oder erstellen Sie eine Verbotsregel in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts.

7. Klicken Sie auf **OK**.

Ihre neu konfigurierten Einstellungen werden gespeichert.

Regeln für die Kontrolle des Programmstarts konfigurieren

Erfahren Sie, wie Sie eine Liste von Regeln erzeugen, importieren und exportieren oder mithilfe der Aufgabe zur Kontrolle des Programmstarts manuell Erlaubnis- oder Verbotsregeln erstellen können.

Regel für die Kontrolle des Programmstarts hinzufügen

Um eine Regel für die Kontrolle des Programmstarts hinzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Eine Regel hinzufügen** aus.

   Das Fenster **Einstellungen der Regel** wird geöffnet.

4. Geben Sie die folgenden Einstellungen an:

   a. Geben Sie im Feld **Name** den Namen der Regel an.

   b. Wählen Sie in der Dropdown-Liste **Typ** den Typ der Regel:

   - **Erlaubnis**, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien erlaubt.
   - **Verbot**, wenn Sie möchten, dass die Regel den Start von Programmen in Übereinstimmung mit den in den Einstellungen der Regel angegebenen Kriterien verbietet.

   c. Wählen Sie in der Dropdown-Liste **Gültigkeitsbereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

   - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Dateien kontrolliert.
   - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.

   d. Geben Sie im Feld **Benutzer und/oder Benutzergruppe** die Benutzer an, denen der Programmstart in Übereinstimmung mit dem Regeltyp erlaubt oder verboten werden soll. Gehen Sie hierzu wie folgt vor:

      1. Klicken Sie auf die Schaltfläche **Durchsuchen**.
      2. Das Microsoft Windows-Standardfenster Benutzer oder Gruppen auswählen wird geöffnet.
      3. Geben Sie die Liste der Benutzer und/oder Benutzergruppen an.
      4. Klicken Sie auf OK.

   e. Gehen Sie wie folgt vor, wenn Sie die Werte für die im Abschnitt **Auslösekriterien für Regeln** genannten Auslösekriterien der Regel aus einer Datei entnehmen möchten:

      1. Klicken Sie auf die Schaltfläche **Auslösekriterien für Regeln aus den Dateieigenschaften vorgeben**.

         Es öffnet sich das Microsoft-Windows-Standardfenster Öffnen.

      2. Wählen Sie die Datei aus.
      3. Klicken Sie auf Öffnen.

         Die Werte der Kriterien in den Dateien werden in den Feldern im Gruppenfeld **Auslösekriterien für Regeln** angezeigt. Standardmäßig wird das erste Kriterium der Liste ausgewählt, dessen Daten in den Dateieigenschaften enthalten sind.

   f. Wählen Sie im Gruppenfeld **Auslösekriterien für Regeln** eine der folgenden Optionen aus:

   - **Digitales Zertifikat**, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, welche mit einem digitalen Zertifikat signiert sind:
     - Aktivieren Sie das Kontrollkästchen **Header verwenden**, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit einem ganz bestimmten

Header signiert sind.

- Aktivieren Sie das Kontrollkästchen **Fingerabdruck verwenden**, wenn Sie möchten, dass die Regel lediglich den Start von Dateien kontrolliert, die mit einem digitalen Zertifikat mit dem angegebenen Fingerabdruck signiert sind.

- **SHA256-Hash**, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, deren Prüfsumme dem angegebenen Wert entspricht.

- **Dateipfad**, wenn Sie möchten, dass die Regel den Start von Programmen kontrolliert, die mithilfe von Dateien gestartet werden, die sich unter dem angegebenen Dateipfad befinden.

  Kaspersky Embedded Systems Security erkennt keine Pfade, die Schrägstriche ("/") enthalten. Verwenden Sie den Backslash ("\"), um den Pfad korrekt einzutragen.

  Bei der Angabe der Objekte können Sie neben Dateimasken (mittels der Zeichen ? und *) die folgenden Arten von Umgebungsvariablen verwenden: %WINDIR%, %SYSTEM32%, %OSDRIVE%, %PROGRAMFILES%.

g. Gehen Sie wie folgt vor, wenn Sie Ausnahmen von den Regeln hinzufügen möchten:

1. Klicken Sie im Abschnitt **Ausnahmen von der Regel** auf Hinzufügen.

   Das Fenster **Ausnahme von der Regel** wird geöffnet.

2. Geben Sie im Feld **Name** den Namen der Ausnahme ein.

3. Geben Sie die Einstellungen für die Ausnahme von Programmdateien von den Regeln für die Kontrolle des Programmstarts an. Sie können die Felder mit den Parametern aus den Dateieigenschaften über die Schaltfläche **Ausnahme auf Grundlage der Dateieigenschaften festlegen** ausfüllen.

   - Digitales Zertifikat
   - Header verwenden
   - Fingerabdruck verwenden
   - SHA256-Hash
   - Dateipfad

4. Klicken Sie auf **OK**.

5. Wiederholen Sie die Schritte (i)-(iv), wenn Sie zusätzliche Ausnahmen hinzufügen möchten.

5. Klicken Sie im Fenster **Einstellungen der Regel** auf **OK**.

Die erstellte Regel wird in der Liste im Fenster **Regeln für die Kontrolle des Programmstarts** angezeigt.

Standarderlaubnismodus aktivieren

Der Standarderlaubnismodus erlaubt den Start aller Programme, sofern diese nicht durch Regeln, oder durch eine KSN-Einstufung als "nicht vertrauenswürdig", blockiert sind. Der Standarderlaubnismodus kann durch Hinzufügen bestimmter Erlaubnisregeln aktiviert werden. Sie können den Standarderlaubnismodus nur für Skripte oder für alle ausführbaren Dateien aktivieren.

Um eine Standarderlaubnisregel hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Eine Regel hinzufügen** aus.

   Das Fenster **Einstellungen der Regel** wird geöffnet.
4. Geben Sie im Feld **Name** den Namen der Regel an.
5. Wählen Sie in der Dropdown-Liste **Typ** den Regel-Typ **Erlaubnis** aus.
6. Wählen Sie in der Dropdown-Liste **Gültigkeitsbereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:

   - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Programmdateien kontrolliert.
   - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.
7. Wählen Sie im Gruppenfeld **Auslösekriterien für Regeln** die Option **Dateipfad** aus.
8. Geben Sie die folgende Maske ein: `?:\`
9. Klicken Sie im Fenster **Einstellungen der Regel** auf **OK**.

Kaspersky Embedded Systems Security übernimmt den Standarderlaubnismodus.

Erlaubnisregeln aus Ereignissen der Aufgabe zur Kontrolle des Programmstarts erstellen

Um eine Konfigurationsdatei mit Erlaubnisregeln zu erstellen, die aus Aufgabenereignissen der Kontrolle des Programmstarts erzeugt wurden, gehen Sie wie folgt vor:

1. Führen Sie die Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** aus, um Informationen über alle Programmstarts auf einem geschützten Gerät im Protokoll der Aufgabenausführung aufzuzeichnen.
2. Nach Abschluss der Aufgabe im Modus **Nur Statistik** öffnen Sie das Protokoll der Aufgabenausführung über die Schaltfläche **Protokoll der Aufgabenausführung öffnen** im Abschnitt **Verwaltung** im Detailbereich des Knotens **Kontrolle des Programmstarts**.
3. Klicken Sie im Fenster **Protokolle** auf die Schaltfläche **Regeln anhand von Ereignissen erstellen**.

Kaspersky Embedded Systems Security erstellt eine Konfigurationsdatei im xml-Format mit einer Liste der Regeln, die anhand der Ereignisse der Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** erstellt wurden. In der Aufgabe zur Kontrolle des Programmstarts können Sie diese Regelliste übernehmen

Bevor Sie die aus den protokollierten Aufgabenereignissen erzeugte Regelliste übernehmen, wird empfohlen, die Liste zu überprüfen und manuell zu verarbeiten, um sicher zu gehen, dass der Start von kritischen Dateien (beispielsweise Systemdateien) durch die angegebene Regel erlaubt wird.

Unabhängig vom Aufgabenmodus werden alle Aufgabenereignisse im Protokoll der Aufgabenausführung aufgezeichnet. Sie können eine Konfigurationsdatei mit der Regelliste anhand des Protokolls erstellen, das erstellt wurde, während die Aufgabe im Modus **Aktiv** ausgeführt wurde. Dieses Szenario wird mit Ausnahme von wichtigen Fällen nicht empfohlen, da eine endgültige Regelliste erzeugt werden muss, bevor die Aufgabe im Modus **Aktiv** ausgeführt wird, damit sie effektiv wird.

Regeln für die Kontrolle des Programmstarts exportieren

Um Regeln für die Kontrolle des Programmstarts in eine Konfigurationsdatei zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.
2. Klicken Sie auf **In Datei exportieren**.

   Das Microsoft-Windows-Standardfenster wird geöffnet.
3. Geben Sie im erscheinenden Fenster die Datei an, in die Sie die Regeln exportieren möchten. Existiert die angegebene Datei nicht, so wird sie erstellt. Existiert bereits eine Datei mit dem angegebenen Namen, so wird ihr Inhalt nach überschrieben, wenn die Regeln exportiert werden.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Regeleinstellungen werden in die angegebene Datei exportiert.

Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren

Um Regeln für die Kontrolle des Programmstarts zu importieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regeln aus XML-Datei importieren** aus.
4. Geben Sie an, auf welche Weise die zu importierenden Regeln hinzugefügt werden sollen. Wählen Sie hierzu einen der Punkte des Kontextmenüs der Schaltfläche **Regeln aus XML-Datei importieren** aus:

   - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
   - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
   - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.

5. Wählen Sie im Microsoft-Windows-Fenster **Öffnen** die XML-Datei aus, welche die Regeln für die Kontrolle des Programmstarts enthält.

6. Klicken Sie auf **Öffnen**.

Die importierten Regeln werden in der Liste im Fenster **Regeln für die Kontrolle des Programmstarts** angezeigt.

Regeln für die Kontrolle des Programmstarts löschen

Um Regeln für die Kontrolle des Programmstarts zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Kontrolle des Programmstarts**.

2. Wählen Sie in der Liste der Regeln eine oder mehrere Regeln aus, die Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Auswahl entfernen**.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die ausgewählten Regeln für die Kontrolle des Programmstarts werden gelöscht.

Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" konfigurieren

Um die Einstellungen der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen** der Aufgabe **Erstellen von Regeln für die Kontrolle des Programmstarts**.

2. Passen Sie die folgenden Einstellungen an:

   - Auf der Registerkarte **Allgemein**:

     - Geben Sie ein **Präfix für Regelnamen** an.

     - Gültigkeitsbereich der Erlaubnisregeln konfigurieren.

   - Geben Sie auf der Registerkarte **Aktionen** die Aktionen an, die Kaspersky Embedded Systems Security ausführen soll.

   - Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** die Einstellungen für den Zeitplan für den Aufgabenstart an.

   - Passen Sie auf der Registerkarte **Mit folgenden Rechten starten** die Einstellungen für den Aufgabenstart mit Benutzerrecht an.

3. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung.

Gültigkeitsbereich der Aufgabe einschränken

Um den Gültigkeitsbereich der Aufgabe "Erstellen von Regeln für die Kontrolle des Programmstarts" zu beschränken, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen** der Aufgabe **Erstellen von Regeln für die Kontrolle des Programmstarts**.
2. Geben Sie an, wie Erlaubnisregeln erstellt werden:
   - **Erlaubnisregeln auf Grundlage gestarteter Programme erstellen**.
   - **Erlaubnisregeln für Programme aus folgenden Ordnern erstellen**.
3. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführenden Aktionen bei der automatischen Erstellung von Regeln

So passen Sie die Aktionen von Kaspersky Embedded Systems Security während der Ausführung und nach Abschluss der Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts an:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen** der Aufgabe **Erstellen von Regeln für die Kontrolle des Programmstarts**.
2. Öffnen Sie die Registerkarte **Einstellungen**.
3. Konfigurieren Sie im Abschnitt **Bei der Erstellung von Erlaubnisregeln** die folgenden Parameter:
   - **Digitales Zertifikat verwenden**
   - **Header und Fingerabdruck des digitalen Zertifikats verwenden**
   - **Falls kein Zertifikat vorhanden, Folgendes verwenden**
     - **SHA256-Hash**. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.
     - **Dateipfad**. Als ein Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm keinen Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle **Erlaubnisregeln für Programme aus folgenden Ordnern erstellen** im Abschnitt **Einstellungen** angegeben wurden.
   - **SHA256-Hash verwenden**
   - **Regeln für Benutzer oder Benutzergruppe erstellen**.

4. Konfigurieren Sie im Abschnitt **Nach Abschluss der Aufgabe** die folgenden Einstellungen:
   - Erlaubnisregeln in die Liste der Regeln für die Kontrolle des Programmstarts aufnehmen.
   - Prinzip für das Hinzufügen.
   - **Erlaubnisregeln in Datei exportieren**.
   - Informationen über das geschützte Gerät zum Dateinamen hinzufügen.
5. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Durchzuführende Aktionen nach Abschluss der automatischen Erstellung von Regeln

Gehen Sie wie folgt vor, um festzulegen, wie sich Kaspersky Embedded Systems Security nach Abschluss der Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts verhalten soll:

1. Öffnen Sie das Fenster Aufgabeneinstellungen der Aufgabe **Erstellen von Regeln für die Kontrolle des Programmstarts**.
2. Öffnen Sie die Registerkarte **Einstellungen**.
3. Konfigurieren Sie im Abschnitt **Nach Abschluss der Aufgabe** die folgenden Einstellungen:
   - Erlaubnisregeln in die Liste der Regeln für die Kontrolle des Programmstarts aufnehmen.
   - Prinzip für das Hinzufügen.
   - **Erlaubnisregeln in Datei exportieren**.
   - Informationen über das geschützte Gerät zum Dateinamen hinzufügen.
4. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Kontrolle des Programmstarts über das Web-Plug-in verwalten

So konfigurieren Sie die Aufgaben zur Kontrolle des Programmstarts über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Überwachung der Desktop-Aktivitäten** aus.
5. Klicken Sie im Unterabschnitt **Kontrolle des Programmstarts** auf **Einstellungen**.

6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen der Aufgabe "Kontrolle des Programmstarts"

Einstellung	Beschreibung
Aufgabenmodus	In dieser Dropdown-Liste können Sie den Modus der Aufgabe zur Kontrolle des Programmstarts auswählen: • **Aktiv**. Kaspersky Embedded Systems Security verwendet die festgelegten Regeln, um den Start jedes Programms zu kontrollieren. • **Nur Statistik**. Kaspersky Embedded Systems Security verwendet die festgelegten Regeln nicht, um den Start von Programmen zu kontrollieren. Stattdessen werden Informationen über Startereignisse im Protokoll der Aufgabenausführung aufgezeichnet. Allen Programmen wird der Start erlaubt. Sie können diesen Modus für die Erstellung einer Liste der Regeln für die Kontrolle des Programmstarts auf Grundlage der im Protokoll der Aufgabenausführung enthaltenen Informationen über verbotene Programmstarts verwenden. Standardmäßig wird die Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** gestartet.
Weitere Starts der überwachten Programme nach gleichem Schema wie beim ersten Start verarbeiten	Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle wiederholter Programmstarts auf Basis von Einträgen des Caches für Ereignisinformationen. Wenn das Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security nachfolgende Starts eines Programms auf der Grundlage der Einstufung der Aufgabe in Bezug auf den ersten Start des Programms. Wenn beispielsweise der erste Programmstart durch die Regeln für die Kontrolle des Programmstarts erlaubt wurde, so verbleibt der Eintrag über diese Entscheidung im Cache und der zweite und alle nachfolgenden Starts dieses Programms werden ohne erneute Überprüfung ebenfalls erlaubt. Ist das Kontrollkästchen deaktiviert, so analysiert Kaspersky Embedded Systems Security ein Programm bei jedem versuchten Programmstart von neuem. Das Kontrollkästchen ist standardmäßig deaktiviert.
Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten	Wenn das Kontrollkästchen aktiviert ist, verbietet Kaspersky Embedded Systems Security den Start des Kommandozeileninterpreters auch dann, wenn der Start von Interpretern erlaubt ist. Ein Kommandozeileninterpreter kann ohne Befehl nur dann gestartet werden, wenn beide der folgenden Bedingungen erfüllt sind: • Der Start des Kommandozeileninterpreters ist erlaubt. • Der auszuführende Befehl ist erlaubt. Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security nur Erlaubnisregeln, wenn ein Kommandozeileninterpreter gestartet wird. Der Start wird verboten, wenn keine Erlaubnisregel übernommen wurde oder der ausführbare Prozess laut KSN nicht vertrauenswürdig ist. Wenn eine Erlaubnisregel übernommen wird oder der Prozess laut KSN vertrauenswürdig ist, kann ein Kommandozeileninterpreter mit oder ohne auszuführenden Befehl gestartet werden.

	Kaspersky Embedded Systems Security erkennt die folgenden Kommandozeileninterpreter: • cmd.exe • powershell.exe • python.exe • perl.exe Das Kontrollkästchen ist standardmäßig deaktiviert.
Regeln für ausführbare Dateien verwenden	Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von ausführbaren Dateien. Ist dieses Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security den Start ausführbarer Dateien mithilfe vorgegebener Regeln, in deren Einstellungen **Ausführbare Dateien** als Geltungsbereich angegeben ist. Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Starts ausführbarer Dateien mithilfe vorgegebener Regeln. Der Start ausführbarer Dateien ist erlaubt. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Laden von DLL-Modulen überwachen	Dieses Kontrollkästchen aktiviert oder deaktiviert die Überwachung des Ladens von DLL-Modulen. Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Embedded Systems Security das Laden von DLL-Modulen mithilfe vorgegebener Regeln, in deren Einstellungen **Ausführbare Dateien** als Geltungsbereich angegeben sind. Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Ladens von DLL-Modulen mithilfe vorgegebener Regeln. Laden von DLL-Modulen ist erlaubt. Das Kontrollkästchen ist aktiv, wenn das Kontrollkästchen **Regeln für ausführbare Dateien verwenden** aktiviert ist. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Regeln für Skripte und MSI-Pakete verwenden	Dieses Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von Skripten und MSI-Paketen. Wenn dieses Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Embedded Systems Security den Start von Skripten und MSI-Paketen mithilfe vorgegebener Regeln, in deren Einstellungen Skripte und MSI-Pakete als Geltungsbereich angegeben sind. Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Embedded Systems Security keine Kontrolle des Starts von Skripten und MSI-Paketen mithilfe vorgegebener Regeln. Das Ausführen von Skripten und MSI-Paketen ist gestattet. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
Start von Programmen, die laut KSN nicht vertrauenswürdig sind, verbieten	Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß der Programmreputation in KSN.

	Ist das Kontrollkästchen aktiviert, blockiert Kaspersky Embedded Systems Security den Start aller Programme, die laut KSN nicht vertrauenswürdig sind. Erlaubnisregeln zur Kontrolle des Programmstarts, die für Programme gelten, die laut KSN nicht vertrauenswürdig sind, werden nicht ausgelöst. Die Aktivierung des Kontrollkästchens gewährleistet zusätzlichen Schutz vor Schadsoftware. Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security die Reputation von Programmen, die laut KSN nicht vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die für diese Programme gelten. Das Kontrollkästchen ist standardmäßig deaktiviert.
Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben	Dieses Kontrollkästchen aktiviert/deaktiviert die Kontrolle des Programmstarts gemäß der Programmreputation in KSN. Ist das Kontrollkästchen aktiviert, erlaubt Kaspersky Embedded Systems Security den Start von Programmen, wenn sie laut KSN vertrauenswürdig sind. Dabei haben die Verbotsregeln für die Kontrolle des Programmstarts, die für die im KSN vertrauenswürdigen Programme gelten, eine höhere Priorität: wenn ein Programm laut den KSN-Diensten vertrauenswürdig ist, wird der Programmstart verboten. Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Embedded Systems Security die Reputation von Programmen, die laut KSN vertrauenswürdig sind, nicht und erlaubt oder verbietet den Start in Übereinstimmung mit den Regeln, die für solche Programme gelten. Das Kontrollkästchen ist standardmäßig deaktiviert.
Benutzer und / oder Benutzergruppen, denen der Start von laut KSN vertrauenswürdigen Programmen erlaubt ist	Wenn das Kontrollkästchen **Start von Programmen, die laut KSN vertrauenswürdig sind, erlauben** aktiviert ist, können Sie hier die Benutzer und Benutzergruppen angeben, denen der Start von laut KSN vertrauenswürdigen Programmen erlaubt ist. Standardmäßig sind die folgenden Benutzer angegeben: **Jeder** und **NT AUTHORITY\SYSTEM**.
Regeln	Passen Sie Erlaubnis- oder Verbotsregeln für die Aufgabe "Kontrolle des Programmstarts" an.
Überwachung von Installationspaketen	Sie können vertrauenswürdiges Installationspakete hinzufügen.
Aufgabenverwaltung	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Gerätekontrolle

Dieser Abschnitt informiert über die Aufgabe zur Gerätekontrolle und erläutert die Konfiguration dieser Aufgabe.

Über die Aufgabe Gerätekontrolle

Kaspersky Embedded Systems Security kontrolliert die Registrierung und die Verwendung von externen Geräten und CD-/DVD-Geräten, um das geschützte Gerät vor Gefahren zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können.

Kaspersky Embedded Systems Security kontrolliert die folgenden Verbindungen zu externen USB-Geräten:

- USB-Flash-Laufwerke
- CD-/DVD-ROM-Laufwerke
- USB-Diskettenlaufwerke
- über USB angeschlossene Netzwerkadapter
- über USB angeschlossene mobile MTP-Geräte

Kaspersky Embedded Systems Security informiert Sie mithilfe eines entsprechenden Ereignisses in den Aufgabenprotokollen und Ereignisprotokollen über alle Geräte, die über USB angeschlossen werden. Das Ereignis enthält den Gerätetyp und den Verbindungspfad. Wenn die Aufgabe zur Gerätekontrolle gestartet wurde, prüft Kaspersky Embedded Systems Security alle USB-Geräte und listet sie auf. Sie können die Benachrichtigungen im Abschnitt "Benachrichtigungen anpassen" in Kaspersky Security Center anpassen.

Die Aufgabe zur Gerätekontrolle überwacht die Verbindungsversuche der externen Geräte mit dem geschützten Gerät 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 externen Gerät einen der folgenden Status zu:

- *Vertrauenswürdig*. Gerät, mit dem der Datenaustausch erlaubt ist. Der *Geräteinstanzpfad* eines solchen Geräts fällt unter den Anwendungsbereich zumindest einer Erlaubnisregel.
- *Nicht vertrauenswürdig*. Gerät, mit dem der Datenaustausch verboten ist. Der Geräteinstanzpfad eines solchen Geräts fällt nicht unter den Anwendungsbereich von Erlaubnisregeln.

Sie können mithilfe der Aufgabe Erstellen von Regeln für die Gerätekontrolle Erlaubnisregeln für externe Geräte erstellen, mit denen Sie einen Datenaustausch erlauben wollen. Sie können den Gültigkeitsbereich von bereits erstellten Erlaubnisregeln auch erweitern. Sie können keine Erlaubnisregeln manuell erstellen.

Kaspersky Embedded Systems Security identifiziert im System registrierte externe Geräte anhand des Wertes des Geräteinstanzpfads. Der Geräteinstanzpfad ist ein eindeutiges Merkmal für jedes externe Gerät. Die Informationen zum Geräteinstanzpfad sind in den Eigenschaften des externen Geräts im Windows-System enthalten und werden von Kaspersky Embedded Systems Security während der Erstellung von Regeln automatisch bestimmt.

Die Aufgabe Gerätekontrolle kann in einem der folgenden beiden Modi ausgeführt werden:

- **Aktiv**. Kaspersky Embedded Systems Security kontrolliert mithilfe der Regeln den Anschluss von Flash-Laufwerken und anderen externen Geräten und verbietet oder erlaubt die Verwendung aller Geräte gemäß dem Prinzip des standardmäßigen Verbots (Default Deny) und den festgelegten Erlaubnisregeln. Die Verwendung von vertrauenswürdigen externen Geräten wird erlaubt. Die Verwendung von nicht vertrauenswürdigen externen Geräten wird standardmäßig verboten.

  Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, vor dem Start der Aufgabe zur Gerätekontrolle im Modus **Aktiv** an das geschützte Gerät angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder das geschützte Gerät neu zu starten. Anderenfalls wird das "Prinzip des standardmäßigen Verbots" für das Gerät nicht übernommen.

- **Nur Statistik**. Kaspersky Embedded Systems Security kontrolliert das Anschließen von Flash-Laufwerken und anderen externen Geräten nicht, sondern speichert lediglich die Informationen zu Anschluss und Registrierung von externen Geräten auf dem geschützten Gerät sowie zu den Erlaubnisregeln zur Gerätekontrolle, denen die angeschlossenen Geräte unterliegen, im Protokoll der Aufgabenausführung. Die Verwendung aller externen Geräte wird erlaubt. Dieser Modus ist standardmäßig eingestellt.

  Sie können diesen Modus für die Erstellung von Regeln aufgrund von Informationen über Blockierung von Geräten verwenden, die während der Aufgabenausführung aufgezeichnet wurden.

Über die Regeln zur Gerätekontrolle

Kaspersky Embedded Systems Security verwendet keine Erlaubnisregeln für MTP-Mobilgeräte.

Die Regeln werden für jedes Gerät, das in diesen Moment oder zuvor an das geschützte Gerät angeschlossen wurde, individuell erstellt, wenn über dieses Gerät Daten im System gespeichert wurden.

So erstellen Sie Erlaubnisregeln zur Gerätekontrolle:

- Die Aufgabe zum Erstellen von Erlaubnisregeln übernehmen.
- Den Modus "Nur Statistik" in der Aufgabe zur Gerätekontrolle verwenden.
- Die Systemdaten über angeschlossene Geräte übernehmen.
- Den Gültigkeitsbereich von bereits erstellen Regeln erweitern.

Die maximale Anzahl der Regeln zur Gerätekontrolle, die Kaspersky Embedded Systems Security unterstützt, beträgt 3072.

Die Regeln für die Gerätekontrolle werden nachfolgend beschrieben.

Regeltyp

Typ der Regel – immer *Erlaubnis*. Die Aufgabe zur Gerätekontrolle sperrt die Verbindung aller Flash-Laufwerke und anderer externer Geräte standardmäßig, wenn sie nicht in den Gültigkeitsbereich von mindestens einer Erlaubnisregel fallen.

Auslösekriterium und Gültigkeitsbereich der Regel

Die Regeln für die Gerätekontrolle identifizieren Flash-Laufwerke und andere externe Geräte anhand des *Geräteinstanzpfad*. Der Geräteinstanzpfad ist ein eindeutiger Identifikator, der dem Gerät vom System zum Zeitpunkt seines Anschlusses und seiner Registrierung als externes Gerät oder CD-/DVD-Laufwerk (beispielsweise IDE oder SCSI) zugewiesen wird.

Kaspersky Embedded Systems Security kontrolliert den Anschluss externer CD-/DVD-Laufwerke unabhängig von der Schnittstelle des Anschlusses. Beim Montieren solcher Geräte über USB registriert das Betriebssystem zwei Werte für die Geräteexemplarklasse: für das externe Gerät, sowie für das CD/DVD-Gerät (beispielsweise IDE oder SCSI). Für einen korrekten Anschluss solcher Geräte sind Erlaubnisregeln für jeden Wert des Geräteinstanzpfades erforderlich.

Kaspersky Embedded Systems Security bestimmt den Geräteinstanzpfad und schlüsselt den gefundenen Wert auf die folgenden Elemente auf:

- Hersteller (VID) des Geräts
- Controller-Typ (PID) des Geräts
- Seriennummer des Geräts

Sie können den Geräteinstanzpfad nicht manuell festlegen. Die in den Eigenschaften der Erlaubnisregel festgelegten Auslösekriterien für die Regel bestimmen den Gültigkeitsbereich dieser Regel. Standardmäßig beinhaltet der Gültigkeitsbereich einer gerade erstellten Erlaubnisregel ein Gerät, auf der Grundlage von dessen Eigenschaften Kaspersky Embedded Systems Security die Erlaubnisregel erstellt hat. Sie können die angegebenen Werte mithilfe der Maske in den Eigenschaften der erstellten Regel bearbeiten, um den Gültigkeitsbereich der Regel auszudehnen.

Daten des Ausgangsgeräts

Die Daten des Geräts, aufgrund von dessen Eigenschaften Kaspersky Embedded Systems Security die Erlaubnisregel gebildet hat, werden in den Eigenschaften der einzelnen Regeln angezeigt.

Die Daten des Ausgangsgeräts enthalten die folgenden Informationen:

- **Geräteinstanzpfad**. Aufgrund dieses Wertes bestimmt Kaspersky Embedded Systems Security die Auslösekriterien für die Regel und füllt die Felder **Hersteller (VID)**, **Controller-Typ (PID)**, **Seriennummer** im Abschnitt **Gültigkeitsbereich der Regel** im Fenster **Eigenschaften der Regel** aus.
- **Anzeigename**. Name, der vom Hersteller in den Eigenschaften des Geräts angegeben ist.

Kaspersky Embedded Systems Security bestimmt die Daten des Ausgangsgeräts zum Zeitpunkt des Erstellens der Regel automatisch. Im Folgenden können Sie diese Werte verwenden, um zu bestimmen, aufgrund der Daten welchen Geräts die Regel erstellt wurde. Die Daten des Ausgangsgeräts können nicht bearbeitet werden.

Beschreibung

Sie können die Zusatzinformationen für jede erstellte Regel für die Gerätekontrolle im Feld **Beschreibung** hinzufügen, beispielsweise, den Namen des angeschlossenen Flash-Laufwerkes oder den Namen seines Inhabers. Der Kommentar wird in der entsprechenden Tabellenspalte im Fenster **Regeln für die Gerätekontrolle** angezeigt.

Der Kommentar und die Daten des Ausgangsgeräts werden bei der Ausführung der Regel nicht berücksichtigt und dienen nur zur Vereinfachung der Kennzeichnung der Geräte und Regeln für den Benutzer.

Über die Erstellung von Regeln für die Gerätekontrolle

Sie können Listen von Erlaubnisregeln zur Gerätekontrolle aus einer XML-Datei importieren, die im Zuge Ausführung der Aufgabe zur Gerätekontrolle oder der Aufgabe Erstellen von Regeln für die Gerätekontrolle automatisch erstellt wird.

Standardmäßig schränkt Kaspersky Embedded Systems Security den Anschluss aller Flash-Laufwerke und anderer externer Geräte ein, die nicht in den Geltungsbereich der festgelegten Regeln für die Gerätekontrolle fallen.

Ziele und Szenarien für die Erstellung von Regeln für die Gerätekontrolle

Szenarium zur Erstellung der Regelliste	Lösungsaufgabe
Aufgabe Erstellen von Regeln für die Gerätekontrolle	• Erlaubnisregeln für bereits verwendete vertrauenswürdige Geräte müssen vor dem ersten Start der Aufgabe zur Gerätekontrolle erstellt werden. • Die Regelliste für die vertrauenswürdigen Geräte muss im Netzwerk des geschützten Geräts erstellt werden.
Erstellen von Regeln aufgrund der Systemdaten	Fügen Sie Erlaubnisregeln für ein oder mehrere externe Geräte hinzu, deren Daten im System gespeichert wurden.
Regelerzeugung basierend auf Daten zu den aktuell verbundenen Geräten	Erneuern Sie eine bereits festgelegte Regelliste, wenn es erforderlich ist, einer kleinen Anzahl von neuen externen Geräten zu vertrauen.
Modus **Nur Statistik** der Aufgabe zur Gerätekontrolle	Erlaubnisregeln für eine große Anzahl von vertrauenswürdigen Geräten müssen erstellt werden.

Verwendung der Aufgabe Erstellen von Regeln für die Gerätekontrolle

Die xml-Datei, die nach Abschluss der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle erstellt wird, enthält die Erlaubnisregeln für Flash-Laufwerke und andere externe Geräte, über deren Anschluss Daten im System gespeichert wurden.

Verwenden Sie diese Methode, wenn Sie möchten, dass beim Erstellen der Erlaubnisregeln die Daten über die jemals angeschlossenen externen Geräte, die in den Systemen aller geschützten Geräte im Netzwerk registriert wurden, berücksichtigt werden, oder wenn Sie möchten, dass nur Daten über Geräte berücksichtigt werden, die momentan an allen geschützten Geräten im Netzwerk angeschlossen sind. Die Aufgabe berücksichtigt auch alle externen Geräte, die während der Ausführung der Gruppenaufgabe angeschlossen wurden. Nach der Ausführung der Gruppenaufgabe erstellt Kaspersky Embedded Systems Security Listen mit Erlaubnisregeln für alle registrierten externen Geräte des Netzwerks und speichert diese Listen in einer xml-Datei im angegebenen allgemeinen Ordner. Im Weiteren können Sie die erstellten Listen mit Regeln manuell in die Einstellungen der Aufgabe "Gerätekontrolle" importieren. Im Gegensatz zur Aufgabe auf einem geschützten Gerät 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 Regeln für die Gerätekontrolle" einrichten.

Es wird empfohlen, dieses Szenario zur Erstellung der Liste mit Erlaubnisregeln vor dem ersten Aufgabenstart die Gerätekontrolle zu verwenden, damit die erstellten Erlaubnisregeln alle externen Geräte berücksichtigen, die auf dem geschützten Gerät verwendet werden.

Verwendung der Systemdaten über alle angeschlossenen Geräte

Im Verlauf der Aufgabenausführung erhält Kaspersky Embedded Systems Security Systemdaten über alle externen Geräte, die früher angeschlossen waren und zum gegenwärtigen Zeitpunkt an das geschützte Gerät angeschlossen sind, und zeigt die gefundenen Geräte im Fenster **Regel auf Grundlage der folgenden Systeminformationen erstellen** in der Liste der gefundenen Geräte an.

Kaspersky Embedded Systems Security bestimmt für jedes gefundene Gerät den Hersteller (VID), den Controller-Typ (PID), den Anzeigenamen, die Seriennummer und den Geräteinstanzpfad. Sie können die Erlaubnisregeln für ein beliebiges externes Gerät erstellen, für das Daten gefunden wurden, und die neuen Regeln sofort zur Liste der festgelegten Regeln zur Gerätekontrolle hinzufügen.

Bei Verwendung dieses Szenarios erstellt Kaspersky Embedded Systems Security Erlaubnisregeln für externe Geräte, die in diesem Moment oder zuvor an das geschützte Gerät angeschlossen wurden, auf dem Kaspersky Security Center installiert ist.

Es wird empfohlen, dieses Szenario für das Update der Regelliste zu verwenden, wenn die Verwendung einer kleinen Anzahl von externen Geräten erlaubt werden soll.

Verwendung von Daten zu den aktuell angeschlossenen Geräten

Bei Verwendung dieses Szenarios erstellt Kaspersky Embedded Systems Security Erlaubnisregeln nur für externe Geräte, die momentan angeschlossen sind. Sie können ein oder mehrere externe Geräte auswählen, für die Sie die Erlaubnisregeln erstellen möchten.

Verwendung der Aufgabe zur Gerätekontrolle im Modus "Nur Statistik"

xml-Datei, die nach Abschluss der Aufgabe zur Gerätekontrolle im Modus **Nur Statistik** auf der Grundlage des Protokolls der Ausgabenausführung erstellt wurde.

Während der Aufgabenausführung protokolliert Kaspersky Embedded Systems Security alle Verbindungen von Flash-Laufwerken und anderen externen Geräten zum geschützten Gerät im Protokoll der Aufgabenausführung. Sie können Erlaubnisregeln anhand von Ereignissen der Aufgabe erstellen und sie in eine XML-Datei exportieren. Vor dem Aufgabenstart im Modus **Nur Statistik** wird empfohlen, den Zeitraum der Aufgabenausführung so anzupassen, dass alle möglichen Verbindungen von externen Geräten mit dem geschützten Gerät im angegebenen Zeitraum ausgeführt wurden.

Es wird empfohlen, dieses Szenario für das Update einer bereits erstellten Regelliste zu verwenden, wenn eine große Anzahl an neuen externen Geräten erlaubt werden soll.

Wenn das Erstellen einer Regelliste nach diesem Szenario auf einem Referenzcomputer ausgeführt wird, können Sie die angelegte Liste mit Erlaubnisregeln für die Einstellungen der Aufgabe "Gerätekontrolle" in Kaspersky Security Center verwenden. Auf diese Weise können Sie die Verwendung von externen Geräten, die einen Referenzcomputer angeschlossen sind, auf allen Geräten des geschützten Netzwerks erlauben.

Über die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle

Mithilfe der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle können Sie automatisch eine Liste der Erlaubnisregeln für den Anschluss von Flash-Laufwerken und anderen externen Geräten auf Basis der Systemdaten der Geräte erstellen, die zuvor an das geschützte Gerät angeschlossen wurden.

Nach Abschluss der Ausführung der Aufgabe erstellt Kaspersky Embedded Systems Security eine Konfigurationsdatei im XML-Format mit der Liste der Erlaubnisregeln für die gefundenen externen Geräte bzw. fügt die erstellten Regeln abhängig von den festgelegten Aufgabeneinstellungen sofort zur Aufgabe zum Erstellen von Regeln für die Gerätekontrolle hinzu. Daraufhin erlaubt das Programm Geräte, für die Erlaubnisregeln automatisch erstellt wurden.

Erzeugte und zur Aufgabe hinzugefügte Regeln werden im Fenster **Regeln für die Gerätekontrolle** angezeigt.

Standardeinstellungen der Aufgabe zur Gerätekontrolle

Die Aufgabe zur Gerätekontrolle weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Standardaufgabeneinstellungen für die Gerätekontrolle

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	**Nur Statistik**	Die Aufgabe speichert das Erlauben und Verbieten des Anschlusses von externen Geräten gemäß den festgelegten Regeln im Protokoll der Aufgabenausführung. Eine tatsächliche Blockierung der Verwendung von externen Geräten findet nicht statt. Sie können zum Schutz des Geräts den Modus **Aktiv** auswählen, damit eine tatsächliche Blockierung der Verwendung von externen Geräten stattfindet.
Die Verwendung aller externen Geräte erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird	Wird nicht verwendet	Kaspersky Embedded Systems Security verbietet die Verwendung von externen Geräten unabhängig vom Ausführungsstatus der Aufgabe zur Gerätekontrolle. Dies gewährleistet die maximale Sicherheit des Computers vor Bedrohungen, die beim Dateiaustausch mit externen Geräten entstehen. Sie können die Einstellung so anpassen, dass Kaspersky Embedded Systems Security die Verwendung aller externen Geräte erlaubt, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Gerätekontrolle wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können den Zeitplan für den Aufgabenstart konfigurieren.

Standardeinstellungen der Aufgabe Erstellen von Regeln für die Gerätekontrolle

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	**Systemdaten zu allen externen Geräten berücksichtigen, die jemals angeschlossen waren**	Der Ausführungsmodus der Aufgabe. Sie können den Aufgabenmodus **Nur momentan angeschlossene externe Geräte berücksichtigen** auswählen.
Aktionen nach Abschluss der Aufgabe	Die Erlaubnisregeln werden der Liste der Regeln zur Gerätekontrolle hinzugefügt; die neuen Regeln werden mit den bestehenden Regeln	Sie können die Regeln den bereits existierenden Regeln hinzufügen, ohne dabei doppelte Regeln zusammenzuführen oder zu löschen oder bestehende Regeln durch neue Erlaubnisregeln zu

	zusammengeführt; doppelte Regeln werden gelöscht.	ersetzen, sowie die Einstellungen für den Export der Erlaubnisregeln in eine Datei konfigurieren.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle wird nicht automatisch beim Hochfahren von Kaspersky Embedded Systems Security ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Gerätekontrolle über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie durch die Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Verbindungen von beliebigen externen Geräten mit allen Servern im Netzwerk verwalten, indem Sie Regellisten für die Gruppen von geschützten Geräten über das Kaspersky Security Center erstellen.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Richtlinieneinstellungen für die Aufgabe zur Gerätekontrolle öffnen

Um die Aufgabeneinstellungen für die Gerätekontrolle über die Richtlinie von Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Überwachung der Desktop-Aktivitäten**.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Gerätekontrolle**.

   Das Fenster **Gerätekontrolle** wird geöffnet.
7. Konfigurieren Sie die Richtlinie nach Bedarf.

Regelliste für die Gerätekontrolle öffnen

Um die Regelliste für die Gerätekontrolle über das Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Überwachung der Desktop-Aktivitäten**.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Gerätekontrolle**.

   Das Fenster **Gerätekontrolle** wird geöffnet.
7. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.
8. Konfigurieren Sie die Richtlinie nach Bedarf.

Assistent und Eigenschaften für die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle öffnen

Um die Erstellung einer Aufgabe zum Erstellen von Regeln für die Gerätekontrolle auszulösen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.
5. Wählen Sie die Aufgabe **Erstellen von Regeln für die Gerätekontrolle** aus.
6. Klicken Sie auf **Weiter**.

   Das Fenster **Einstellungen** wird geöffnet.

Um die bestehende Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Aufgaben** aus.
4. Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben von Kaspersky Security Center.

Das Fenster **Eigenschaften: Erstellen von Regeln für die Gerätekontrolle** wird geöffnet.

Details darüber, wie Sie die Aufgabe konfigurieren, finden Sie im Abschnitt Aufgabe zum Erstellen von Regeln für die Gerätekontrolle konfigurieren.

Aufgabe zur Gerätekontrolle konfigurieren

Um die Einstellungen der Aufgabe zur Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Gerätekontrolle**.
2. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:
   - Wählen Sie im Abschnitt **Aufgabenmodus** einen Aufgabenmodus aus:
     - **Aktiv**.

       Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, vor dem Start der Aufgabe zur Gerätekontrolle im Modus "Aktiv" an das geschützte Gerät angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder das geschützte Gerät neu zu starten. Anderenfalls wird das "Prinzip des standardmäßigen Verbots" für das Gerät nicht übernommen.

     - **Nur Statistik**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Die Verwendung aller externen Geräte erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird**.
3. Klicken Sie auf die Schaltfläche der Liste **Regelliste**, um die Liste der Regeln für die Gerätekontrolle zu bearbeiten.
4. Passen Sie bei Bedarf die Einstellungen des Zeitplans für den Aufgabenstart auf der Registerkarte **Aufgabenverwaltung** an.
5. Klicken Sie im Fenster **Gerätekontrolle** auf OK.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Aufgabe zum Erstellen von Regeln für die Gerätekontrolle konfigurieren

Um die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Erstellen von Regeln für die Gerätekontrolle**.
2. Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.

Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

3. Im Abschnitt **Einstellungen** können Sie die folgenden Einstellungen konfigurieren:

   - Wählen Sie den Betriebsmodus aus: Berücksichtigen Sie Systemdaten über alle jemals angeschlossenen externen Geräte oder berücksichtigen Sie nur derzeit angeschlossene externe Geräte.
   - Passen Sie die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln an, die von Kaspersky Embedded Systems Security nach Abschluss der Aufgaben erstellt werden.

4. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).

5. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten die Aufgabe ausgeführt wird.

6. Geben Sie bei Bedarf im Abschnitt **Ausnahmen vom Gültigkeitsbereich** der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

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

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Regeln für die Gerätekontrolle über das Kaspersky Security Center konfigurieren

Erfahren Sie, wie Sie auf der Grundlage von verschiedenen Kriterien eine Liste von Regeln erzeugen oder mithilfe der Aufgabe zur Gerätekontrolle manuell Erlaubnis- oder Verbotsregeln erstellen können.

Erlaubnisregeln auf Grundlage von Systemdaten des Systems in einer Richtlinie von Kaspersky Security Center erstellen

*Um die Erlaubnisregeln mithilfe der Option **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Aufgabe "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Schließen Sie an das geschützte Gerät mit der installierten Verwaltungskonsole von Kaspersky Security Center erforderlichenfalls ein neues externes Gerät an, das Sie vertrauenswürdig machen möchten.

2. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.

3. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regel auf Grundlage der folgenden Systemdaten erstellen**.

4. Wählen Sie ein Gerät in der Liste der Geräte im Fenster **Regel auf Grundlage der folgenden Systeminformationen erstellen** aus.

5. Klicken Sie auf **Regel für ausgewählte Geräte hinzufügen**.

6. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Gerätekontrolle**.

Die Liste der Regeln in der Aufgabe Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des geschützten Geräts mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Regeln für angeschlossene Geräte erstellen

*Um die Erlaubnisregeln mithilfe der Option **Regeln für momentan angeschlossene Geräte berücksichtigen** in den Einstellungen der Aufgabe "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.

2. 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 Systeminformationen erstellen** wird geöffnet.

3. Wählen Sie in der Liste der gefundenen Geräte, die an das geschützte Gerät angeschlossen sind, die Geräte aus, für die Sie Erlaubnisregeln erstellen möchten.

4. Klicken Sie auf die Schaltfläche **Regel für ausgewählte Geräte hinzufügen**.

5. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Gerätekontrolle**.

Die Liste der Regeln in der Aufgabe Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des geschützten Geräts mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Regeln aus dem Bericht von Kaspersky Security Center über blockierte Geräte importieren

Sie können Daten über blockierte Geräteverbindungen aus dem Bericht importieren, der in Kaspersky Security Center nach der Ausführung der Aufgabe zur Gerätekontrolle im Modus **Nur Statistik** erstellt wurde, und diese Daten für die Erstellung einer Liste von Erlaubnisregeln für die Gerätekontrolle in der konfigurierten Richtlinie verwenden.

Bei der Berichterstellung über Ereignisse, die während der Ausführung der Aufgabe zur Gerätekontrolle eintreten, können Sie verfolgen, für welche Programme die Verbindung blockiert wird.

Gehen Sie wie folgt vor, um auf Grundlage eines Berichts aus Kaspersky Security Center über blockierten Geräte Erlaubnisregeln für Geräteverbindungen für eine Gruppe von geschützten Geräten festzulegen:

1. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisbenachrichtigungen**, dass:

   - Für die Prioritätsstufe **Kritische Ereignisse** die Zeitspanne zum Speichern des Protokolls der Aufgabenausführung für das Ereignis *Nicht vertrauenswürdiges externes Gerät erkannt und eingeschränkt* die geplante Betriebsdauer im Modus **Nur Statistik** übersteigt (der Standardwert beträgt 30 Tage).

- Für die Prioritätsstufe **Warnung** die Zeitspanne zum Speichern des Protokolls der Aufgabenausführung für das Ereignis *Nur Statistik: nicht vertrauenswürdiges externes Gerät erkannt* die geplante Betriebsdauer der Aufgabe im Modus **Nur Statistik** übersteigt (der Standardwert beträgt 30 Tage).

  Nach Ablauf der Zeitspanne für das Speichern von Ereignissen werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in die Protokolldatei aufgenommen. Vergewissern Sie sich vor dem Start der Aufgabe "Gerätekontrolle" im Modus **Nur Statistik**, dass die Ausführungsdauer der Aufgabe die eingestellte Speicherzeit für die angegebenen Ereignisse nicht überschreitet.

2. Starten Sie die Aufgabe zur Gerätekontrolle im Modus **Nur Statistik**.

   a. Wählen Sie im Arbeitsbereich des Knotens **Administrationsserver** in Kaspersky Security Center die Registerkarte **Ereignisse** aus.

   b. Klicken Sie auf die Schaltfläche **Auswahl erstellen** und erstellen Sie eine Auswahl von Ereignissen auf der Grundlage des Kriteriums *Nicht vertrauenswürdiges externes Gerät erkannt und eingeschränkt*, um die Geräte anzuzeigen, deren Verbindungen durch die Aufgabe zur Gerätekontrolle eingeschränkt werden.

   c. Klicken Sie im Ergebnisfenster der Auswahl auf den Link **Ereignisse in Datei exportieren**, um den Bericht über eingeschränkte Verbindungen in einer TXT-Datei zu speichern.

Vergewissern Sie sich vor dem Import und der Verwendung des erstellten Berichts in der Richtlinie, dass der Bericht nur Daten derjenigen Geräte enthält, deren Verbindung Sie erlauben möchten.

3. Importieren Sie die Daten über die Verbindungen eingeschränkter Geräte in die Aufgabe "Gerätekontrolle":

   a. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regeln aus Datei des Kaspersky Security Center-Berichts über blockierte Geräte importieren**.

   c. Wählen Sie das Prinzip aus, nach dem die Regeln aus der auf Grundlage des Berichts von Kaspersky Security Center erstellten Liste zur Liste der bereits bestehenden Regeln zur Gerätekontrolle hinzugefügt werden.

      - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
      - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
      - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   d. Wählen Sie im erscheinenden Windows-Standardfenster die TXT-Datei aus, in welche die Ereignisse aus dem Bericht über die blockierten Geräte exportiert wurden.

   e. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Gerätekontrolle**.

4. Klicken Sie im Fenster **Gerätekontrolle** auf **OK**.

Die auf Grundlage des Berichts von Kaspersky Security Center über die blockierten Geräte erstellten Regeln werden der Liste der Regeln in der Richtlinie zur Gerätekontrolle hinzugefügt.

Regeln mithilfe der Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen

Um Erlaubnisregeln für die Gerätekontrolle für eine Gruppe von geschützten Geräten mithilfe der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle festzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Einstellungen** im Assistenten für neue Aufgaben.
2. Passen Sie Folgendes an:
   - Im Abschnitt **Modus**:
     - **Systemdaten zu allen externen Geräten berücksichtigen, die jemals angeschlossen waren**.
     - **Nur momentan angeschlossene externe Geräte berücksichtigen**.
   - Im Abschnitt **Nach Abschluss der Aufgabe**:
     - **Erlaubnisregeln in die Liste der Regeln für die Gerätekontrolle aufnehmen**.
     - **Prinzip für das Hinzufügen**.
     - **Erlaubnisregeln in Datei exportieren**.
     - **Informationen über das geschützte Gerät zum Dateinamen hinzufügen**.
3. Klicken Sie auf Weiter.
4. Legen Sie im Fenster **Zeitplan** die Einstellungen für den Zeitplan für den Aufgabenstart fest.
5. Klicken Sie auf Weiter.
6. Legen Sie im Fenster Konto für das Ausführen der Aufgabe auswählen das Konto fest, das Sie verwenden möchten.
7. Klicken Sie auf Weiter.
8. Geben Sie einen Aufgabennamen an.
9. Klicken Sie auf Weiter.

   Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

   Das Fenster Erstellung der Aufgabe fertig stellen wird geöffnet.
10. Sie können die Aufgabe optional ausführen, nachdem der Assistent abgeschlossen wurde, indem Sie das Kontrollkästchen Aufgabe nach Abschluss des Assistenten starten aktivieren.
11. Klicken Sie auf Fertig stellen, um die Erstellung der Aufgabe abzuschließen.

12. Wählen Sie auf der Registerkarte Aufgaben im Arbeitsbereich der konfigurierten Gruppe von geschützten Geräten in der Liste der Gruppenaufgaben die erstellte Aufgabe zum Erstellen von Regeln für die Gerätekontrolle aus.

13. Klicken Sie auf die Schaltfläche Starten, um die Aufgabe zu starten.

    Nach Abschluss der Aufgabe werden die automatisch erstellten Listen mit Erlaubnisregeln in Form von XML-Dateien in einem freigegebenen Ordner gespeichert.

> Stellen Sie bei der Übernahme der Richtlinie für Gerätekontrolle im Netzwerk sicher, dass für alle geschützten Geräte 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 "Erstellen von Regeln für die Gerätekontrolle" der Gerätekontrolle auf einer Gruppe von geschützten Testgeräten oder einem Referenzcomputer zu starten.

Erzeugte Regeln in die Regelliste für die Gerätekontrolle aufnehmen

Um die erzeugten Listen mit Erlaubnisregeln zur Aufgabe zur Gerätekontrolle hinzuzufügen, gehen Sie wie folgt vor.

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** die Option **Regeln aus XML-Datei importieren** aus.

4. Wählen Sie das Prinzip aus, nach dem automatisch erstellte Erlaubnisregeln der Liste der bereits festgelegten Regeln zur Gerätekontrolle hinzugefügt werden sollen.

   - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.

   - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.

   - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

5. Wählen Sie im erscheinenden Standardfenster von Windows die XML-Dateien aus, die nach Abschluss der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellt wurden.

6. Klicken Sie auf Öffnen.

   Alle erzeugten Regeln aus der XML-Datei werden entsprechend dem ausgewählten Prinzip zur Liste hinzugefügt.

7. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Gerätekontrolle**.

8. Wenn Sie die erstellten Regeln für die Gerätekontrolle verwenden möchten, wählen Sie in den Eigenschaften der Richtlinie zur **Gerätekontrolle** den Aufgabenmodus **Aktiv**.

Automatisch auf Grundlage der Systemdaten auf jedem einzelnen geschützten Gerät erstellte Erlaubnisregeln werden für alle geschützten Geräte im Netzwerk, auf denen die konfigurierte Richtlinie übernommen wird, übernommen. Für diese geschützten Geräte erlaubt das Programm nur die Verbindung von Geräten, für die Erlaubnisregeln erstellt wurden.

Gerätekontrolle über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem geschützten Gerät konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Einstellungen der Aufgabe zur Gerätekontrolle öffnen

Um die Einstellungen der Aufgabe zur Gerätekontrolle über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Gerätekontrolle** aus.
3. Klicken Sie im Detailbereich des untergeordneten Knotens **Gerätekontrolle** auf den Link **Eigenschaften**.
   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Konfigurieren Sie die Aufgabe nach Bedarf.

Fenster "Regeln für die Gerätekontrolle" öffnen

Um die Regelliste für die Gerätekontrolle über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Gerätekontrolle** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Gerätekontrolle** auf den Link **Regeln für die Gerätekontrolle**.
   Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.
4. Konfigurieren Sie die Regelliste nach Bedarf.

Einstellungen für das Erstellen von Regeln für die Gerätekontrolle öffnen

Um die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Automatisches Erstellen von Regeln**.
2. Wählen Sie den untergeordneten Knoten **Erstellen von Regeln für die Gerätekontrolle**.
3. Klicken Sie im Ergebnisbereich des untergeordneten Knotens **Erstellen von Regeln für die Gerätekontrolle** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Konfigurieren Sie die Aufgabe nach Bedarf.

Einstellungen der Aufgabe Gerätekontrolle anpassen

Um die Einstellungen der Aufgabe zur Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Aufgabeneinstellungen**.
2. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:
   - Wählen Sie im Abschnitt **Aufgabenmodus** einen Aufgabenmodus aus:
     - Aktiv.

       Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, vor dem Start der Aufgabe zur Gerätekontrolle im Modus "Aktiv" an das geschützte Gerät angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder das geschützte Gerät neu zu starten. Anderenfalls wird das "Prinzip des standardmäßigen Verbots" für das Gerät nicht übernommen.
     - **Nur Statistik**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Die Verwendung aller externen Geräte erlauben, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird**.
3. Passen Sie erforderlichenfalls auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an.
4. Um die Regelliste für die Gerätekontrolle zu bearbeiten, klicken Sie auf den Link **Regeln für die Gerätekontrolle** im unteren Teil des Ergebnisfensters des Knotens **Gerätekontrolle**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Regeln für die Gerätekontrolle konfigurieren

Erfahren Sie, wie Sie eine Liste von Regeln erzeugen, importieren und exportieren oder mithilfe der Aufgabe zur Gerätekontrolle manuell Erlaubnis- oder Verbotsregeln erstellen können.

Regeln für die Gerätekontrolle aus einer XML-Datei importieren

So importieren Sie Regeln für die Gerätekontrolle:

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regeln aus XML-Datei importieren** aus.
4. Geben Sie an, auf welche Weise die zu importierenden Regeln hinzugefügt werden sollen. Wählen Sie hierzu einen der Punkte des Kontextmenüs der Schaltfläche **Regeln aus XML-Datei importieren** aus:

   - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
   - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
   - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.
5. Wählen Sie im Fenster **Öffnen** die XML-Datei aus, in der die Einstellungen der Regeln für die Gerätekontrolle enthalten sind.
6. Klicken Sie auf **Öffnen**.

Die importierten Regeln erscheinen in der Liste im Fenster **Regeln für die Gerätekontrolle**.

Liste der Regeln nach den Ereignissen der Aufgabe Gerätekontrolle erstellen

Um die Konfigurationsdatei mit der Liste der Regeln zur Gerätekontrolle, die anhand von Ereignissen der Aufgabe Gerätekontrolle erstellt wurde, zu erstellen, gehen Sie wie folgt vor:

1. Führen Sie die Aufgabe zur Gerätekontrolle im Modus **Nur Statistik** aus, um alle Ereignisse zu protokollieren, die beim Anschluss von Flash-Laufwerken und anderen externen Geräten an einem geschützten Gerät auftreten.
2. Nach Abschluss der Aufgabe im Modus **Nur Statistik** öffnen Sie den Bericht über Aufgabenausführung über die Schaltfläche **Protokoll der Aufgabenausführung öffnen** im Abschnitt **Verwaltung** im Ergebnisbereich des Knotens **Gerätekontrolle**.
3. Klicken Sie im Fenster **Protokolle** auf die Schaltfläche **Regeln anhand von Ereignissen erstellen**.

Kaspersky Embedded Systems Security erstellt die Konfigurationsdatei im xml-Format mit der Liste der Regeln, die anhand der Ereignisse der Ausführung der Aufgabe zur Gerätekontrolle im Modus **Nur Statistik** erstellt wurden. Sie können diese Liste in der Aufgabe zur Gerätekontrolle übernehmen.

Vor der Anwendung der Regelliste, die anhand von Ereignissen der Aufgabe erstellt wurde, wird empfohlen, die Liste der Regeln anzuzeigen und manuell zu bearbeiten, um sicherzustellen, dass die Verbindung von nicht vertrauenswürdigen Geräten nicht durch die festgelegten Regeln erlaubt ist.

Beim Konvertieren der XML-Datei mit den Ereignissen der Aufgabenausführung in die Liste der Regeln zur Gerätekontrolle erstellt das Programm Erlaubnisregeln für alle gespeicherten Ereignisse, darunter auch für Ereignisse der Gerätesperre.

In beiden Modi werden alle Ereignisse der Aufgabenausführung im Protokoll der Aufgabenausführung registriert. Sie können eine Konfigurationsdatei mit der Regelliste anhand von Ereignissen der Aufgabe im Modus **Aktiv** erstellen. Dieses Szenario wird nicht empfohlen, mit Ausnahme von dringlichen Fällen, da für die effektive Ausführung der Aufgabe die Erstellung von Listen bis zum Start der Aufgabe im aktiven Modus erforderlich ist.

Erlaubnisregel für ein oder mehrere externe Geräte hinzufügen

In der Aufgabe zur Gerätekontrolle ist die Funktion des manuellen Hinzufügens einer Regel nicht vorgesehen. Falls Sie jedoch Erlaubnisregeln für einen oder mehrere neue externe Geräte hinzufügen müssen, können Sie die Option **Regel auf Grundlage der folgenden Systemdaten erstellen** verwenden. Bei Verwendung dieses Szenarios zur Ergänzung der Regelliste verwendet das Programm die Windows-Daten über alle angeschlossenen externen Geräte, die jemals im System registriert wurden, und berücksichtigt die externen Geräte, die momentan angeschlossen sind.

Um eine Erlaubnisregel für ein oder mehrere externe Geräte, die zum aktuellen Zeitpunkt angeschlossen sind, hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie im Kontextmenü den Punkt **Regel auf Grundlage der folgenden Systemdaten erstellen**.
4. Wählen Sie im folgenden Fenster in der Liste der gefundenen Geräte ein Gerät oder mehrere Geräte aus, deren Verwendung auf dem geschützten Gerät erlaubt werden soll.
5. Klicken Sie auf die Schaltfläche **Regel für ausgewählte Geräte hinzufügen**.

Die neuen Regeln werden zur Liste der Regeln zur Gerätekontrolle hinzugefügt.

Regeln der Gerätekontrolle löschen

Um Regeln für die Gerätekontrolle zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.
2. Wählen Sie in der Liste der Regeln eine oder mehrere Regeln aus, die Sie entfernen möchten.
3. Klicken Sie auf die Schaltfläche **Auswahl entfernen**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die ausgewählten Regeln zur Gerätekontrolle werden gelöscht.

Regeln der Gerätekontrolle exportieren

Um Regeln für die Gerätekontrolle in eine Konfigurationsdatei zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.
2. Klicken Sie auf **In Datei exportieren**.

   Das Microsoft-Windows-Standardfenster wird geöffnet.
3. Geben Sie im erscheinenden Fenster die Datei an, in die Sie die Regeln exportieren möchten. Existiert die angegebene Datei nicht, so wird sie erstellt. Existiert bereits eine Datei mit dem angegebenen Namen, so wird ihr Inhalt nach Abschluss des Exports der Regeln überschrieben.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Regeln und ihre Einstellungen werden in die angegebene Datei exportiert.

Regeln zur Gerätekontrolle aktivieren und deaktivieren

Sie können die Anwendung der erstellten Erlaubnisregeln zur Gerätekontrolle aktivieren und deaktivieren, ohne sie zu löschen.

So aktivieren oder deaktivieren Sie eine erstellte Regel für die Gerätekontrolle:

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.
2. Öffnen Sie in der Liste der angegebenen Regeln das Fenster **Eigenschaften der Regel**, indem Sie mit der rechten Maustaste auf die Regel doppelklicken, deren Einstellungen Sie anpassen wollen.
3. Deaktivieren oder aktivieren Sie im folgenden Fenster das Kontrollkästchen **Regel übernehmen**.
4. Klicken Sie auf **OK**.

Der Status der Anwendung der Regel wird gespeichert und für die angegebene Regel angezeigt.

Gültigkeitsbereich der Regeln zur Gerätekontrolle erweitern

Jede automatisch erstellte Regel für die Gerätekontrolle erlaubt die Verbindung nur eines externen Geräts. Sie können den Gültigkeitsbereich der Regel manuell erweitern, indem Sie die Maske des Pfads der Geräteexemplarklasse in den Eigenschaften einer beliebigen festgelegten Regel für die Gerätekontrolle anwenden.

Die Anwendung der Maske des Pfads der Geräteexemplarklasse verringert die Anzahl der Erlaubnisregeln der Gerätekontrolle und vereinfacht den Prozess ihrer manuellen Verarbeitung. Die Erweiterung des Gültigkeitsbereichs der Regeln kann jedoch die Effektivität der Kontrolle von externen Geräten verringern.

Um eine Maske des Geräteinstanzpfads in den Eigenschaften der Erlaubnisregel für die Gerätekontrolle zu übernehmen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Regeln für die Gerätekontrolle**.

2. Wählen Sie im folgenden Fenster eine Regel aus, deren Eigenschaften Sie für die Maske des Programms verwenden möchten.

3. Öffnen Sie das Fenster **Eigenschaften der Regel** mit einem Doppelklick auf der ausgewählten Regel für die Gerätekontrolle.

4. Im nächsten Fenster gehen Sie wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Maske verwenden** neben dem Feld **Controller-Typ (PID)**, wenn Sie möchten, dass eine ausgewählte Regel die Verbindung aller externen Geräte nach den festgelegten Daten über den Hersteller und den Controller-Typ des Geräts erlaubt.

   - Aktivieren Sie das Kontrollkästchen **Maske verwenden** neben dem Feld **Seriennummer**, wenn Sie möchten, dass eine ausgewählte Regel die Verbindung aller externen Geräte nach den festgelegten Daten über den Hersteller und die Seriennummer des Geräts erlaubt.

   - Aktivieren Sie die Kontrollkästchen **Maske verwenden** neben den Feldern **Controller-Typ (PID)** und **Seriennummer**, wenn Sie möchten, dass eine ausgewählte Regel die Verbindung aller externen Geräte nach den festgelegten Daten über den Hersteller sowohl Controller-Typ als auch Seriennummer des Geräts erlaubt.

   Wenn in mindestens einem Feld das Kontrollkästchen **Maske verwenden** aktiviert ist, werden die Informationen in den Feldern, in denen dieses Kontrollkästchen aktiviert ist, durch das Zeichen * ersetzt und beim Auslösen der Regel nicht berücksichtigt.

5. Geben Sie im Feld **Beschreibung** bei Bedarf zusätzlich erläuternde Informationen zur Regel an. Geben Sie z. B. an, für welche Geräte die Regel gelten soll.

6. Klicken Sie auf **OK**.

Die vorgenommenen Regel-Einstellungen werden gespeichert. Der Gültigkeitsbereich der Regel wird entsprechend der angegebenen Maske des Pfads der Geräteexemplarklasse erweitert.

Aufgabe "Erstellen von Regeln für die Gerätekontrolle"

Um die Aufgabe zum Erstellen von Regeln für die Gerätekontrolle zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Automatisches Erstellen von Regeln**.

2. Wählen Sie den untergeordneten Knoten **Erstellen von Regeln für die Gerätekontrolle**.

3. Klicken Sie im Ergebnisbereich des Knotens **Erstellen von Regeln für die Gerätekontrolle** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

4. Wählen Sie auf der Registerkarte **Allgemein** im Abschnitt **Aufgabenmodus** den Modus der Aufgabenausführung aus:

   - **Systemdaten zu allen externen Geräten berücksichtigen, die jemals angeschlossen waren**.

   - **Nur momentan angeschlossene externe Geräte berücksichtigen**.

5. Geben Sie im Abschnitt **Nach Abschluss der Aufgabe** die Aktionen an, die Kaspersky Embedded Systems Security beim Abschluss der Aufgabe ausführen soll:

- Erlaubnisregeln in die Liste der Regeln für die Gerätekontrolle aufnehmen.
- Prinzip für das Hinzufügen.
- Erlaubnisregeln in Datei exportieren.
- Informationen über das geschützte Gerät zum Dateinamen hinzufügen.

6. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** die Einstellungen für den Zeitplan für den Aufgabenstart an.
7. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben zu Datum und Uhrzeit der Änderung der Einstellungen sowie die Werte der Aufgabeneinstellungen vor und nach der Änderung werden im Systemaudit-Protokoll gespeichert.

Gerätekontrolle über das Web-Plug-in der Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Web-Plug-ins navigieren und Aufgabeneinstellungen auf einem geschützten Gerät konfigurieren.

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Überwachung der Desktop-Aktivitäten** aus.
5. Klicken Sie im Unterabschnitt **Gerätekontrolle** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen der Aufgaben für die Gerätekontrolle

Einstellung	Beschreibung
Aktiv	Kaspersky Embedded Systems Security kontrolliert mithilfe der Regeln den Anschluss von Wechseldatenträgern 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.
Nur Statistik	Kaspersky Embedded Systems Security kontrolliert das Anschließen von Wechseldatenträgern und anderen externen Geräten nicht, sondern speichert lediglich die Informationen zu Anschluss und Registrierung von externen Geräten auf dem geschützten Gerät sowie zu den Erlaubnisregeln zur Gerätekontrolle, denen die angeschlossenen Geräte unterliegen, im Protokoll der Aufgabenausführung. Die Verwendung aller externen Geräte wird erlaubt. Dieser Modus ist standardmäßig eingestellt.
Die Verwendung aller externen Geräte erlauben, wenn die Aufgabe	Das Kontrollkästchen erlaubt oder verbietet die Verwendung von externen Geräten, wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird.

zur Gerätekontrolle nicht ausgeführt wird	Wenn das Kontrollkästchen aktiviert ist und die Aufgabe zur Gerätekontrolle nicht ausgeführt wird, erlaubt Kaspersky Embedded Systems Security die Verwendung beliebiger externer Geräte auf dem geschützten Gerät. Wenn das Kontrollkästchen deaktiviert ist, verbietet das Programm die Verwendung von nicht vertrauenswürdigen externen Geräten auf dem geschützten Gerät in den folgenden Fällen: wenn die Aufgabe zur Gerätekontrolle nicht ausgeführt wird oder wenn Kaspersky Security Service angehalten ist. Es wird empfohlen, zur Gewährleistung maximaler Sicherheit des Computers vor Bedrohungen, die beim Dateiaustausch mit den externen Geräten entstehen, diese Variante zu verwenden. Das Kontrollkästchen ist standardmäßig deaktiviert.
Regeln für die Gerätekontrolle	Sie können die Liste der Regeln für die Gerätekontrolle ändern.
Aufgabenverwaltung	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Firewall-Verwaltung

Dieser Abschnitt informiert über die Aufgabe zur Firewall-Verwaltung und erläutert die Konfiguration dieser Aufgabe.

Über die Aufgabe zur Firewall-Verwaltung

Kaspersky Embedded Systems Security stellt eine sichere und bequeme Lösung für den Schutz von Netzwerkverbindungen mithilfe der Aufgabe zur Firewall-Verwaltung zur Verfügung.

Die Aufgabe zur Firewall-Verwaltung führt keine selbstständige Filterung des Datenverkehrs durch, sondern ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Embedded Systems Security zu verwalten. Während der Ausführung der Aufgabe zur Firewall-Verwaltung übernimmt Kaspersky Embedded Systems Security die vollständige Verwaltung der Einstellungen und Regeln der Firewall des Betriebssystems und blockiert jeden Versuch, die Firewall-Einstellungen auf andere Weise anzupassen.

Bei der Programminstallation liest und kopiert die Komponente Firewall-Verwaltung den Status der Windows-Firewall sowie alle festgelegten Regeln. Von diesem Zeitpunkt an kann die Änderung der Regelsätze und Einstellungen sowie das Anhalten oder der Start der Firewall nur über Kaspersky Embedded Systems Security vorgenommen werden.

Wenn die Windows-Firewall bei der Installation von Kaspersky Embedded Systems Security deaktiviert ist, wird die Aufgabe zur Firewall-Verwaltung nach Abschluss der Installation nicht ausgeführt. Wenn die Windows-Firewall bei der Programminstallation aktiviert ist, wird die Aufgabe zur Firewall-Verwaltung nach Abschluss der Installation ausgeführt und blockiert alle Netzwerkverbindungen, die nicht von den festgelegten Regeln erlaubt sind.

Die Komponente Firewall-Verwaltung gehört nicht zu den Komponenten der empfohlenen Installation und wird nicht standardmäßig installiert.

Die Aufgabe zur Firewall-Verwaltung erzwingt das Blockieren aller eingehenden und ausgehenden Verbindungen, wenn sie nicht von den festgelegten Regeln der Aufgabe erlaubt sind.

Die Aufgabe fragt regelmäßig die Windows-Firewall ab und überprüft ihren Zustand. Standardmäßig beträgt das Abfrageintervall 1 Minute und kann nicht geändert werden. Wenn Kaspersky Embedded Systems Security 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.

Kaspersky Embedded Systems Security prüft durch die minutenweise Abfrage der Windows-Firewall Folgendes:

- Status der Funktion der Windows-Firewall.
- Status der Regeln, die nach der Installation von Kaspersky Embedded Systems Security hinzugefügt wurden (z. B. Hinzufügen einer neuen Regel des Programms für einen Port oder eine App mithilfe von wf.msc).

Wenn Sie neue Regeln auf die Windows-Firewall anwenden, erstellt Kaspersky Security für Windows Server einen Regelsatz unter der Gruppe "Kaspersky Security" im Snap-in der Windows-Firewall. Dieser Regelsatz enthält alle Regeln, die von Kaspersky Security für Windows Server mithilfe der Aufgabe zur Firewall-Verwaltung erstellt wurden. Die Regeln, die zur Gruppe Kaspersky Security Group gehören, werden vom Programm bei der Abfrage nicht überprüft und nicht automatisch mit der Liste der Regeln synchronisiert, die in den Einstellungen der Aufgabe zur Firewall-Verwaltung festgelegt wurden. Bei Bedarf können Sie das Update der Regeln von Kaspersky Security Group manuell vornehmen.

Um die Regelliste von Kaspersky Security Group manuell zu aktualisieren,

starten Sie die Aufgabe zur Firewall-Verwaltung in Kaspersky Embedded Systems Security neu.

Außerdem können Sie die Regeln von Kaspersky Security Group manuell über das Snap-In Windows Firewall anpassen.

Der Start der Aufgabe zur Firewall-Verwaltung ist nicht möglich, wenn die Windows-Firewall von einer 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 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 diese Regel.
- Wenn in den Einstellungen der Windows-Firewall eine bereits vorhandene Regel gelöscht wird, stellt Kaspersky Embedded Systems Security diese Regel bei einem Neustart der Aufgabe wieder her.
- Wenn in den Einstellungen der Windows-Firewall die Einstellungen einer vorhandenen Regel geändert werden, verwirft Kaspersky Embedded Systems Security die Änderungen.
- Wenn in den Einstellungen der Aufgabe zur Firewall-Verwaltung eine neue Regel erstellt wird, erzwingt Kaspersky Embedded Systems Security die Übernahme dieser Regel durch die Windows-Firewall.
- Wenn in den Einstellungen der Aufgabe zur Firewall-Verwaltung eine bereits vorhandene Regel gelöscht wird, erzwingt Kaspersky Embedded Systems Security das Löschen dieser Regel aus den Einstellungen der Windows-Firewall.

Kaspersky Embedded Systems Security funktioniert nicht mit Verbotsregeln sowie mit Regeln, die den ausgehenden Datenverkehr kontrollieren. Zum Zeitpunkt des Starts der Aufgabe zur Firewall-Verwaltung löscht Kaspersky Embedded Systems Security alle Regeln dieser Art aus den Einstellungen der Windows-Firewall.

Zur Filterung des eingehenden Datenverkehrs können Sie Regeln festlegen, löschen und bearbeiten.

Für die Kontrolle des ausgehenden Datenverkehrs können Sie keine neue Regel in den Einstellungen der Aufgabe zur Firewall-Verwaltung festlegen. Alle Firewall-Regeln, die über Kaspersky Embedded Systems Security festgelegt werden, kontrollieren nur den eingehenden Datenverkehr.

Sie können verschiedene Arten von Firewall-Regeln verwalten: für Anwendungen und für Ports.

Programmregeln

Regeln dieser Art erlauben Netzwerkverbindungen für ausgewählte angegebene Apps. Ein Auslösekriterium für solche Regeln ist der Pfad zur ausführbaren Datei.

Sie können die Programmregeln 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

Portregeln

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 Portregeln 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 Portregeln erlauben, reduzieren Sie die Sicherheitsstufe des geschützten Geräts.

Standardeinstellungen der Aufgabe zur Firewall-Verwaltung

Die Aufgabe zur Firewall-Verwaltung weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Standardeinstellungen der Aufgabe zur Firewall-Verwaltung

Einstellung	Standardwert	Beschreibung

Firewall-Regeln für das Programm	Zwei Standardregeln für das Programm aktiviert	Sie können die Standardregeln deaktivieren oder neue Regeln hinzufügen.
Firewall-Regeln für Ports	Sechs Standardregeln für Ports aktiviert	Sie können die Standardregeln deaktivieren oder neue Regeln hinzufügen.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Firewall-Verwaltung wird beim Start von Kaspersky Embedded Systems Security nicht automatisch ausgeführt. Sie können den Zeitplan für den Aufgabenstart konfigurieren.

Firewall-Regeln über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie Firewall-Regeln über die Benutzeroberfläche des Verwaltungs-Plug-ins verwalten.

Firewall-Regeln aktivieren und deaktivieren

Um eine bereits vorhandene Regel zur Filterung des eingehenden Datenverkehrs zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Firewall-Verwaltung**.
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
6. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
7. Suchen Sie in der Liste der Regeln die Regel aus, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

- Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

  Die ausgewählte Regel wird aktiviert.

- Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

  Die ausgewählte Regel wird deaktiviert.

8. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **OK**.

9. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.

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

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln manuell hinzufügen

Sie können nur Regeln für Apps und Ports hinzufügen und bearbeiten. Sie können für Gruppen keine neuen Regeln hinzufügen oder bereits vorhandene Regeln bearbeiten.

So fügen Sie eine neue Regel zur Filterung des eingehenden Datenverkehrs hinzu oder ändern eine bereits vorhandene Regel:

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

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

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Firewall-Verwaltung**.

5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Firewall-Regeln** wird geöffnet.

6. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus – je nachdem, welche Art der Regel Sie hinzufügen möchten – und führen Sie eine der folgenden Aktionen aus:

- Um eine bereits vorhandene Regel zu ändern, wählen Sie in der Regelliste die Regel aus, deren Einstellungen Sie anpassen möchten, und klicken Sie auf **Ändern**.
- Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**.

  Je nach Art der angepassten Regel öffnet sich das Fenster **Regel für Programm anpassen** oder das Fenster **Regel für Port anpassen**.

7. Im nächsten 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 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 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 Regel an.
     b. Geben Sie 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 Adressen ist nur im Format IPv4 zulässig.

8. Klicken Sie im Fenster **Regel für Programm anpassen** oder **Regel für Port anpassen** auf **OK**.
9. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.
10. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln löschen

Sie können nur Regeln für Apps und Ports löschen. Sie können bereits vorhandene Regeln für Gruppen nicht löschen.

Um eine bereits vorhandene Regel zur Filterung von eingehendem Datenverkehr zu löschen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Unterabschnitt **Firewall-Verwaltung**.
5. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
6. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
7. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
8. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählte Regel wird gelöscht.
9. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **OK**.
10. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.
11. Klicken Sie im Fenster **Eigenschaften: <Name der Richtlinie>** auf **OK**.

Die angegebenen Aufgabeneinstellungen für die Firewall-Verwaltung werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie Firewall-Regeln über die Benutzeroberfläche der Programmkonsole hinzufügen und konfigurieren.

Firewall-Regeln aktivieren und deaktivieren

Um eine bereits vorhandene Regel zur Filterung des eingehenden Datenverkehrs zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Firewall-Verwaltung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Firewall-Verwaltung** auf den Link **Firewall-Regeln**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
4. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
5. Suchen Sie in der Liste der Regeln die Regel aus, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

   - Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird aktiviert.
   - Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird deaktiviert.
6. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln manuell hinzufügen

So fügen Sie eine neue Regel zur Filterung des eingehenden Datenverkehrs hinzu oder ändern eine bereits vorhandene Regel:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Firewall-Verwaltung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Firewall-Verwaltung** auf den Link **Firewall-Regeln**.

   Das Fenster **Firewall-Regeln** wird geöffnet.
4. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus – je nachdem, welche Art der Regel Sie hinzufügen möchten – und führen Sie eine der folgenden Aktionen aus:

   - Um eine bereits vorhandene Regel zu ändern, wählen Sie in der Regelliste die Regel aus, deren Einstellungen Sie anpassen möchten, und klicken Sie auf **Ändern**.
   - Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**.

     Je nach Art der angepassten Regel öffnet sich das Fenster **Regel für Programm anpassen** oder das Fenster **Regel für Port anpassen**.
5. Im nächsten 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 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 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 Regel an.

b. Geben Sie 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 Adressen ist nur im Format IPv4 zulässig.

6. Klicken Sie im Fenster **Regel für Programm anpassen** oder **Regel für Port anpassen** auf **OK**.
7. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln löschen

Sie können nur Regeln für Apps und Ports löschen. Sie können bereits vorhandene Regeln für Gruppen nicht löschen.

Um eine bereits vorhandene Regel zur Filterung von eingehendem Datenverkehr zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Computer-Kontrolle**.
2. Wählen Sie den untergeordneten Knoten **Firewall-Verwaltung** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Firewall-Verwaltung** auf den Link **Firewall-Regeln**.

Das Fenster **Firewall-Regeln** wird geöffnet.

4. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
5. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
6. Klicken Sie auf die Schaltfläche **Löschen**.

Die ausgewählte Regel wird gelöscht.

7. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln über das Web-Plug-in verwalten

So konfigurieren Sie die Firewall-Regeln über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Netzwerküberwachung** aus.
5. Klicken Sie im Unterabschnitt **Firewall-Verwaltung** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen der Aufgabe zur Firewall-Verwaltung

Einstellung	Beschreibung
Programmregeln	Sie können die Programmregeln verwalten. Regeln dieser Art erlauben Netzwerkverbindungen für ausgewählte angegebene Apps. Ein Auslösekriterium für solche Regeln ist der Pfad zur ausführbaren Datei.
Portregeln	Sie können Portregeln verwalten. Regeln dieser Art erlauben Netzwerkverbindungen für angegebene Ports und Protokolle (TCP/UDP). Die Auslösekriterien solcher Regeln sind die Portnummer und der Typ des Protokolls.
Aufgabenverwaltung	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

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. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Netzwerküberwachung** aus.
5. Klicken Sie im Unterabschnitt **Firewall-Verwaltung** auf **Einstellungen**.

6. Wählen Sie die Registerkarte **Programmregeln** oder **Portregeln** aus, je nachdem für welchen Regeltyp Sie den Status ändern möchten.

7. Suchen Sie in der Liste der Regeln die Regel aus, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

   - Damit eine inaktive Regel angewendet wird, aktivieren Sie die Umschaltfläche links neben dem Namen der Regel.

   - Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie die Umschaltfläche links neben dem Namen der Regel.

8. Klicken Sie auf **OK**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln manuell hinzufügen

So fügen Sie eine neue Regel zur Filterung des eingehenden Datenverkehrs hinzu oder ändern eine bereits vorhandene Regel:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.

2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.

4. Wählen Sie den Abschnitt **Netzwerküberwachung** aus.

5. Klicken Sie im Unterabschnitt **Firewall-Verwaltung** auf **Einstellungen**.

6. Wählen Sie die Registerkarte **Programmregeln** oder **Portregeln** aus – je nachdem, für welchen Regeltyp Sie den Status ändern möchten –, und führen Sie eine der folgenden Aktionen aus:

   - Um eine bereits vorhandene Regel zu ändern, wählen Sie die Regel aus, deren Einstellungen Sie anpassen möchten, und klicken Sie auf **Ändern**.

   - Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**.

7. Führen Sie im rechten Bildschirmbereich die folgenden Aktionen aus:

   - Wenn Sie eine Regel für Apps anpassen, gehen Sie wie folgt vor:

     a. Geben Sie im Feld **Regelname** den Namen der 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.

     c. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

     Die Angabe von 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 Regel an.

  b. Geben Sie 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 Adressen ist nur im Format IPv4 zulässig.

8. Klicken Sie auf **OK**.
9. Klicken Sie im Fenster **Firewall-Verwaltung** auf die Schaltfläche **OK**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln löschen

Sie können nur Regeln für Apps und Ports löschen. Sie können bereits vorhandene Regeln für Gruppen nicht löschen.

Um eine bereits vorhandene Regel zur Filterung von eingehendem Datenverkehr zu löschen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Netzwerküberwachung** aus.
5. Klicken Sie im Unterabschnitt **Firewall-Verwaltung** auf **Einstellungen**.
6. Wählen Sie die Registerkarte **Programmregeln** oder **Portregeln** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
7. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
8. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählte Regel wird gelöscht.
9. Klicken Sie auf **OK**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Überwachung der Datei-Integrität

Dieser Abschnitt enthält Informationen über den Start und das Anpassen der Aufgabe zur Überwachung der Datei-Integrität.

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 Gerät 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 externes Gerät nicht physisch auf einem geschützten Gerät vorhanden ist. Kaspersky Embedded Systems Security benachrichtigt Sie über gefundene Dateioperationen im Überwachungsbereich, sobald wieder ein externes Gerät 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 Gerät müssen ReFS- oder NTFS-Dateisysteme verwendet werden.
- 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 für den Überwachungsbereich erstellen. 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 zur Überwachung der Datei-Integrität wird auf der Grundlage der Regeln zur Überwachung von Datei-Operationen ausgeführt. Sie können mithilfe von Auslösekriterien für Regeln die Bedingungen zum Auslösen der Aufgabe anpassen und die Prioritätsstufe für gefundene Dateioperationen bestimmen, die im Protokoll der Aufgabenausführung gespeichert werden.

Die Regel zur Überwachung von Datei-Operationen wird für jeden festgelegten Überwachungsbereich angegeben.

Sie können folgende Auslösekriterien für Regeln anpassen:

- Vertrauenswürdige Benutzer
- Datei-Operations-Marker

Vertrauenswürdige Benutzer

Standardmäßig stuft das Programm die Aktionen aller Benutzer als potenzielle Verletzungen der Sicherheit ein. Die Liste mit vertrauenswürdigen Benutzern ist leer. Sie können die Prioritätsstufe des Ereignisses anpassen, indem Sie eine Liste mit vertrauenswürdigen Benutzern in den Einstellungen der Regel zur Überwachung von Datei-Operationen erstellen.

Nicht vertrauenswürdiger Benutzer ist ein Status, der einem Benutzer zugewiesen wird, der in den Einstellungen des Überwachungsbereichs nicht zur Liste vertrauenswürdiger Benutzer hinzugefügt wurde. Wenn Kaspersky Embedded Systems Security eine Dateioperation findet, die von einem nicht vertrauenswürdigen Benutzer ausgeführt wurde, protokolliert die Aufgabe zur Überwachung der Datei-Integrität ein Ereignis mit der Ereigniskategorie "Kritisches Ereignis" im Protokoll der Aufgabenausführung.

Vertrauenswürdiger Benutzer ist ein Status, der einem Benutzer oder einer Benutzergruppe zugewiesen wird, dem/der das Ausführen von Dateioperationen im angegebenen Überwachungsbereich erlaubt ist. Wenn Kaspersky Embedded Systems Security Dateioperationen findet, die von einem vertrauenswürdigen Benutzer ausgeführt wurden, protokolliert die Aufgabe zur Überwachung der Datei-Integrität ein Informatives Ereignis im Protokoll der Aufgabenausführung.

Kaspersky Embedded Systems Security kann Benutzer nicht bestimmen, die Operationen in einem Zeitraum, in dem die Überwachung unterbrochen war, ausführen. In diesem Fall wird der Status des Benutzers als Unbekannt angegeben.

Unbekannter Benutzer ist ein Status, der einem Benutzer zugewiesen wird, wenn Kaspersky Embedded Systems Security keine Daten über den Benutzer abrufen kann, da die Aufgabe unterbrochen wurde oder eine Störung in der Synchronisierung der Treiberdaten oder des USN-Protokolls aufgetreten ist. Wenn Kaspersky Embedded Systems Security eine Dateioperation findet, die von einem unbekannten Benutzer ausgeführt wurde, speichert die Aufgabe zur Überwachung der Datei-Integrität das Ereignis mit der Ereigniskategorie *Warnung* im Protokoll der Aufgabenausführung.

Datei-Operations-Marker

Während der Ausführung der Aufgabe zur Überwachung der Datei-Integrität ermittelt Kaspersky Embedded Systems Security mithilfe von Datei-Operations-Markern, ob eine Aktion mit einer Datei ausgeführt wurde.

Der Datei-Operations-Marker ist ein eindeutiges Merkmal, mit dem eine Dateioperation charakterisiert werden kann.

Jede Dateioperation kann eine einzelne Aktion oder eine Kette von Aktionen mit Dateien darstellen. Jede solche Aktion wird einem Datei-Operations-Marker gleichgestellt. Wenn in der Kette der Dateioperationen ein Marker gefunden wird, der von Ihnen als Auslösekriterium für eine Überwachungsregel festgelegt wurde, protokolliert das Programm das Ereignis nach der Durchführung einer solchen Dateioperation.

Die Prioritätsstufe der protokollierten Ereignisse hängt nicht von den ausgewählten Datei-Operations-Markern oder ihrer Anzahl ab.

Standardmäßig werden von Kaspersky Embedded Systems Security alle verfügbaren Marker für Datei-Operationen berücksichtigt. Sie können Datei-Operations-Marker manuell in den Einstellungen der Aufgabenregeln auswählen (s. Tabelle unten).

Datei-Operations-Marker

ID der Dateioperation	Datei-Operations-Marker	Unterstützte Dateisysteme
BASIC_INFO_CHANGE	Attribute oder Zeitstempel der Datei bzw. des Ordners wurden verändert	NTFS, ReFS
COMPRESSION_CHANGE	Die Komprimierungsrate der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
DATA_EXTEND	Die Größe der Datei bzw. des Ordners hat sich erhöht	NTFS, ReFS
DATA_OVERWRITE	Daten in der Datei bzw. dem Ordner wurden überschrieben	NTFS, ReFS
DATA_TRUNCATION	Die Datei bzw. der Ordner wurde gekürzt	NTFS, ReFS
EA_CHANGE	Erweiterte Attribute von Datei oder Ordner wurden verändert	Nur NTFS
ENCRYPTION_CHANGE	Der Verschlüsselungsstatus der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
FILE_CREATE	Die Datei bzw. der Ordner wurde zum ersten Mal erstellt	NTFS, ReFS
FILE_DELETE	Eine Datei oder ein Ordner wurde mit der Tastenkombination UMSCHALT+ENTF permanent gelöscht.	NTFS, ReFS
HARD_LINK_CHANGE	Für die Datei bzw. den Ordner wurde ein harter Link erstellt oder gelöscht	Nur NTFS
INDEXABLE_CHANGE	Der Indizierungsstatus der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
INTEGRITY_CHANGE	Das Integritätsattribut für den benannten Dateidatenstrom wurde verändert	Nur ReFS
NAMED_DATA_EXTEND	Die Größe des benannten Dateidatenstroms hat sich erhöht	NTFS, ReFS
NAMED_DATA_OVERWRITE	Ein benannter Dateidatenstrom wurde überschrieben	NTFS, ReFS
NAMED_DATA_TRUNCATION	Ein benannter Dateidatenstrom wurde gekürzt	NTFS, ReFS

OBJECT_ID_CHANGE	Die ID der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
RENAME_NEW_NAME	Der Datei bzw. dem Ordner wurde ein neuer Name zugewiesen	NTFS, ReFS
REPARSE_POINT_CHANGE	Für die Datei bzw. den Ordner wurde ein neuer Analysepunkt erstellt oder ein vorhandener Punkt verändert	NTFS, ReFS
SECURITY_CHANGE	Die Zugriffsrechte zur Datei bzw. zum Ordner wurden verändert	NTFS, ReFS
STREAM_CHANGE	Ein neuer benannter Dateidatenstrom wurde erstellt oder ein vorhandener verändert	NTFS, ReFS
TRANSACTED_CHANGE	Ein benannter Dateidatenstrom wurde durch die TxF-Transaktion verändert	Nur ReFS

Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Die Aufgabe "Überwachung der Datei-Integrität" weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter für folgende Komponenten anpassen:

- Verwaltungs-Plug-in
- Programmkonsole
- Web-Plug-in

Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Standardwert	Beschreibung
Überwachungsbereich	Nicht festgelegt.	Verwenden Sie diese Option, um Ordner und Dateien anzugeben, deren Aktionen überwacht werden sollen. Für die Ordner und Dateien des angegebenen Überwachungsbereichs werden Überwachungsereignisse erstellt.
Liste **Vertrauenswürdige Benutzer**	Nicht festgelegt.	Verwenden Sie diese Option, um Benutzer und\oder Benutzergruppen anzugeben, deren Aktionen in den angegebenen Ordnern von der Komponente als sicher eingestuft werden sollen.
Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden	Wird verwendet	Verwenden Sie diese Option, um das in den angegebenen Überwachungsbereichen durchgeführte Protokollieren von Dateioperationen dann zu aktivieren oder zu deaktivieren, wenn die Aufgabe nicht ausgeführt wird. Standardmäßig werden für vertrauenswürdige Benutzer Statistiken erstellt, unabhängig von konfigurierten Regeln.
Versuche zur Kompromittierung des USN-Protokolls blockieren	Wird verwendet	Verwenden Sie diese Option, um den Schutz des USN-Protokolls zu aktivieren und zu deaktivieren.
Vertrauenswürdige Zone anwenden	Deaktiviert	Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, um die Ausschlüsse der

		Vertrauenswürdige Zone zusätzlich zum Überwachungsbereich der konfigurierten Regel anzuwenden.
Alle Dateioperationen blockieren	Deaktiviert	Aktivieren oder Deaktivieren Sie das Kontrollkästchen **Alle Dateioperationen blockieren**, wenn Sie alle Änderungen für die ausgewählten Überwachungsbereiche blockieren wollen.
Folgende Ordner aus der Überwachung ausschließen	Wird nicht verwendet	Verwenden Sie diese Option, um die Verwendung von Ausschlüssen für die Ordner zu aktivieren, in denen keine Dateioperationen überwacht werden müssen. Bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität überspringt Kaspersky Embedded Systems Security Überwachungsbereiche, die als Ausnahmen festgelegt wurden.
Berechnung der Prüfsumme	Wird nicht verwendet	Verwenden Sie diese Option, um die Berechnung der Dateiprüfsumme nach Dateiänderungen zu konfigurieren.
Marker für Datei-Operationen	Es werden alle verfügbaren Datei-Operations-Marker berücksichtigt.	Verwenden Sie diese Option, um die Marker für Datei-Operationen festzulegen. Wenn eine im Überwachungsbereich ausgeführte Dateioperation mit einem oder mehreren angegebenen Marker gekennzeichnet ist, erstellt Kaspersky Embedded Systems Security ein Systemaudit-Ereignis.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt	Sie können die Einstellungen zum Starten der Aufgabe nach einem Zeitplan konfigurieren.

Überwachung der Datei-Integrität über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung der Datei-Integrität über das Verwaltungs-Plug-in konfigurieren.

Aufgabe "Überwachung der Datei-Integrität" anpassen

So konfigurieren Sie die allgemeinen Einstellungen der Aufgabe zur Überwachung der Dateiintegrität:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **System-Diagnose** im Unterabschnitt **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung der Datei-Integrität** wird geöffnet.

5. Passen Sie im folgenden Fenster auf der Registerkarte **Einstellungen zur Überwachung von Dateioperationen** die folgenden Einstellungen an:

   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden**.

     Das Kontrollkästchen aktiviert oder deaktiviert die Überwachung der Dateioperationen, die in den Einstellungen der Aufgabe Überwachung der Datei-Integrität ausgewählt sind, auch in Zeiträumen, in denen die Aufgabenausführung aus irgendeinem Grund unterbrochen ist (Entfernung der Festplatte, Beenden der Aufgabe durch Benutzer, Funktionsstörung der Software).

     Wenn das Kontrollkästchen aktiviert ist, protokolliert Kaspersky Embedded Systems Security die Ereignisse in allen Überwachungsbereichen während der Unterbrechung der Aufgabe zur Überwachung der Datei-Integrität.

     Wenn das Kontrollkästchen deaktiviert ist, werden die Dateioperationen in den Überwachungsbereichen bei einer Unterbrechung der Aufgabe nicht vom Programm protokolliert.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Versuche zur Kompromittierung des USN-Protokolls blockieren**.

     Das Kontrollkästchen aktiviert oder deaktiviert den Schutz des USN-Protokolls.

     Bei aktiviertem Kontrollkästchen blockiert Kaspersky Embedded Systems Security die Versuche, das USN-Protokoll zu löschen oder den Inhalt des USN-Protokolls zu gefährden.

     Wenn das Kontrollkästchen deaktiviert ist, überwacht das Programm die Änderungen am USN-Protokoll nicht.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden** entsprechend Ihren Bedürfnissen.

     Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **Ausschlüsse** und **vertrauenswürdigen Prozesse** zusätzlich zur konfigurierten Regel auf den Überwachungsbereich angewendet.

     Wenn das Kontrollkästchen **Vertrauenswürdige Zone** anwenden deaktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **Ausschlüsse** und **vertrauenswürdigen Prozesse** nicht auf den Überwachungsbereich angewendet.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

   - Fügen Sie die Überwachungsbereiche hinzu, die von der Aufgabe überwacht werden sollen.

6. Konfigurieren Sie auf der Registerkarte **Aufgabenverwaltung** die Aufgabeneinstellungen für den Start der Aufgabe nach einem Zeitplan.

7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben über Datum und Uhrzeit zur Veränderungen der Einstellungen werden im Systemaudit-Protokoll gespeichert.

Einstellungen der Überwachungsregeln anpassen

Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:

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

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

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

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

   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **System-Diagnose** im Unterabschnitt **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung der Datei-Integrität** wird geöffnet.

5. Klicken Sie im Abschnitt **Überwachungsbereich** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regel zur Überwachung von Dateioperationen** wird geöffnet.

6. Fügen Sie den Überwachungsbereich auf eine der folgenden Arten hinzu:

   - Wenn Sie im Standarddialog von Microsoft Windows Ordner auswählen möchten:

     a. Klicken Sie auf die Schaltfläche **Durchsuchen**.

        Das Microsoft-Windows-Standardfenster **Ordner durchsuchen** wird geöffnet.

     b. Wählen Sie im sich öffnenden Fenster **Ordner durchsuchen** den Ordner aus, dessen Dateioperationen Sie überwachen möchten, und klicken Sie auf **OK**.

   - Um den Überwachungsbereich manuell festzulegen, fügen Sie mithilfe einer der unterstützten Masken einen Pfad hinzu:

     - <*.ext> — alle Dateien mit der Erweiterung <ext> unabhängig von ihrem Speicherort

- <*\name.ext> — alle Dateien mit dem Namen <name> und der Erweiterung <ext> unabhängig von ihrem Speicherort
- <\dir*> — alle Dateien im Ordner <\dir>
- <\dir*\name.ext> — alle Dateien mit dem Namen <name> und der Erweiterung <ext> im Ordner <\dir> und allen Unterordnern

Stellen Sie bei der manuellen Angabe des Überwachungsbereichs sicher, dass der Pfad dem folgenden Format entspricht: <Laufwerksbuchstabe>:\<Maske>. Wenn der Laufwerksbuchstabe fehlt, fügt Kaspersky Embedded Systems Security den angegebenen Überwachungsbereich nicht hinzu.

7. Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

   Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** erscheint.

8. Wählen Sie die Benutzer oder Benutzergruppen aus, die Dateioperationen in den ausgewählten Überwachungsbereichen ausführen dürfen, und klicken Sie auf **OK**.

   Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein und erstellt für sie kritische Ereignisse. Für vertrauenswürdige Benutzer werden Statistiken erstellt.

9. Wählen Sie die Registerkarte **Datei-Operations-Marker** aus.

10. Um mehrere Marker nach Bedarf auszuwählen, folgen Sie den Schritten:

    a. Wählen Sie die Option **Dateioperationen anhand folgender Marker erkennen** aus.

    b. Aktivieren Sie in der Liste der verfügbaren Dateioperationen die Kontrollkästchen aller Operationen, die Sie überwachen möchten.

    Standardmäßig überwacht Kaspersky Embedded Systems Security alle verfügbaren Dateioperationen, wenn die Option **Dateioperationen anhand aller bekannten Marker erkennen** ausgewählt ist.

11. Wenn Sie alle Dateioperationen für den ausgewählten Bereich blockieren möchten, aktivieren Sie das Kontrollkästchen **Alle Dateioperationen blockieren**.

12. Wenn Sie möchten, dass Kaspersky Embedded Systems Security eine Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen **Prüfsumme der Datei berechnen, wenn möglich. Die Prüfsumme wird im Bericht zur Aufgabenausführung angegeben** angezeigt.

    b. Wählen Sie in der Dropdownliste **Prüfsummentyp** eine der folgenden Optionen aus:

    - **MD5-Hash**
    - **SHA256-Hash**

13. Wenn Sie nicht alle Dateioperationen überwachen möchten, aktivieren Sie in der Liste der verfügbaren Dateioperationen die Kontrollkästchen neben den Operationen, die Sie überwachen möchten.

14. Fügen Sie bei Bedarf ausgeschlossene Überwachungsbereich hinzu:

    a. Wählen Sie die Registerkarte **Ausnahmen** aus.

    b. Aktivieren Sie das Kontrollkästchen **Folgende Ordner aus der Überwachung ausschließen**.

    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.

15. Klicken Sie im Fenster **Regel zur Überwachung von Dateioperationen** auf **OK**.

    Die angegebenen Einstellungen der Regeln werden im ausgewählten Überwachungsbereich der Aufgabe zur Überwachung der Datei-Integrität angewendet.

Überwachung der Datei-Integrität über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung der Datei-Integrität über die Programmkonsole konfigurieren.

Einstellungen der Aufgabe Überwachung der Datei-Integrität anpassen

So konfigurieren Sie die allgemeinen Einstellungen der Aufgabe zur Überwachung der Dateiintegrität:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Überwachung der Datei-Integrität** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Überwachung der Datei-Integrität** auf den Link **Eigenschaften**.

    Das Fenster **Aufgabeneinstellungen** erscheint.

4. Konfigurieren Sie im geöffneten Fenster auf der Registerkarte **Allgemein** die folgenden Einstellungen:

    a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden**.

Das Kontrollkästchen aktiviert oder deaktiviert die Überwachung der Dateioperationen, die in den Einstellungen der Aufgabe Überwachung der Datei-Integrität ausgewählt sind, auch in Zeiträumen, in denen die Aufgabenausführung aus irgendeinem Grund unterbrochen ist (Entfernung der Festplatte, Beenden der Aufgabe durch Benutzer, Funktionsstörung der Software).

Wenn das Kontrollkästchen aktiviert ist, protokolliert Kaspersky Embedded Systems Security die Ereignisse in allen Überwachungsbereichen während der Unterbrechung der Aufgabe zur Überwachung der Datei-Integrität.

Wenn das Kontrollkästchen deaktiviert ist, werden die Dateioperationen in den Überwachungsbereichen bei einer Unterbrechung der Aufgabe nicht vom Programm protokolliert.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

b. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Versuche zur Kompromittierung des USN-Protokolls blockieren**.

Das Kontrollkästchen aktiviert oder deaktiviert den Schutz des USN-Protokolls.

Bei aktiviertem Kontrollkästchen blockiert Kaspersky Embedded Systems Security die Versuche, das USN-Protokoll zu löschen oder den Inhalt des USN-Protokolls zu gefährden.

Wenn das Kontrollkästchen deaktiviert ist, überwacht das Programm die Änderungen am USN-Protokoll nicht.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

c. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden** entsprechend Ihren Bedürfnissen.

Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **Ausschlüsse** und **vertrauenswürdigen Prozesse** zusätzlich zur konfigurierten Regel auf den Überwachungsbereich angewendet.

Wenn das Kontrollkästchen **Vertrauenswürdige Zone** anwenden deaktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **Ausschlüsse** und **vertrauenswürdigen Prozesse** nicht auf den Überwachungsbereich angewendet.

Das Kontrollkästchen ist standardmäßig deaktiviert.

5. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben über Datum und Uhrzeit zur Veränderungen der Einstellungen werden im Systemaudit-Protokoll gespeichert.

Einstellungen der Überwachungsregeln anpassen

Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.

2. Wählen Sie darin den untergeordneten Knoten **Überwachung der Datei-Integrität** aus.

3. Klicken Sie im Ergebnisbereich des Knotens **Überwachung der Datei-Integrität** auf den Link **Regeln zur Überwachung von Datei-Operationen**.

   Das Fenster **Überwachung von Dateioperationen** wird geöffnet.

4. Fügen Sie den Überwachungsbereich auf eine der folgenden Arten hinzu:

   - Wenn Sie im Standarddialog von Microsoft Windows Ordner auswählen möchten:

     a. Klicken Sie im linken Bereich des Fensters auf die Schaltfläche **Durchsuchen.**

        Das Microsoft-Windows-Standardfenster **Ordner durchsuchen** erscheint.

     b. Wählen Sie im Fenster **Ordner durchsuchen** den Ordner aus, dessen Dateioperationen Sie überwachen möchten, und klicken Sie auf **OK**.

     c. Klicken Sie auf **Hinzufügen**, Kaspersky Embedded Systems Security damit beginnt, Dateioperationen im angegebenen Überwachungsbereich zu überwachen.

   - Um den Überwachungsbereich manuell festzulegen, fügen Sie mithilfe einer der unterstützten Masken einen Pfad hinzu:

     - <*.ext> — alle Dateien mit der Erweiterung <ext> unabhängig von ihrem Speicherort
     - <*\name.ext> — alle Dateien mit dem Namen <name> und der Erweiterung <ext> unabhängig von ihrem Speicherort
     - <\dir*> — alle Dateien im Ordner <\dir>
     - <\dir*\name.ext> — alle Dateien mit dem Namen <name> und der Erweiterung <ext> im Ordner <\dir> und allen Unterordnern

   Stellen Sie bei der manuellen Angabe des Überwachungsbereichs sicher, dass der Pfad dem folgenden Format entspricht: <Laufwerksbuchstabe>:\<Maske>. Wenn der Laufwerksbuchstabe fehlt, fügt Kaspersky Embedded Systems Security den angegebenen Überwachungsbereich nicht hinzu.

   Im rechten Fensterbereich auf der Registerkarte **Regelbeschreibung** werden vertrauenswürdige Benutzer und Marker für Datei-Operationen angezeigt, die für diesen Überwachungsbereich gewählt wurden.

5. Wählen Sie in der Liste der hinzugefügten Überwachungsbereiche die Einstellungen des Bereichs aus, den Sie anpassen möchten.

6. Wählen Sie die Registerkarte **Vertrauenswürdige Benutzer** aus.

7. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Microsoft-Windows-Standardfenster **Benutzer oder Gruppen auswählen** erscheint.

8. Wählen Sie die Benutzer oder Benutzergruppen aus, die Kaspersky Embedded Systems Security für den ausgewählten Überwachungsbereich als vertrauenswürdig einstufen soll.

9. Klicken Sie auf **OK**.

   Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein und erstellt für sie kritische Ereignisse. Für vertrauenswürdige Benutzer werden Statistiken erstellt.

10. Wählen Sie die Registerkarte **Marker für Datei-Operationen** aus.

11. Gehen Sie wie folgt vor, um bei Bedarf mehrere Marker auszuwählen:

    a. Wählen Sie die Option **Dateioperationen anhand folgender Marker erkennen** aus.

    b. Aktivieren Sie in der Liste der verfügbaren Dateioperationen die Kontrollkästchen aller Operationen, die Sie überwachen möchten.

    Standardmäßig überwacht Kaspersky Embedded Systems Security alle verfügbaren Dateioperationen, d. h., die Option **Dateioperationen anhand aller bekannten Marker erkennen** ist ausgewählt.

12. Wenn Sie alle Dateioperationen für den ausgewählten Bereich blockieren möchten, aktivieren Sie das Kontrollkästchen **Alle Dateioperationen blockieren**.

13. Wenn Sie möchten, dass Kaspersky Embedded Systems Security eine Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:

    a. Aktivieren Sie im Abschnitt **Berechnung der Prüfsumme** die Option **Prüfsumme der geänderten Datei berechnen, wenn möglich. Die Prüfsumme wird im Protokoll der Aufgabenausführung angegeben** angezeigt.

    b. Wählen Sie in der Dropdown-Liste **Prüfsumme anhand von Algorithmus berechnen** eine der folgenden Optionen aus:

    - **MD5-Hash**.
    - **SHA256-Hash**.

14. Fügen Sie bei Bedarf ausgeschlossene Überwachungsbereich hinzu:

    a. Wählen Sie die Registerkarte **Ausnahmen** aus.

    b. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene Überwachungsbereiche berücksichtigen**.

    c. Klicken Sie auf die Schaltfläche **Durchsuchen**.

    Das Microsoft-Windows-Standardfenster **Ordner durchsuchen** erscheint.

    d. Wählen Sie im Fenster **Ordner durchsuchen** den Ordner aus, den Sie aus dem Überwachungsbereich ausschließen möchten.

    e. Klicken Sie auf **OK**.

    f. Klicken Sie auf die Schaltfläche **Hinzufügen**.

    Der angegebene Ordner wird zur Liste der ausgeschlossenen Bereiche hinzugefügt.

    Sie können Ausnahmen für Überwachungsbereiche auch manuell hinzufügen, indem Sie die gleichen Masken verwenden wie für die Angabe des Überwachungsbereichs.

15. Klicken Sie auf die Schaltfläche **Speichern**, um die neue Konfigurationsdatei der Regel zu übernehmen.

Die angegebenen Einstellungen der Regeln werden sofort im festgelegten Überwachungsbereich der Aufgabe zur **Überwachung der Datei-Integrität** angewendet.

Überwachung der Dateiintegrität über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung der Dateiintegrität über das Web-Plug-in konfigurieren.

Aufgabe "Überwachung der Datei-Integrität" anpassen

So konfigurieren Sie die Aufgabe "Überwachung der Dateiintegrität" über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **System-Diagnose** aus.
5. Klicken Sie im Unterabschnitt **Überwachung der Datei-Integrität** auf **Einstellungen**.
6. Nehmen Sie im erscheinenden Fenster **Überwachung der Datei-Integrität** auf der Registerkarte **Einstellungen zur Überwachung von Dateioperationen** die folgenden Anpassungen vor:

   a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden**.

   Das Kontrollkästchen aktiviert oder deaktiviert die Überwachung der Dateioperationen, die in den Einstellungen der Aufgabe Überwachung der Datei-Integrität ausgewählt sind, auch in Zeiträumen, in denen die Aufgabenausführung aus irgendeinem Grund unterbrochen ist (Entfernung der Festplatte, Beenden der Aufgabe durch Benutzer, Funktionsstörung der Software).

   Wenn das Kontrollkästchen aktiviert ist, protokolliert Kaspersky Embedded Systems Security die Ereignisse in allen Überwachungsbereichen während der Unterbrechung der Aufgabe zur Überwachung der Datei-Integrität.

   Wenn das Kontrollkästchen deaktiviert ist, werden die Dateioperationen in den Überwachungsbereichen bei einer Unterbrechung der Aufgabe nicht vom Programm protokolliert.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   b. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Versuche zur Kompromittierung des USN-Protokolls blockieren**.

   Das Kontrollkästchen aktiviert oder deaktiviert den Schutz des USN-Protokolls.

   Bei aktiviertem Kontrollkästchen blockiert Kaspersky Embedded Systems Security die Versuche, das USN-Protokoll zu löschen oder den Inhalt des USN-Protokolls zu gefährden.

   Wenn das Kontrollkästchen deaktiviert ist, überwacht das Programm die Änderungen am USN-Protokoll nicht.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   c. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden** entsprechend Ihren Bedürfnissen.

Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **Ausschlüsse** und **vertrauenswürdigen Prozesse** zusätzlich zur konfigurierten Regel auf den Überwachungsbereich angewendet.

Wenn das Kontrollkästchen **Vertrauenswürdige Zone** anwenden deaktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **Ausschlüsse** und **vertrauenswürdigen Prozesse** nicht auf den Überwachungsbereich angewendet.

Das Kontrollkästchen ist standardmäßig deaktiviert.

7. Passen Sie auf der Registerkarte **Aufgabenverwaltung** den Zeitplan für den Aufgabenstart an.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben über Datum und Uhrzeit zur Veränderungen der Einstellungen werden im Systemaudit-Protokoll gespeichert.

Einstellungen der Überwachungsregeln anpassen

Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **System-Diagnose** aus.
5. Klicken Sie im Unterabschnitt **Überwachung der Datei-Integrität** auf **Einstellungen**.
6. Öffnen Sie im nächsten Fenster **Überwachung der Datei-Integrität** die Registerkarte **Einstellungen zur Überwachung von Dateioperationen**.
7. Klicken Sie im Abschnitt **USN-Protokoll** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regel zur Überwachung von Dateioperationen** erscheint.
8. Geben Sie unter **Dateioperationen im folgenden Bereich überwachen** mithilfe einer der unterstützten Masken einen Pfad an:
   - <*.ext> – alle Dateien mit der Erweiterung <ext> unabhängig von ihrem Speicherort
   - <*\name.ext> – alle Dateien mit dem Namen <name> und der Erweiterung <ext> unabhängig von ihrem Speicherort
   - <\dir*> – alle Dateien im Ordner <\dir>
   - <\dir*\name.ext> – alle Dateien mit dem Namen <name> und der Erweiterung <ext> im Ordner <\dir> und allen Unterordnern

Stellen Sie bei der manuellen Angabe des Überwachungsbereichs sicher, dass der Pfad dem folgenden Format entspricht: <Laufwerksbuchstabe>:\<Maske>. Wenn der Laufwerksbuchstabe fehlt, fügt Kaspersky Embedded Systems Security den angegebenen Überwachungsbereich nicht hinzu.

9. Auf der Registerkarte **Vertrauenswürdige Benutzer** führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Schaltfläche **Hinzufügen** und geben in dem sich öffnenden Fenster den Benutzer im Feld **Benutzername** in SID-Notation an.
   - Klicken Sie auf die Schaltfläche **Vom Administrationsserver hinzufügen** und wählen im anschließend erscheinenden Fenster den Benutzer aus der Liste aus.

   Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein und erstellt für sie kritische Ereignisse. Für vertrauenswürdige Benutzer werden Statistiken erstellt.

10. Klicken Sie auf **OK**.
11. Wählen Sie die Registerkarte **Datei-Operations-Marker** aus.
12. Um mehrere Marker nach Bedarf auszuwählen, folgen Sie den Schritten:

    a. Wählen Sie die Option **Dateioperationen anhand folgender Marker erkennen** aus.

    b. Aktivieren Sie in der Liste der verfügbaren Dateioperationen die Kontrollkästchen aller Operationen, die Sie überwachen möchten.

    Standardmäßig überwacht Kaspersky Embedded Systems Security alle verfügbaren Dateioperationen, wenn die Option **Dateioperationen anhand aller bekannten Marker erkennen** ausgewählt ist.

13. Wenn Sie alle Dateioperationen für den ausgewählten Bereich blockieren möchten, aktivieren Sie das Kontrollkästchen **Alle Dateioperationen blockieren**.
14. Wenn Sie möchten, dass Kaspersky Embedded Systems Security eine Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:

    a. Aktivieren Sie das Kontrollkästchen **Prüfsumme der Datei berechnen, wenn möglich. Die Prüfsumme wird im Bericht zur Aufgabenausführung angegeben** angezeigt.

    b. Wählen Sie in der Dropdownliste **Prüfsummentyp** eine der folgenden Optionen aus:

    - **SHA256-Hash**
    - **MD5-Hash**

15. Wenn Sie nicht alle Dateioperationen überwachen möchten, aktivieren Sie in der Liste der verfügbaren Dateioperationen die Kontrollkästchen neben den Operationen, die Sie überwachen möchten.
16. Fügen Sie bei Bedarf ausgeschlossene Überwachungsbereich hinzu:

    a. Wählen Sie die Registerkarte **Ausnahmen** aus.

b. Aktivieren Sie das Kontrollkästchen **Folgende Ordner aus der Überwachung ausschließen**.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Das Fenster **Ordner zum Hinzufügen auswählen** wird geöffnet.

d. Wählen Sie in dem Bereich, der rechts geöffnet wird, 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.

17. Klicken Sie im Fenster **Regel zur Überwachung von Dateioperationen** auf **OK**.

Die angegebenen Einstellungen der Regeln werden im ausgewählten Überwachungsbereich der Aufgabe zur Überwachung der Datei-Integrität angewendet.

Überwachung des Registrierungszugriffs

In diesem Abschnitt wird erläutert, wie Sie die Aufgabe zur Überwachung des Registrierungszugriffs starten und konfigurieren.

Über die Aufgabe zur Überwachung des Registrierungszugriffs

Die Aufgabe zur Überwachung des Registrierungszugriffs überwacht Aktionen, die mit bestimmten Registrierungspfaden und Registrierungsschlüsseln ausgeführt werden, im Rahmen von Überwachungsbereichen, die in den Einstellungen der Aufgabe festgelegt wurden. Mithilfe der Aufgabe können Sie Änderungen erkennen, die eventuell auf eine Verletzung der Sicherheit auf dem geschützten Gerät hindeuten.

Um die Aufgabe zur Überwachung des Registrierungszugriffs zu starten, müssen Sie mindestens eine Überwachungsregel konfigurieren.

Über die Regeln zur Überwachung der Systemregistrierung

Die Aufgabe Überwachung des Registrierungszugriffs wird auf Grundlage der Regeln zur Überwachung des Systemregistrierung ausgeführt. Sie können mithilfe von Auslösekriterien für Regeln die Bedingungen zum Auslösen der Aufgabe anpassen und die Prioritätsstufe für gefundene Ereignisse bestimmen, die im Protokoll der Aufgabenausführung gespeichert werden.

Die Regel zur Überwachung der Systemregistrierung wird für jeden festgelegten Überwachungsbereich angegeben.

Sie können folgende Auslösekriterien für Regeln anpassen:

- **Aktionen**
- **Registrierungswerte**
- **Vertrauenswürdige Benutzer**

Aktionen

Wenn die Aufgabe zur Überwachung des Registrierungszugriffs gestartet ist, verwendet Kaspersky Embedded Systems Security eine Liste mit Vorgängen, auf welche die Registrierung überwacht wird (siehe Tabelle unten).

Wenn ein als Auslösekriterium für Regeln festgelegter Vorgang erkannt wird, protokolliert das Programm ein entsprechendes Ereignis.

Die Prioritätsstufe der protokollierten Ereignisse hängt nicht von den ausgewählten Vorgängen oder ihrer Anzahl ab.

Standardmäßig betrachtet Kaspersky Embedded Systems Security alle Vorgänge. Sie können die Liste mit Vorgängen in den Einstellungen der Aufgabenregeln manuell konfigurieren.

Aktion	Einschränkungen	Betriebssystem
Schlüssel erstellen	• Wenn Sie unter Windows XP und Windows Server 2003 den Vorgang **Schlüssel erstellen** zur Liste mit **Aktionen** hinzufügen und anschließend den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, wird das Erstellen des Schlüssels in den genannten Betriebssystemen aufgrund von Systembeschränkungen nicht blockiert. Der Schlüssel wird erstellt und es wird eine entsprechende Nachricht an die Ereignisprotokollierung gesendet. • Wenn Sie das Erstellen eines bestimmten Schlüssel mittels Registrierungs-Editor verbieten möchten, erstellen Sie eine Regel für einen übergeordneten Schlüssel und stellen Sie sicher, dass Sie den Vorgang **Unterschlüssel erstellen** zur Liste mit **Aktionen** hinzugefügt haben. Wählen Sie anschließend den Modus **Vorgänge entsprechend den Regeln blockieren** aus.	Windows XP und höher
Schlüssel löschen	Wenn Sie einen übergeordneten Schlüssel löschen möchten, stellen Sie sicher, dass Sie die Optionen **Schlüssel löschen** und **Unterschlüssel löschen** für einen konfigurierten Schlüssel auf der Liste der überwachten **Aktionen** deaktiviert haben, da ein übergeordneter Schlüssel nur mitsamt seiner Unterschlüssel gelöscht werden kann.	Windows XP und höher
Schlüssel umbenennen	N/V	Windows XP und höher
Sicherheitseinstellungen des Schlüssels ändern	N/V	Windows Vista und höher
Werte löschen	N/V	Windows XP und höher
Werte festlegen	Wenn Sie den Vorgang **Werte festlegen** zur Liste mit **Aktionen** hinzufügen und in der Regel für einen Schlüssel den Standard-**Name des Werts** festlegen sowie anschließend den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, wird dieser Schlüssel nicht erstellt, da ein neuer Schlüssel nur mit einem Standardwert erstellt werden kann.	Windows XP und höher
Unterschlüssel erstellen	N/V	Windows XP und höher
Unterschlüssel löschen	N/V	Windows XP und höher
Unterschlüssel umbenennen	N/V	Windows XP und höher
Sicherheitseinstellungen der Unterschlüssel ändern	N/V	Windows Vista und höher

Registrierungswerte

Zusätzlich zur Überwachung der Registrierungsschlüssel können Sie Änderungen für existierende Registrierungswerte blockieren oder überwachen. Die folgenden Optionen sind verfügbar:

- **Wert festlegen** – erstellt neue Registrierungswerte oder ändert existierende Registrierungswerte
- **Wert löschen** – löscht existierende Registrierungswerte

Das Umbenennen oder Ändern der Sicherheitseinstellungen steht für Registrierungswerte nicht zur Verfügung.

Vertrauenswürdige Benutzer

Standardmäßig stuft das Programm die Aktionen aller Benutzer als potenzielle Verletzungen der Sicherheit ein. Die Liste mit vertrauenswürdigen Benutzern ist leer. Sie können die Prioritätsstufe des Ereignisses anpassen, indem Sie eine Liste mit vertrauenswürdigen Benutzern in den Einstellungen der Regel zur Überwachung der Systemregistrierung 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 einen Vorgang erkennt, der von einem nicht vertrauenswürdigen Benutzer ausgeführt wurde, protokolliert die Aufgabe zur Überwachung des Registrierungszugriffs ein kritisches Ereignis im Protokoll der Aufgabenausführung.

Ein vertrauenswürdiger Benutzer ist ein Benutzer oder eine Benutzergruppe, dem/der das Ausführen von Vorgängen innerhalb des angegebenen Überwachungsbereich erlaubt ist. Wenn Kaspersky Embedded Systems Security einen Vorgang erkennt, der von einem vertrauenswürdigen Benutzer ausgeführt wurde, protokolliert die Aufgabe zur Überwachung des Registrierungszugriffs ein Informatives Ereignis im Protokoll der Aufgabenausführung.

Standardeinstellungen der Aufgabe zur Überwachung des Registrierungszugriffs

Die Standardeinstellungen der Aufgabe Überwachung des Registrierungszugriffs werden in der unteren Tabelle beschrieben. Sie können die Werte dieser Parameter für folgende Komponenten anpassen:

- Verwaltungs-Plug-in
- Programmkonsole
- Web-Plug-in

Standardeinstellungen der Aufgabe zur Überwachung des Registrierungszugriffs

Einstellung	Standardwert	Beschreibung
Überwachungsbereich	Nicht festgelegt.	Verwenden Sie diese Option, um die zu überwachenden übergeordneten Registrierungsschlüssel und Unterschlüssel anzugeben. Die Überwachungsereignisse werden für die angegeben übergeordneten Registrierungsschlüssel und Unterschlüssel in dem festgelegten Überwachungsbereich erstellt.
Aktionen	Es sind alle Objekte auf der Liste mit	Verwenden Sie diese Option, um eine Liste mit Vorgängen entsprechend Ihren Bedürfnissen durch aktivieren bzw. deaktivieren der Kontrollkästchen zu konfigurieren.

	Vorgängen ausgewählt	
Registrierungswerte	Nicht festgelegt.	Verwenden Sie diese Option, um für den Überwachungsbereich zu überwachende Registrierungswerte hinzufügen, zu ändern oder zu entfernen.
Vertrauenswürdige Benutzer	Nicht festgelegt.	Verwenden Sie diese Option, um Benutzer und Benutzergruppen anzugeben, die zum Ausführen der festgelegten Registrierungsvorgänge für die angegebenen Registrierungsschlüssel berechtigt sind.
Aufgabenmodus	Nur Statistik	Sie können entweder den Aufgabenmodus **Vorgänge entsprechend den Regeln blockieren** auswählen oder den Modus **Nur Statistik** auswählen, um lediglich benachrichtigt zu werden.
Vertrauenswürdige Zone anwenden	Deaktiviert	Sie können das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktivieren, um die Ausschlüsse der **Vertrauenswürdige Zone** zusätzlich zu denen, die für die Regel konfiguriert wurden, anzuwenden.
Zeitplan für den Aufgabenstart	Nicht festgelegt.	Sie können die Einstellungen zum Starten der Aufgabe nach einem Zeitplan konfigurieren.

Überwachung des Registrierungszugriffs über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung des Registrierungszugriffs über das Verwaltungs-Plug-in konfigurieren.

Einstellungen der Aufgabe zur Überwachung des Registrierungszugriffs anpassen

So konfigurieren Sie die Einstellungen der Überwachung des Registrierungszugriffs:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

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

4. Klicken Sie im Abschnitt **System-Diagnose** im Unterabschnitt **Überwachung des Registrierungszugriffs** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung des Registrierungszugriffs** wird geöffnet.

5. Passen Sie auf der Registerkarte **Einstellungen der Überwachung des Registrierungszugriffs** folgende Einstellungen an:

   - Wählen Sie in der Gruppe **Aufgabenmodus** die benötigte Option von der Liste aus:

     - **Vorgänge entsprechend den Regeln blockieren**

       Wenn Sie den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, blockiert Kaspersky Embedded Systems Security die **Vorgänge**, die für den Überwachungsbereich festgelegt wurden. Wenn auch das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, blockiert Kaspersky Embedded Systems Security die unter **Vertrauenswürdige Zone** festgelegten Prozesse nicht.

       Standardmäßig wird der Modus **Nur Statistik** angewendet.

     - **Nur Statistik**

       Wenn für den Überwachungsbereich der Modus **Nur Statistik** ausgewählt ist, erstellt Kaspersky Embedded Systems Security die Statistiken für die Registrierungsschlüssel entsprechend der festgelegten Regeln. Wenn auch das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, erstellt Kaspersky Embedded Systems Security keine Statistiken für die unter **Vertrauenswürdige Zone** festgelegten Prozesse.

       Standardmäßig wird der Modus **Nur Statistik** angewendet.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden** entsprechend Ihren Bedürfnissen.

     Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **vertrauenswürdigen Prozesse** zusätzlich zur konfigurierten Regel auf den Überwachungsbereich angewendet.

     Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** deaktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **vertrauenswürdigen Prozesse** nicht auf den Überwachungsbereich angewendet.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

6. Fügen Sie die Überwachungsbereiche hinzu, die von der Aufgabe überwacht werden sollen.

7. Konfigurieren Sie auf der Registerkarte **Aufgabenverwaltung** die Zeitplan-Einstellungen für eine Aufgabe.

8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben über Datum und Uhrzeit zur Veränderungen der Einstellungen werden im Systemaudit-Protokoll gespeichert.

Einstellungen der Überwachungsregeln anpassen

Die Überwachungsregeln werden nacheinander, entsprechend ihrer Reihenfolge in der Liste der konfigurierten Regeln, angewendet.

Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **System-Diagnose** im Unterabschnitt **Überwachung des Registrierungszugriffs** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung des Registrierungszugriffs** wird geöffnet.
5. Klicken Sie im Abschnitt **Vorgänge zur Registrierung im folgenden Bereich überwachen** auf die Schaltfläche **Hinzufügen**.
6. Um im Fenster **Bereich der Überwachung des Registrierungszugriffs** einen Überwachungsbereich hinzuzufügen, geben Sie unter Verwendung der **unterstützten Masken** einen Pfad an.

Wenn Sie einen Pfad eingeben, können Sie `?` und `*` als Masken verwenden.

Stellen Sie sicher, dass Sie bei der Pfadangabe zu einem Stammregistrierungsschlüssel den vollständigen Pfad ohne Masken angeben, z. B. `HKEY_USERS`. Die folgende Liste enthält gültige Stammregistrierungsschlüssel:

- `HKEY_LOCAL_MACHINE`
- `HKLM`
- `HKEY_CURRENT_USER`
- `HKCU`
- `HKEY_USERS`
- `HKUS`
- `HKU`
- `HKEY_CURRENT_CONFIG`
- `HKEY_CLASSES_ROOT`
- `HKCR`

Vermeiden Sie beim Erstellen der Regeln die Verwendung von unterstützten Masken für die Stammschlüssel.
Wenn Sie nur einen Stammschlüssel, wie "HKEY_CURRENT_USER", oder einen Stammschlüssel mit einer Maske für alle untergeordneten Schlüssel, wie "HKEY_CURRENT_USER*", angeben, wird eine sehr große Menge an Nachrichten bezüglich der angegeben untergeordneten Schlüssel erstellt. Das führt zu verminderter Leistung. Wenn Sie einen Stammschlüssel, wie "HKEY_CURRENT_USER", oder einen Stammschlüssel mit einer Maske für alle untergeordneten Schlüssel, wie "HKEY_CURRENT_USER*", angeben und den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, ist das System nicht in der Lage, Schlüssel zu ändern oder auszulesen, die für das Funktionieren des Betriebssystems notwendig sind. Das führt zu einem nicht funktionsfähigen System.

7. Konfigurieren Sie auf der Registerkarte **Hinzufügen** die Liste der verfügbaren Vorgänge.

8. Wenn Sie bestimmte **Registrierungswerte** überwachen möchten, gehen Sie wie folgt vor:

   - Klicken Sie auf der Registerkarte **Registrierungswerte** auf die Schaltfläche **Hinzufügen**.
   - Geben Sie im Fenster **Regel für den Registrierungswert** die **Wertemaske** an und legen Sie die **Überwachte Vorgänge** fest.
   - Klicken Sie auf **OK**, um die Änderungen zu speichern.

9. Wenn Sie **Vertrauenswürdige Benutzer** angeben möchten, gehen Sie wie folgt vor:

   - Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

- Wählen Sie im Fenster **Benutzer oder Gruppen auswählen** die Benutzer oder Benutzergruppen aus, die zum Ausführen der angegebenen Vorgänge berechtigt sind.
- Klicken Sie auf **OK**, um die Änderungen zu speichern.

Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein und erstellt für sie kritische Ereignisse. Für vertrauenswürdige Benutzer werden Statistiken erstellt.

10. Klicken Sie im Fenster **Bereich der Überwachung des Registrierungszugriffs** auf **OK**.

Die angegebenen Einstellungen der Regeln gelten sofort im ausgewählten Überwachungsbereich der Aufgabe zur **Überwachung des Registrierungszugriffs**.

Überwachung des Registrierungszugriffs über die Verwaltungskonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung des Registrierungszugriffs über die Programmkonsole konfigurieren.

Einstellungen der Aufgabe zur Überwachung des Registrierungszugriffs anpassen

So konfigurieren Sie die Einstellungen der Überwachung des Registrierungszugriffs:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Überwachung des Registrierungszugriffs** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Überwachung des Registrierungszugriffs** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** erscheint.
4. Konfigurieren Sie im Fenster **Aufgabeneinstellungen** auf der Registerkarte **Allgemein** die folgenden Einstellungen:
   - Wählen Sie in der Gruppe **Aufgabenmodus** die benötigte Option von der Liste aus:
     - Vorgänge entsprechend den Regeln blockieren

       Wenn Sie den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, blockiert Kaspersky Embedded Systems Security die **Vorgänge**, die für den Überwachungsbereich festgelegt wurden. Wenn auch das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, blockiert Kaspersky Embedded Systems Security die unter **Vertrauenswürdige Zone** festgelegten Prozesse nicht.

       Standardmäßig wird der Modus **Nur Statistik** angewendet.

- Nur Statistik

  Wenn für den Überwachungsbereich der Modus **Nur Statistik** ausgewählt ist, erstellt Kaspersky Embedded Systems Security die Statistiken für die Registrierungsschlüssel entsprechend der festgelegten Regeln. Wenn auch das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, erstellt Kaspersky Embedded Systems Security keine Statistiken für die unter **Vertrauenswürdige Zone** festgelegten Prozesse.

  Standardmäßig wird der Modus **Nur Statistik** angewendet.

- Aktivieren oder deaktivieren Sie das Kontrollkästchen Vertrauenswürdige Zone anwenden entsprechend Ihren Bedürfnissen.

  Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **vertrauenswürdigen Prozesse** zusätzlich zur konfigurierten Regel auf den Überwachungsbereich angewendet.

  Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** deaktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **vertrauenswürdigen Prozesse** nicht auf den Überwachungsbereich angewendet.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

5. Passen Sie auf den Registerkarten **Zeitplan** und **Erweitert** den Zeitplan für den Aufgabenstart an.
6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben über Datum und Uhrzeit zur Veränderungen der Einstellungen werden im Systemaudit-Protokoll gespeichert.

Einstellungen der Überwachungsregeln anpassen

Die Überwachungsregeln werden nacheinander, entsprechend ihrer Reihenfolge in der Liste der konfigurierten Regeln, angewendet.

Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Überwachung des Registrierungszugriffs** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Überwachung des Registrierungszugriffs** auf den Knoten **Regeln der Überwachung des Registrierungszugriffs**.

   Das Fenster **Überwachung des Registrierungszugriffs** wird geöffnet.
4. Geben Sie im Fenster **Überwachung des Registrierungszugriffs**, unter **Systemregistrierungsschlüssel zur Überwachung hinzufügen**, einen Pfad unter Verwendung unterstützter Masken an, und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

Vermeiden Sie beim Erstellen der Regeln die Verwendung von unterstützten Masken für die Stammschlüssel.
Wenn Sie nur einen Stammschlüssel, wie "HKEY_CURRENT_USER", oder einen Stammschlüssel mit einer Maske für alle untergeordneten Schlüssel, wie "HKEY_CURRENT_USER*", angeben, wird eine sehr große Menge an Nachrichten bezüglich der angegeben untergeordneten Schlüssel erstellt. Das führt zu verminderter Leistung.
Wenn Sie einen Stammschlüssel, wie "HKEY_CURRENT_USER", oder einen Stammschlüssel mit einer Maske für alle untergeordneten Schlüssel, wie "HKEY_CURRENT_USER*", angeben und den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, ist das System nicht in der Lage, Schlüssel zu ändern oder auszulesen, die für das Funktionieren des Betriebssystems notwendig sind. Das führt zu einem nicht funktionsfähigen System.

5. Konfigurieren Sie auf der Registerkarte **Aktionen** die Liste der anwendbaren Vorgänge für den ausgewählten Überwachungsbereich.

6. Wenn Sie bestimmte **Registrierungswerte** überwachen möchten, gehen Sie wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Registrierungswerte** auf die Schaltfläche **Hinzufügen**.

   b. Geben Sie im Fenster **Regel für den Registrierungswert** die **Wertemaske** an und legen Sie die notwendigen **Überwachte Vorgänge** fest.

   c. Klicken Sie auf **OK**, um die Änderungen zu speichern.

7. Wenn Sie **Vertrauenswürdige Benutzer** angeben möchten, gehen Sie wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

   b. Wählen Sie im Fenster **Benutzer oder Gruppen auswählen** die Benutzer oder Benutzergruppen aus, die zum Ausführen der angegebenen Vorgänge berechtigt sind.

   c. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein und erstellt für sie kritische Ereignisse. Für vertrauenswürdige Benutzer werden Statistiken erstellt.

8. Klicken Sie im Fenster **Bereich der Überwachung des Registrierungszugriffs** auf **Speichern**.

   Die angegebenen Einstellungen der Regeln gelten sofort im ausgewählten Überwachungsbereich der Aufgabe zur **Überwachung des Registrierungszugriffs**.

Überwachung des Registrierungszugriffs über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie die Überwachung des Registrierungszugriffs über das Web-Plug-in konfigurieren.

Einstellungen der Aufgabe zur Überwachung des Registrierungszugriffs anpassen

So konfigurieren Sie die Aufgabe zur Überwachung des Registrierungszugriffs über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **System-Diagnose** aus.
5. Klicken Sie im Unterabschnitt **Überwachung des Registrierungszugriffs** auf **Einstellungen**.
6. Konfigurieren Sie im Fenster **Überwachung des Registrierungszugriffs** auf der Registerkarte **Einstellungen der Überwachung des Registrierungszugriffs** die folgenden Einstellungen:
   - Wählen Sie in der Gruppe **Aufgabenmodus** die benötigte Option von der Liste aus:
     - Vorgänge entsprechend den Regeln blockieren

       Wenn Sie den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, blockiert Kaspersky Embedded Systems Security die **Vorgänge**, die für den Überwachungsbereich festgelegt wurden. Wenn auch das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, blockiert Kaspersky Embedded Systems Security die unter **Vertrauenswürdige Zone** festgelegten Prozesse nicht.

       Standardmäßig wird der Modus **Nur Statistik** angewendet.

     - Nur Statistik

       Wenn für den Überwachungsbereich der Modus **Nur Statistik** ausgewählt ist, erstellt Kaspersky Embedded Systems Security die Statistiken für die Registrierungsschlüssel entsprechend der festgelegten Regeln. Wenn auch das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, erstellt Kaspersky Embedded Systems Security keine Statistiken für die unter **Vertrauenswürdige Zone** festgelegten Prozesse.

       Standardmäßig wird der Modus **Nur Statistik** angewendet.

   - Aktivieren oder deaktivieren Sie das Kontrollkästchen Vertrauenswürdige Zone anwenden entsprechend Ihren Bedürfnissen.

     Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** aktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **vertrauenswürdigen Prozesse** zusätzlich zur konfigurierten Regel auf den Überwachungsbereich angewendet.

     Wenn das Kontrollkästchen **Vertrauenswürdige Zone anwenden** deaktiviert ist, werden die in der **vertrauenswürdigen Zone** konfigurierten **vertrauenswürdigen Prozesse** nicht auf den Überwachungsbereich angewendet.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
7. Passen Sie auf der Registerkarte **Aufgabenverwaltung** den Zeitplan für den Aufgabenstart an.
8. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Kaspersky Embedded Systems Security übernimmt die neuen Einstellungen unmittelbar in der ausgeführten Aufgabe. Angaben über Datum und Uhrzeit zur Veränderungen der Einstellungen werden im Systemaudit-Protokoll gespeichert.

Einstellungen der Überwachungsregeln anpassen

Die Überwachungsregeln werden nacheinander, entsprechend ihrer Reihenfolge in der Liste der konfigurierten Regeln, angewendet.

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **System-Diagnose** aus.
5. Klicken Sie im Unterabschnitt **Überwachung des Registrierungszugriffs** auf **Einstellungen**.
6. Öffnen Sie im nächsten Fenster **Überwachung des Registrierungszugriffs** die Registerkarte **Einstellungen der Überwachung des Registrierungszugriffs**.
7. Klicken Sie im Abschnitt **Regeln der Überwachung des Registrierungszugriffs** auf **Hinzufügen**.
8. Geben Sie im Fenster **Bereich der Überwachung des Registrierungszugriffs** unter **Vorgänge zur Registrierung im folgenden Bereich überwachen** einen Pfad unter Verwendung der **unterstützten Masken** an.

Wenn Sie einen Pfad eingeben, können Sie `?` und `*` als Masken verwenden.

Stellen Sie sicher, dass Sie bei der Pfadangabe zu einem Stammregistrierungsschlüssel den vollständigen Pfad ohne Masken angeben, z. B. `HKEY_USERS`. Die folgende Liste enthält gültige Stammregistrierungsschlüssel:

- `HKEY_LOCAL_MACHINE`
- `HKLM`
- `HKEY_CURRENT_USER`
- `HKCU`
- `HKEY_USERS`
- `HKUS`
- `HKU`
- `HKEY_CURRENT_CONFIG`
- `HKEY_CLASSES_ROOT`
- `HKCR`

Vermeiden Sie beim Erstellen der Regeln die Verwendung von unterstützten Masken für die Stammschlüssel.
Wenn Sie nur einen Stammschlüssel, wie "HKEY_CURRENT_USER", oder einen Stammschlüssel mit einer Maske für alle untergeordneten Schlüssel, wie "HKEY_CURRENT_USER*", angeben, wird eine sehr große Menge an Nachrichten bezüglich der angegeben untergeordneten Schlüssel erstellt. Das führt zu verminderter Leistung.
Wenn Sie einen Stammschlüssel, wie "HKEY_CURRENT_USER", oder einen Stammschlüssel mit einer Maske für alle untergeordneten Schlüssel, wie "HKEY_CURRENT_USER*", angeben und den Modus **Vorgänge entsprechend den Regeln blockieren** auswählen, ist das System nicht in der Lage, Schlüssel zu ändern oder auszulesen, die für das Funktionieren des Betriebssystems notwendig sind. Das führt zu einem nicht funktionsfähigen System.

9. Konfigurieren Sie auf der Registerkarte **Aktionen** die Liste der anwendbaren Vorgänge für den ausgewählten Überwachungsbereich.

10. Wenn Sie bestimmte **Registrierungswerte** überwachen möchten, gehen Sie wie folgt vor:

    a. Klicken Sie auf der Registerkarte **Registrierungswerte** auf die Schaltfläche **Hinzufügen**.

    b. Geben Sie im Fenster **Regel für den Registrierungswert** die **Wertemaske** an und legen Sie die benötigte **Liste mit Vorgängen** fest.

    c. Klicken Sie auf **OK**, um die Änderungen zu speichern.

11. Wenn Sie **Vertrauenswürdige Benutzer** angeben möchten, gehen Sie wie folgt vor:

a. Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

b. Geben Sie den **Benutzername** ein oder klicken Sie auf **Als SID "Jeder" festlegen**, um die Benutzer festzulegen, welche die Berechtigung zum Ausführen der ausgewählten Vorgänge besitzen.

c. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Standardmäßig stuft Kaspersky Embedded Systems Security alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein und erstellt für sie kritische Ereignisse. Für vertrauenswürdige Benutzer werden Statistiken erstellt.

12. Klicken Sie im Fenster **Bereich der Überwachung des Registrierungszugriffs** auf **OK**, um die Änderungen zu speichern.

    Die angegebenen Einstellungen der Regeln gelten sofort im ausgewählten Überwachungsbereich der Aufgabe zur **Überwachung des Registrierungszugriffs**.

Protokollanalyse

Dieser Abschnitt enthält Informationen über die Aufgabe zur Protokollanalyse und die Aufgabeneinstellungen.

Über die Aufgabe Protokollanalyse

Während der Ausführung der Aufgabe zur Protokollanalyse überwacht Kaspersky Embedded Systems Security die Integrität der geschützten Umgebung auf Basis der Ergebnisse der Analyse der Windows-Ereignisprotokolle. Das Programm benachrichtigt den Administrator, wenn Anzeichen für untypisches Verhalten gefunden werden, die möglicherweise auf versuchte Cyberattacken hindeuten.

Kaspersky Embedded Systems Security analysiert die Daten der Windows-Ereignisprotokolle 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 vordefinierte Regeln anwenden, die auf bestehenden Heuristiken basieren. Die heuristische Analyse ermittelt das Vorhandensein von anomaler Aktivität auf dem geschützten Gerät, 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 jede 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 verwendet keine Heuristiken für die Analyse von Windows-Protokollen, wenn die heuristische Analyse nicht von der Aufgabe verwendet wird. Standardmäßig ist die heuristische Analyse aktiviert.

Beim Anwenden der Regeln protokolliert das Programm ein *Kritisches Ereignis* im Protokoll der Aufgabenausführung der Aufgabe zur Protokollanalyse.

Benutzerdefinierte Regeln der Aufgabe Protokollanalyse

Mithilfe der Einstellungen der Regeln 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 diese 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 in dieser Regel angegebene Ereignis-ID enthalten. Sie können IDs für jede angegebene Regel hinzufügen und löschen.

- Ereignisquelle

  Sie können für jede Regel ein Protokoll innerhalb des Windows-Ereignisprotokolls festlegen. Das Programm wird nur in diesem Protokoll nach Einträgen mit den angegebenen Ereignis-IDs suchen. Sie können eines der Standard-Protokolle (Programm, Sicherheit oder System) auswählen, oder ein benutzerdefiniertes Protokoll angeben, in dem Sie den Namen im Feld zur Auswahl der Quelle angeben.

  > Das Programm prüft nicht, ob das angegebene Protokoll tatsächlich im Windows-Ereignisprotokoll vorhanden ist.

Wenn die Regel ausgelöst wird, protokolliert Kaspersky Embedded Systems Security ein "Kritisches Ereignis" im Protokoll der Aufgabenausführung der Protokollanalyse.

Standardmäßig übernimmt die Aufgabe zur Protokollanalyse benutzerdefinierte Regeln.

> Bevor Sie die Aufgabe zur Protokollanalyse starten, vergewissern Sie sich, dass die Systemaudit-Richtlinie korrekt eingerichtet ist. Weitere Informationen finden Sie in dem Microsoft-Artikel.

Standardeinstellungen der Aufgabe "Protokollanalyse"

Die Aufgabe zur Protokollanalyse weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Standardeinstellungen der Aufgabe "Protokollanalyse"

Einstellung	Standardwert	Beschreibung
Benutzerdefinierte Regeln für die Protokollanalyse verwenden	Wird nicht verwendet.	Sie können die benutzerdefinierten Regeln aktivieren, deaktivieren, hinzufügen oder ändern.
Vorkonfigurierte Regeln für die Protokollanalyse verwenden	Wird verwendet	Sie können die heuristische Analyse zur Erkennung von anomaler Aktivität auf dem geschützten Gerät aktivieren oder deaktivieren.
Verarbeitung von Brute-Force	10 Anmeldefehler pro 300 Sekunden.	Sie können die Anzahl der Versuche sowie den Zeitraum angeben, die als Auslösekriterien der heuristischen Analyse dienen sollen.
Netzwerkanmeldung	00:00:00 Uhr.	Sie können den Anfang und das Ende der Zeitspanne angeben, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.
Ausnahmen	Wird nicht	Sie können Benutzer und IP-Adressen angeben, die keine

	verwendet.	heuristische Analyse auslösen.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Regeln für die Protokollanalyse über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie Regeln für die Protokollanalyse über das Verwaltungs-Plug-in hinzufügen und konfigurieren.

Regeln für vorkonfigurierte Aufgaben anpassen

Um die vorkonfigurierten Regeln für die Aufgabe zur Protokollanalyse anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie Programmeinstellungen konfigurieren möchten.
3. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Aufgabeneinstellungen für eine Gruppe von geschützten Geräten anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Einstellungen: <Name der Richtlinie>**.
   - Um die Programmeinstellungen für ein einzelnes geschütztes Gerät anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen**.

     Wenn auf ein Gerät eine aktive Richtlinie von Kaspersky Security Center angewendet wird und diese Änderungen an Programmeinstellungen blockiert, dann können diese Einstellungen im Fenster **Programmeinstellungen** nicht bearbeitet werden.
4. Klicken Sie im Abschnitt **System-Diagnose** im Unterabschnitt **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.
5. Wählen Sie die Registerkarte **Vorkonfigurierte Regeln** aus.
6. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Vorkonfigurierte Regeln für die Protokollanalyse verwenden**.

   Für die Ausführung der Aufgabe muss zumindest eine Regel für die Protokollanalyse ausgewählt sein.
7. Wählen Sie aus der Liste der vorkonfigurierten Regeln jene Regeln aus, die Sie für die Protokollanalyse verwenden möchten:
   - Ein möglicher Versuch, das Kennwort anhand von Brute-Force zu knacken, wurde entdeckt
   - Anzeichen für eine Gefährdung der Windows-Protokolle wurden gefunden

- Verdächtige Aktivitäten des neu installierten Dienstes wurden gefunden
- Eine verdächtige Authentifizierung mit eindeutiger Angabe von Anmeldedaten wurde gefunden
- Anzeichen für den Angriff Kerberos forged PAC (MS14-068) wurden gefunden
- Verdächtige Veränderungen in der privilegierten Gruppe Administratoren wurden gefunden
- Verdächtige Aktivitäten während der Anmeldesitzung im Netzwerk wurden gefunden

8. Um die ausgewählten Regeln anzupassen, klicken Sie auf die Schaltfläche **Erweiterte Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

9. Geben Sie im Abschnitt **Verarbeitung von Brute-Force** die Anzahl der Versuche sowie den Zeitraum an, in dem die Versuche ausgeführt wurden, die als Auslösekriterien der heuristischen Analyse dienen sollen.

10. Geben Sie im Abschnitt **Netzwerk-Anmeldungserkennung** den Anfang und das Ende der Zeitspanne an, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.

11. Wählen Sie die Registerkarte **Ausnahmen** aus.

12. Um Benutzer hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:

    a. Klicken Sie auf die Schaltfläche **Durchsuchen**.

    b. Wählen Sie einen Benutzer aus.

    c. Klicken Sie auf **OK**.

    Der angegebene Benutzer wird zur Liste der vertrauenswürdigen Benutzer hinzugefügt.

13. Um IP-Adressen hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:

    a. Geben Sie die IP-Adresse ein.

    b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

14. Die angegebene IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.

15. Passen Sie auf der Registerkarte **Aufgabenverwaltung** den Zeitplan für den Aufgabenstart an.

16. Klicken Sie im Fenster **Protokollanalyse** auf **OK**.

Die Einstellungen der Aufgabe zur Protokollanalyse werden gespeichert.

Regeln für die Protokollanalyse über das Verwaltungs-Plug-in hinzufügen

Um eine neue benutzerdefinierte Regel für die Protokollanalyse hinzuzufügen und anzupassen, gehen Sie wie folgt vor:

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

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

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

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

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

4. Klicken Sie im Abschnitt **System-Diagnose** im Unterabschnitt **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

5. Deaktivieren oder aktivieren Sie auf der Registerkarte **Benutzerdefinierte Regeln** das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Sie können kontrollieren, ob die vordefinierten Regeln für die Protokollanalyse übernommen werden. Aktivieren Sie die Kontrollkästchen neben den Regeln, die Sie für die Protokollanalyse übernehmen möchten.

6. Um eine neue benutzerdefinierte Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Benutzerdefinierte Regel für die Protokollanalyse** wird geöffnet.

7. Geben Sie im Abschnitt **Allgemein** die folgenden Daten der neuen Regel an:

   - **Regelname**
   - **Die Regel wird beim Erkennen neuer Einträge im Windows-Ereignisprotokoll ausgelöst, wenn der angegebene Identifikator (ID) in den Ereignisparametern gefunden wird**

8. Geben Sie im Abschnitt **Auslösekriterium** die ID der Einträge an, durch welche die Regel ausgelöst wird:

   a. Geben Sie eine ID ein.

   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Die eingegebene Ereignis-ID wird zur Liste hinzugefügt. Sie können zu jeder Regel eine unbegrenzte Anzahl von IDs hinzufügen.

9. Klicken Sie auf **OK**.

   Die Regel für die Protokollanalyse wird zur allgemeinen Regelliste hinzugefügt.

Regeln für die Protokollanalyse über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie Regeln für die Protokollanalyse über die Programmkonsole hinzufügen und konfigurieren.

Regeln für vorkonfigurierte Aufgaben anpassen

Um die Einstellungen der heuristischen Analyse für die Aufgabe zur Protokollanalyse anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Protokollanalyse** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Protokollanalyse** auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
4. Wählen Sie die Registerkarte **Vorkonfigurierte Regeln** aus.
5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Vorkonfigurierte Regeln für die Protokollanalyse verwenden**.

   Für die Ausführung der Aufgabe muss zumindest eine Regel für die Protokollanalyse ausgewählt sein.
6. Wählen Sie aus der Liste der vorkonfigurierten Regeln jene Regeln aus, die Sie für die Protokollanalyse verwenden möchten:
   - Ein möglicher Versuch, das Kennwort anhand von Brute-Force zu knacken, wurde entdeckt
   - Anzeichen für eine Gefährdung der Windows-Protokolle wurden gefunden
   - Verdächtige Aktivitäten des neu installierten Dienstes wurden gefunden
   - Eine verdächtige Authentifizierung mit eindeutiger Angabe von Anmeldedaten wurde gefunden
   - Anzeichen für den Angriff Kerberos forged PAC (MS14-068) wurden gefunden
   - Verdächtige Veränderungen in der privilegierten Gruppe Administratoren wurden gefunden
   - Verdächtige Aktivitäten während der Anmeldesitzung im Netzwerk wurden gefunden
7. Um die Einstellungen der ausgewählten Regeln anzupassen, klicken Sie auf die Registerkarte **Zusätzlich**.
8. Geben Sie im Abschnitt **Verarbeitung von Brute-Force** die Anzahl der Versuche sowie den Zeitraum an, in dem die Versuche ausgeführt wurden, die als Auslösekriterien der heuristischen Analyse dienen sollen.
9. Geben Sie im Abschnitt **Netzwerkanmeldung** den Anfang und das Ende der Zeitspanne an, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.
10. Wählen Sie die Registerkarte **Ausnahmen** aus.
11. Um Benutzer hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Klicken Sie auf die Schaltfläche **Durchsuchen**.
    b. Wählen Sie einen Benutzer aus.

c. Klicken Sie auf **OK**.

Der angegebene Benutzer wird zur Liste der vertrauenswürdigen Benutzer hinzugefügt.

12. Um IP-Adressen hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:

a. Geben Sie die IP-Adresse ein.

b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Die angegebene IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.

13. Wählen Sie die Registerkarten **Zeitplan** und **Erweitert** aus, um den Zeitplan für den Aufgabenstart anzupassen.

14. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Die Einstellungen der Aufgabe zur Protokollanalyse werden gespeichert.

Regeln für die Protokollanalyse über die Programmkonsole hinzufügen

So fügen Sie eine neue benutzerdefinierte Regel für die Protokollanalyse hinzu und konfigurieren sie:

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie darin den untergeordneten Knoten **Protokollanalyse** aus.
3. Klicken Sie im Ergebnisbereich des Knotens **Protokollanalyse** auf den Link **Regeln für die Protokollanalyse**.
4. Das Fenster **Regeln für die Protokollanalyse** wird geöffnet.
5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse anwenden. Bei deaktiviertem Kontrollkästchen werden die Einstellungen der Regeln nicht angewendet** angezeigt.

> Sie können kontrollieren, ob die vordefinierten Regeln für die Protokollanalyse übernommen werden. Aktivieren Sie die Kontrollkästchen neben den Regeln, die Sie für die Protokollanalyse übernehmen möchten.

6. So erstellen Sie eine neue benutzerdefinierte Regel:

a. Geben Sie den Namen der neuen Regel ein.

b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Die erstellte Regel wird zur allgemeinen Regelliste hinzugefügt.

7. Um eine Regel zu konfigurieren:

a. Wählen Sie eine Regel aus der Liste aus.

Im rechten Bereich des Fensters werden auf der Registerkarte **Beschreibung** allgemeine Informationen über die Regel angezeigt.

> Die Beschreibung für eine neue Regel ist leer.

b. Wählen Sie die Registerkarte **Regelbeschreibung** aus.

8. Geben Sie im Abschnitt **Allgemein** die folgenden Daten der neuen Regel an:

   - **Regelname**
   - **Protokollname**
   - **Die Regel wird beim Erkennen neuer Einträge im Windows-Ereignisprotokoll ausgelöst, wenn der angegebene Identifikator (ID) in den Ereignisparametern gefunden wird**

9. Geben Sie im Abschnitt **Ereignis-IDs** die IDs der Einträge an, durch welche die Regel ausgelöst wird:

   a. Geben Sie eine Ereignis-ID ein.

   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die eingegebene Ereignis-ID wird zur Liste hinzugefügt. Sie können zu jeder Regel eine unbegrenzte Anzahl von IDs hinzufügen.

10. Klicken Sie auf die Schaltfläche **Speichern**.

Die festgelegten Einstellungen der Regeln für die Protokollanalyse werden angewendet.

Regeln für die Protokollanalyse über das Web-Plug-in verwalten

So fügen Sie Regeln für die Protokollanalyse über das Web-Plug-in hinzu und konfigurieren sie:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **System-Diagnose** aus.
5. Klicken Sie im Unterabschnitt **Protokollanalyse** auf **Einstellungen**.
6. Konfigurieren Sie die in der folgenden Tabelle aufgeführten Einstellungen.

Einstellungen der Aufgabe "Protokollanalyse"

Einstellung	Beschreibung
Benutzerdefinierte Regeln für die Protokollanalyse verwenden	Sie können die benutzerdefinierten Regeln aktivieren, deaktivieren, hinzufügen oder ändern. Die Einstellung wird in der Tabelle mit der Liste der benutzerdefinierten Regeln aufgeführt.
Vorkonfigurierte Regeln für die Protokollanalyse verwenden	Sie können die heuristische Analyse zur Erkennung von anomaler Aktivität auf dem geschützten Gerät aktivieren oder deaktivieren. Die Einstellung wird in der Tabelle mit der Liste der benutzerdefinierten Regeln aufgeführt.
Erfolglose Versuche der Kennworteingabe als Brute-Force-	Sie können die Anzahl der Versuche sowie den Zeitraum angeben, die als Auslösekriterien der heuristischen Analyse

Angriff ansehen, wenn sie mit der angegebenen Häufigkeit geschehen	dienen sollen.
Netzwerkanmeldungen im folgenden Zeitraum erkennen	Sie können den Anfang und das Ende der Zeitspanne angeben, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Embedded Systems Security als anomale Aktivität betrachtet wird.
Ausgeschlossene Benutzer	Sie können Benutzer angeben, die keine heuristische Analyse auslösen.
Ausgeschlossene IP-Adressen	Sie können IP-Adressen angeben, die keine heuristische Analyse auslösen.
Aufgabenverwaltung	Sie können die Einstellungen anpassen, sodass die Aufgaben nach einem Zeitplan ausgeführt werden.

Untersuchung auf Befehl

Dieser Abschnitt enthält Informationen über die Aufgaben zur Untersuchung auf Befehl und erläutert das Anpassen der Aufgaben zur Untersuchung auf Befehl und der Sicherheitseinstellungen des geschützten Geräts.

Über Aufgaben zur Untersuchung auf Befehl

Kaspersky Embedded Systems Security untersucht den angegebenen Bereich auf Viren und andere Bedrohungen der Computersicherheit. Kaspersky Embedded Systems Security überprüft Daten des geschützten Geräts, den Arbeitsspeicher sowie Autostart-Objekte.

Kaspersky Embedded Systems Security enthält die folgenden Aufgaben zur Untersuchung auf Befehl:

- Die Aufgabe Untersuchung beim Hochfahren des Betriebssystems wird jedes Mal ausgeführt, wenn Kaspersky Embedded Systems Security gestartet wird. Kaspersky Embedded Systems Security untersucht die Bootsektoren und Master-Bootsektoren der Festplatten, Wechseldatenträger, Systemspeicher und Prozess-Speicher. Jedes Mal, wenn Kaspersky Embedded Systems Security die Aufgabe ausführt, wird eine Kopie der nicht infizierten Bootsektoren erstellt. Wenn eine Bedrohung in diesen Abschnitten gefunden wird, wenn die Aufgabe das nächste Mal ausgeführt wird, werden diese durch die Backup-Kopie ersetzt.

  > Es ist möglich, dass die Aufgabe zur Untersuchung beim Hochfahren des Betriebssystems nicht ausgeführt wird, wenn das geschützte Gerät aus einem Sleep- oder Hibernate-Modus gestartet wird. Auf geschützten Geräten wird die Aufgabe nur ausgeführt, wenn das Gerät neu startet oder in einem komplett ausgeschalteten Zustand gestartet wird.

- Die Aufgabe Untersuchung wichtiger Bereiche wird standardmäßig wöchentlich nach Zeitplan ausgeführt. Kaspersky Embedded Systems Security untersucht Objekte, die sich in kritischen Bereichen des Betriebssystems befinden: Autostart-Objekte, Bootsektoren und Master-Bootsektoren von Festplatten und Wechseldatenträgern, Systemspeicher und Prozess-Speicher. Das Programm untersucht Dateien in Systemordnern, z. B. %windir%\system32. Kaspersky Embedded Systems Security verwendet die Sicherheitseinstellungen, die der Sicherheitsstufe "Empfohlen" entsprechen. Sie können die Parameter für die Aufgabe Untersuchung wichtiger Bereiche ändern.

- Die Aufgabe Untersuchung von Quarantäne-Objekten wird standardmäßig jedes Mal nach dem Update der Programm-Datenbanken nach Zeitplan ausgeführt. Sie können den Umfang der Aufgabe "Untersuchung von Quarantäne-Objekten" nicht ändern.

- Die Aufgabe "Integritätsprüfung für Programme" wird täglich ausgeführt. Sie gewährleistet die Untersuchung der Module von Kaspersky Embedded Systems Security auf Beschädigungen oder Änderungen. Es wird der Installationsordner des Programms geprüft. Die Statistiken über die Aufgabenausführung geben Auskunft über die Anzahl der geprüften Module und die Anzahl der als beschädigt bewerteten Module. Die Parameterwerte einer Aufgabe werden vom Programm vorgegeben und lassen sich nicht ändern. Die Einstellungen im Zeitplan für den Aufgabenstart lassen sich dagegen für so eine Aufgabe ändern.

Zusätzlich können Sie benutzerdefinierte Aufgaben zur Untersuchung auf Befehl erstellen, beispielsweise eine Aufgabe zur Untersuchung freigegebener Ordner auf dem geschützten Gerät.

Kaspersky Embedded Systems Security kann gleichzeitig mehrere Aufgaben zur Untersuchung auf Befehl ausführen.

Über den Untersuchungsbereich von Aufgaben und Sicherheitseinstellungen

In der Programmkonsole wird der Untersuchungsbereich der ausgewählten Aufgabe zur Untersuchung auf Befehl als Struktur oder Liste jener Dateiressourcen des geschützten Geräts dargestellt, die von Kaspersky Embedded Systems Security überwacht werden können. Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Geräts als Liste angezeigt.

Im Verwaltungs-Plug-in steht nur die Listenansicht zur Verfügung.

Um freigegebene Netzwerkordner in der Programmkonsole in der Baumstruktur anzuzeigen, gehen Sie wie folgt vor:

Wählen Sie im linken unteren Teil des Einstellungsfensters **Untersuchungsbereich - Einstellungen** aus der Dropdown-Liste den Punkt **Als Baumstruktur anzeigen**.

Die Elemente oder Knoten werden in einer Listenansicht oder in einer Baumstruktur der Dateiressourcen des geschützten Geräts auf folgende Weise dargestellt:

☑ Der Knoten gehört zum Untersuchungsbereich.

☐ Der Knoten gehört nicht zum Untersuchungsbereich.

☑ Mindestens ein diesem Knoten untergeordneter Knoten gehört nicht zum Untersuchungsbereich oder die Sicherheitsparameter des oder der untergeordneten Knoten unterscheiden sich von den Sicherheitsparametern dieses Knotens (nur für die Baumstruktur-Ansicht).

Das Symbol ☑ wird angezeigt, wenn alle untergeordneten Knoten ausgewählt sind, nicht jedoch der übergeordnete Knoten. In diesem Fall werden Änderungen der Datei- und Ordnerzusammensetzung des übergeordneten Knotens bei der Einrichtung eines Untersuchungsbereichs für den ausgewählten untergeordneten Knoten nicht automatisch berücksichtigt.

Mithilfe der Programmkonsole können Sie auch virtuelle Festplatten zum Untersuchungsbereich hinzufügen. Die Namen von virtuellen Nodes werden in blauer Schrift dargestellt.

Parameter für Sicherheit

In der ausgewählten Aufgabe zur Untersuchung auf Befehl können Sie die standardmäßigen Sicherheitseinstellungen ändern. Dabei können Sie entweder einheitliche Werte für den gesamten Schutzbereich bzw. Untersuchungsbereich oder individuelle Werte für bestimmte Knoten oder Elemente der Struktur oder Liste der Ressourcen des Geräts festlegen.

Die Sicherheitseinstellungen, die für den ausgewählten übergeordneten Knoten konfiguriert wurden, werden automatisch für alle untergeordneten Knotens übernommen. Die Sicherheitseinstellungen des übergeordneten Knotens werden für untergeordnete Knoten, die gesondert konfiguriert werden, nicht übernommen.

Sie können die Parameter eines ausgewählten Schutzbereichs bzw. Untersuchungsbereichs auf eine der folgenden Weisen anpassen:

- durch Auswahl einer der drei vordefinierten Sicherheitsstufen (**Maximale Leistung**, **Empfohlen** oder **Maximale Sicherheit**).
- Durch manuelle Änderung der Sicherheitseinstellungen für die ausgewählten Knoten oder Elemente in der Struktur oder Liste der Dateiressourcen des geschützten Geräts (die Sicherheitsstufe nimmt den Wert **Benutzerdefiniert** an).

Sie können den Parametersatz eines Knotens in einer Vorlage speichern, um diese Vorlage später für andere Knoten zu übernehmen.

Vordefinierte Untersuchungsbereiche

Die Liste oder Dateistruktur des geschützten Geräts wird der ausgewählten Aufgabe zur Untersuchung auf Befehl wird im Fenster **Untersuchungsbereich - Einstellungen** angezeigt.

Die Dateistruktur oder Liste der Dateiressourcen zeigt die Knoten an, für die Sie nach den Sicherheitseinstellungen in Microsoft Windows über Leserechte verfügen.

Kaspersky Embedded Systems Security enthält die folgenden vordefinierten Untersuchungsbereiche:

- **Arbeitsplatz**. Kaspersky Embedded Systems Security untersucht das gesamte geschützte Gerät.
- **Lokale Festplatten**. Kaspersky Embedded Systems Security untersucht Objekte auf den Festplatten des geschützten Geräts. Sie können alle Festplatten sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.
- **Wechseldatenträger**. Kaspersky Embedded Systems Security untersucht Dateien auf externen Geräten, z. B. auf CDs oder Wechseldatenträgern. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.
- **Netzwerkumgebung**. Sie können dem Untersuchungsbereich Netzwerkordner oder Dateien hinzufügen, indem Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) angeben. Das für den Aufgabenstart verwendete Benutzerkonto muss über Zugriffsrechte für die hinzugefügten Netzwerkordner oder Dateien verfügen. Standardmäßig werden die Aufgaben zur Untersuchung auf Befehl unter dem Systemkonto ausgeführt.

  Verbundene Netzlaufwerke werden nicht in der Dateistruktur des geschützten Geräts angezeigt. Um Objekte auf einem Netzlaufwerk in den Untersuchungsbereich aufzunehmen, geben Sie den Pfad des Ordners an, der dem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

- **Systemspeicher**. Kaspersky Embedded Systems Security untersucht ausführbare Dateien und Module von Prozessen, die während der Untersuchung im Betriebssystem ausgeführt werden.
- **Autostart-Objekte**. Kaspersky Embedded Systems Security untersucht Objekte, auf die sich Registrierungsschlüssel und Konfigurationsdateien beziehen, beispielsweise WIN.INI oder SYSTEM.INI, sowie die Programm-Module, die beim Hochfahren des geschützten Geräts automatisch gestartet werden.
- **Freigegebene Ordner**. Sie können die freigegebenen Ordner auf dem geschützten Gerät in den Untersuchungsbereich einschließen.
- **Virtuelle Festplatten**. Sie können in den Untersuchungsbereich dynamische Laufwerke, Ordner und Dateien sowie Laufwerke aufnehmen, die auf dem geschützten Gerät eingebunden werden, z. B. gemeinsame Cluster-Laufwerke.

Virtuelle Laufwerke, die mit dem Befehl SUBST erzeugt wurden, werden in der Dateistruktur des geschützten Geräts in der Programmkonsole nicht angezeigt. Um Objekte auf einer virtuellen Festplatte zu untersuchen, nehmen Sie den Ordner auf dem geschützten Gerät, mit dem die virtuelle Festplatte verbunden ist, in den Untersuchungsbereich auf.

Die vordefinierten Untersuchungsbereiche werden standardmäßig in der Struktur der freigegebenen Netzwerkordner des Computers angezeigt und sind zum Hinzufügen in die Liste der Dateiressourcen bei ihrer Erstellung in den Einstellungen des Untersuchungsbereichs verfügbar.

Standardmäßig werden die Aufgaben zur Untersuchung auf Befehl in den folgenden Bereichen ausgeführt:

- Aufgabe zur Untersuchung beim Hochfahren des Betriebssystems:
  - **Lokale Festplatten**
  - **Wechseldatenträger**
  - **Systemspeicher**
- Untersuchung wichtiger Bereiche:
  - **Lokale Festplatten** (mit Ausnahme der Windows-Ordner)
  - **Wechseldatenträger**
  - **Systemspeicher**
  - **Autostart-Objekte**
- Andere Aufgaben:
  - **Lokale Festplatten** (mit Ausnahme der Windows-Ordner)
  - **Wechseldatenträger**
  - **Systemspeicher**
  - **Autostart-Objekte**
  - **Freigegebene Ordner**

Untersuchung von Online-Speicherdateien

Über Cloud-Dateien

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

Kaspersky Embedded Systems Security unterstützt keine anderen Online-Speicher.

OneDrive Files On-Demand ermöglicht Ihnen den Zugriff auf all Ihre OneDrive-Dateien, ohne dass sie heruntergeladen werden müssen und Speicherplatz auf Ihrem Gerät belegen. Sie können die Dateien bei Bedarf auf Ihre Festplatte herunterladen.

Wenn die Funktion "OneDrive Files On-Demand" aktiviert ist, werden im Datei-Explorer neben jeder Datei in der Spalte **Status** Statussymbole angezeigt. Jede Datei besitzt eine der folgenden Statusvarianten:

Dieses Statussymbol zeigt an, dass die Datei *nur online verfügbar* ist. Dateien, die nur online verfügbar sind, werden nicht physisch auf Ihrer Festplatte gespeichert. Sie können Dateien, die nur online verfügbar sind, nicht öffnen, wenn Ihr Gerät keine Internetverbindung hat.

Dieses Statussymbol zeigt an, dass die Datei *lokal verfügbar* ist. Dies ist der Fall, wenn Sie eine nur online verfügbare Datei öffnen und auf Ihr Gerät herunterladen. Sie können eine lokal verfügbare Datei jederzeit auch ohne Internetzugang öffnen. Um Speicherplatz freizugeben, können Sie die Datei wieder nur online verfügbar machen ( ).

Dieses Statussymbol zeigt an, dass die Datei *auf Ihrer Festplatte gespeichert und immer verfügbar* ist.

Untersuchung von Cloud-Dateien

Kaspersky Embedded Systems Security kann nur Cloud-Dateien untersuchen, die lokal auf einem geschützten Gerät gespeichert sind. Solche OneDrive-Dateien besitzen die Status und . Die Dateien mit dem Status werden bei der Untersuchung übersprungen, da sie sich nicht physisch auf dem geschützten Gerät befinden.

> Kaspersky Embedded Systems Security lädt Dateien mit dem Status während der Untersuchung nicht automatisch aus der Cloud herunter, selbst wenn sie zum Untersuchungsbereich gehören.

Cloud-Dateien werden je nach Aufgabetyp von mehreren Aufgaben von Kaspersky Embedded Systems Security in unterschiedlichen Szenarien verarbeitet:

- Untersuchung von Cloud-Dateien in Echtzeit: Sie können Ordner mit Cloud-Dateien zum Schutzbereich der Aufgabe "Echtzeitschutz für Dateien" hinzufügen. Eine Datei wird untersucht, wenn der Benutzer auf sie zugreift. Wenn der Benutzer auf eine Datei mit dem Status zugreift, wird sie heruntergeladen und lokal verfügbar gemacht und ihr Status wechselt zu . So kann die Datei von der Aufgabe "Echtzeitschutz für Dateien" verarbeitet werden.

- Untersuchung von Cloud-Dateien auf Befehl: Sie können Ordner mit Cloud-Dateien zum Untersuchungsbereich der Aufgabe "Untersuchung auf Befehl" hinzufügen. Die Aufgabe untersucht Dateien mit dem Status und . Wenn Dateien mit dem Status im Untersuchungsbereich gefunden werden, werden sie bei der Untersuchung übersprungen. Im Protokoll der Aufgabenausführung wird ein informatives Ereignis gespeichert, das darauf hinweist, dass die untersuchte Datei nur ein Platzhalter für eine Cloud-Datei ist und nicht auf einer lokalen Festplatte verfügbar ist.

- Erstellung und Verwendung der Regeln für die Programmkontrolle: Sie können für Dateien mit dem Status und mithilfe der Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts Erlaubnisregeln und Verbotsregeln erstellen. Die Aufgabe zur Kontrolle des Programmstarts wendet das Prinzip des standardmäßigen Verbots (Default Deny) an und erstellt Regeln zum Verarbeiten und Blockieren von Cloud-Dateien.

  > Die Aufgabe zur Kontrolle des Programmstarts blockiert den Start aller Cloud-Dateien unabhängig von ihrem Status. Dateien mit dem Status werden nicht in den Gültigkeitsbereich der Erstellung von Regeln aufgenommen, da sie nicht physisch auf Ihrer Festplatte gespeichert sind. Da für solche Dateien keine Erlaubnisregeln erstellt werden können, gilt für sie das Prinzip des standardmäßigen Verbots (Default Deny).

Wenn in einer OneDrive Cloud-Datei eine Bedrohung gefunden wird, wendet das Programm die Aktion an, die in den Einstellungen der Aufgabe festgelegt ist, welche die Untersuchung ausführt. Auf diese Weise kann die Datei gelöscht, desinfiziert, in Quarantäne oder ins Backup verschoben werden.

Änderungen an lokalen Dateien werden mit den in OneDrive gespeicherten Kopien synchronisiert, wobei die Prinzipien zur Anwendung kommen, die in der entsprechenden Dokumentation zu Microsoft OneDrive beschrieben sind.

Über vordefinierte Sicherheitsstufen

Die Sicherheitseinstellungen **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden**, **Heuristische Analyse verwenden** und **Dateien auf Microsoft-Signatur überprüfen** gehören nicht zu den Einstellungen für die vordefinierten Sicherheitsstufen. Wenn sich die Einstellungen **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden**, **Heuristische Analyse verwenden** und **Dateien auf Microsoft-Signatur überprüfen** ändern, ändert sich die von Ihnen gewählte vordefinierte Sicherheitsstufe nicht.

Sie können eine der folgenden drei vordefinierten Sicherheitsstufen für einen in der Baumstruktur der Dateiressourcen des Geräts ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen** oder **Maximale Sicherheit**. Jede dieser Stufen besitzt eigene vordefinierte Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird empfohlen, wenn Ihr Netzwerk über zusätzliche Sicherheitsmaßnahmen verfügt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien, die über die Verwendung von Kaspersky Embedded Systems Security auf geschützten Geräten hinausgehen.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Geräte. Die Experten von Kaspersky empfehlen diese Stufe als ausreichenden Schutz von Geräten in den meisten Unternehmensnetzwerken. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximale Sicherheit

Die Sicherheitsstufe **Maximale Sicherheit** wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Gerätesicherheit hat.

Vordefinierte Sicherheitsstufen und entsprechende Werte für die Sicherheitsparameter

Einstellungen	Sicherheitsstufe		
	Maximale Leistung	**Empfohlen**	**Maximale Sicherheit**
Objekte untersuchen	Nach Format	Alle Objekte	Alle Objekte
Nur neue und veränderte Dateien untersuchen	Aktiviert	Deaktiviert	Deaktiviert
Aktion für infizierte und	Desinfizieren.	Empfohlene Aktion ausführen	Desinfizieren.

andere Objekte	Irreparable Objekte löschen	(Desinfizieren. Irreparable Objekte löschen)	Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte	Quarantäne	Empfohlene Aktion ausführen (Quarantäne)	Quarantäne
Dateien ausschließen	Nein	Nein	Nein
Nicht erkennen	Nein	Nein	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	60 Sek.	Nein	Nein
Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)	8 MB	Nein	Nein
Alternative NTFS-Ströme	Ja	Ja	Ja
Bootsektoren und MBR	Ja	Ja	Ja
Zusammengesetzte Objekte untersuchen	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Alle Objekte	• Archive* • SFX-Archive* • E-Mail-Datenbanken* • Dateien in Mail-Formaten* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Alle Objekte

Über die Untersuchung von Wechseldatenträgern

Sie können die Untersuchung von Wechseldatenträgern anpassen, die über USB an das geschützte Gerät angeschlossen werden.

Kaspersky Embedded Systems Security führt die Untersuchung von Wechseldatenträgern mithilfe der Aufgabe Untersuchung auf Befehl aus. Das Programm erstellt automatisch eine neue Aufgabe zur Untersuchung auf Befehl, wenn ein Wechseldatenträger angeschlossen wird, und löscht die erstellte Aufgabe nach Abschluss der Untersuchung. Die erstellte Aufgabe wird mit der vordefinierten Sicherheitsstufe ausgeführt, die für die Untersuchung von Wechseldatenträgern festgelegt wurde. Sie können die Einstellungen der vorübergehenden Aufgabe zur Untersuchung auf Befehl nicht anpassen.

Wenn Sie Kaspersky Embedded Systems Security ohne Antiviren-Datenbanken installiert haben, ist die Untersuchung von Wechseldatenträgern nicht verfügbar.

Kaspersky Embedded Systems Security startet die Untersuchung von Wechseldatenträgern, wenn diese im Betriebssystem als externe USB-Geräte registriert werden. Das Programm führt keine Untersuchung des Wechseldatenträgers durch, wenn sein Anschluss von der Aufgabe zur Gerätekontrolle blockiert wird. Das Programm führt keine Untersuchung von MTP-Mobilgeräten durch.

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

Die Ergebnisse der Untersuchung jedes Wechseldatenträgers werden im Protokoll der Aufgabe "Untersuchung auf Befehl" gespeichert, wenn der jeweilige Datenträger angeschlossen wird.

Sie können die Einstellungswerte der Komponente Wechseldatenträger untersuchen bearbeiten (s. Tabelle unten).

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 das geschützte Gerät aktivieren und deaktivieren.
Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)	8192 MB	Sie können den Bereich, in dem die Komponente aktiviert wird, reduzieren, indem Sie die Höchstmenge der Daten auf dem Wechseldatenträger angeben. Kaspersky Embedded Systems Security wird einen Wechseldatenträger nicht untersuchen, wenn die Menge der darauf gespeicherten Daten den angegebenen Wert übersteigt.
Untersuchung starten mit Sicherheitsstufe	Maximale Sicherheit	Sie können die Einstellungen der zu erstellenden Aufgaben zur Untersuchung auf Befehl anpassen, indem Sie eine der folgenden drei Sicherheitsstufen wählen: • **Maximale Sicherheit** • **Empfohlen** • **Maximale Leistung** Der Algorithmus der Aktionen beim Entdecken infizierter, möglicherweise infizierter und anderer Objekte, sowie andere Untersuchungseinstellungen für jede Sicherheitsstufe entsprechen den vorinstallierten Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl.

Über die Aufgabe zur Überwachung der Baseline-Integrität

Während der Aufgabe zur Überwachung der Baseline-Integrität überprüft Kaspersky Embedded Systems Security keine gesperrten Dateien, Ordner, Dateiverknüpfungen und Cloud-Dateien.

Die Aufgabe zur Überwachung der Baseline-Integrität überwacht die Integrität von Dateien im Überwachungsbereich, indem der Hash der Dateien (MD5-Hash oder SHA256-Hash) mit einer Baseline verglichen wird.

Bei der ersten Ausführung der Aufgabe zur Überwachung der Baseline-Integrität erstellt Kaspersky Embedded Systems Security eine Baseline, indem Hash-Werte für Dateien im Überwachungsbereich der Aufgabe berechnet und gespeichert werden. Wenn der Überwachungsbereich einer Aufgabe zur Überwachung der Baseline-Integrität geändert wurde, aktualisiert Kaspersky Embedded Systems Security die Baseline für die nächste Aufgabe zur Überwachung der Baseline-Integrität, indem Hash-Werte für Dateien im Überwachungsbereich der Aufgabe berechnet und gespeichert werden. Wenn eine Aufgabe zur Überwachung der Baseline-Integrität gelöscht wurde, löscht Kaspersky Embedded Systems Security die Baseline für diese Aufgabe zur Überwachung der Baseline-Integrität.

Sie können eine Baseline löschen, ohne die Aufgabe zur Überwachung der Baseline-Integrität zu löschen, indem Sie die Befehlszeile verwenden.

Die Aufgabe zur Überwachung der Baseline-Integrität überwacht die folgenden Änderungen an Dateien im Überwachungsbereich:

- Der Überwachungsbereich enthält eine Datei, die nicht in der Baseline vorhanden ist.
- Im Überwachungsbereich fehlt eine Datei, die in der Baseline vorhanden ist.
- Der Hash einer Datei im Überwachungsbereich weicht von dem Hash dieser Datei in der Baseline ab.

Die Aufgabe zur Überwachung der Baseline-Integrität überwacht keine Änderungen an Attributen und zusätzlichen Strömen der Datei.

Wenn auf eine Datei oder einen Ordner nicht zugegriffen werden kann, fügt Kaspersky Embedded Systems Security diese Datei oder diesen Ordner während der Baseline-Erstellung nicht zur Baseline hinzu und erstellt während der Ausführung der Aufgabe zur Überwachung der Baseline-Integrität ein Ereignis über einem Fehler bei der Prüfsummenberechnung der Datei.

Der Zugriff auf eine Datei oder einen Ordner ist möglicherweise aus den folgenden Gründen nicht möglich:

- Der angegebene Pfad existiert nicht.
- Ein von der Maske angegebener Dateityp ist in dem angegebenen Pfad nicht vorhanden.
- Die angegebene Datei ist gesperrt.
- Die angegebene Datei ist leer.

Aktivieren des Starts von Untersuchungen auf Befehl aus dem Kontextmenü heraus.

Sie können die Aufgabe einer Untersuchung auf Befehl für eine oder mehrere Dateien aus einem Kontextmenü in Microsoft Windows Explorer heraus starten.

Um die Aufgabe "Untersuchung auf Befehl" aus dem Kontextmenü zu starten, gehen Sie wie folgt vor:

1. Erstellen Sie die folgenden REG-Dateien:

```
Windows-Registrierungs-Editor Version 5.0.0
[HKEY_CLASSES_ROOT\Directory\shell\kess\command]
```

```
@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Scan with Kaspersky Embedded Systems Security\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Scan with Kaspersky Embedded Systems Security\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems
Security\\kavshell.exe"="~ RUNASADMIN"
```

Sie müssen den tatsächlichen Speicherort des Installationsordners für Kaspersky Embedded Systems Security angeben.

2. Legen Sie die Datei `scan.cmd` mit folgendem Inhalt an:

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Scanning is in progress...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

Die Datei `scan.cmd` muss folgende Informationen beinhalten:

- Speicherort der Datei `kavshell.exe`.
- Speicherort der temporären Datei mit den Untersuchungsergebnissen.
- Parameter für den Befehl `KAVSHELL SCAN`.
- Timeout-Wert zum Schließen des Konsolenfensters nach Beendigung der Aufgabe.

3. Kopieren Sie die Datei `scan.cmd` in den Ordner, der in der REG-Datei `[HKEY_CLASSES_ROOT\Directory\shell\kess\command]` angegeben wurde.

Der Ordner `C:\Temp` ist beispielhaft angegeben.

Sie müssen das Betriebssystem nicht neu starten.

Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl

Die Standardeinstellungen von Aufgaben zur Untersuchung auf Befehl werden in folgender Tabelle beschrieben. Lokale Systemaufgaben und benutzerdefinierte Aufgaben zur Untersuchung auf Befehl lassen sich konfigurieren.

Standardeinstellungen für Aufgaben zur Untersuchung auf Befehl

Einstellung	Standardwert	Beschreibung
Untersuchungsbereich	Wird in den folgenden lokalen Systemaufgaben und benutzerdefinierten Aufgaben verwendet: • **Untersuchung beim Hochfahren des Betriebssystems**: das gesamte geschützte Gerät mit Ausnahme der freigegebenen Ordner und der Objekte des Autostarts. • **Untersuchung wichtiger Bereiche**: das gesamte geschützte Gerät mit Ausnahme der freigegebenen Ordner und einiger Dateien des Betriebssystems. • Benutzerdefinierte **Untersuchung auf Befehl**: das gesamte geschützte Gerät.	Sie können den Untersuchungsbereich ändern. Der Untersuchungsbereich für die lokalen Systemaufgaben zur **Untersuchung von Quarantäne-Objekten** und **Integritätsprüfung für Programme** kann nicht konfiguriert werden.
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Sie können für die ausgewählten Knoten in der Struktur oder Liste der Dateiressourcen des geschützten Geräts folgende Aktionen ausführen: • eine andere vordefinierte Sicherheitsstufe auswählen • Sicherheitseinstellungen manuell ändern. Sie können eine Gruppe von Sicherheitsparametern für den ausgewählten Knoten in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen.
Heuristische Analyse verwenden	Für die Aufgaben Untersuchung wichtiger Bereiche und Untersuchung beim Hochfahren des Betriebssystems sowie für benutzerdefinierte	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen. Sie können die Analysestufe für die Aufgabe Untersuchung von Quarantäne-Objekten nicht ändern.

	Untersuchungsaufgaben wird die Analysestufe **Mittel** verwendet. Für die Aufgabe Untersuchung von Quarantäne-Objekten wird die Analysestufe **Tief** verwendet.	Heuristische Analyse wird in den Aufgaben zur Integritätsprüfung für Programme und zur Überwachung der Baseline-Integrität nicht verwendet.
Vertrauenswürdige Zone anwenden	Übernommen (Nicht übernommen für Aufgabe zur Untersuchung von Quarantäne-Objekten)	Einheitliche Liste mit Ausnahmen, die Sie in bestimmten Aufgaben verwenden können.
KSN bei der Untersuchung verwenden	Wird verwendet	Sie können Ihr Gerät durch die Nutzung der Cloud-Dienst-Infrastruktur von Kaspersky Security Network effektiver schützen.
Einstellungen zum Start der Aufgabe mit spezifischen Rechten	Die Aufgabe wird mit den Rechten des Systemkontos gestartet.	Sie können Einstellungen für den Start mit den Rechten von Benutzerkonten für alle Systemaufgaben und benutzerdefinierten Aufgaben für die Untersuchung auf Befehl ändern, mit Ausnahme der Aufgaben Untersuchung von Quarantäne-Objekten und Integritätsprüfung für Programme.
Aufgabe im Hintergrundmodus ausführen (geringe Priorität)	Wird nicht verwendet	Sie können die Priorität der Aufgaben für die Untersuchung auf Befehl festlegen.
Zeitplan für den Aufgabenstart	Wird in den folgenden lokalen Systemaufgaben verwendet: • Untersuchung beim Hochfahren des Betriebssystems – **Bei Programmstart** • Untersuchung wichtiger Bereiche – **Wöchentlich** • Untersuchung von Quarantäne-Objekten – **Nach dem Update der Programm-Datenbanken**. • Integritätsprüfung für Programme – **Alle n Tage** Wird in neu erstellten benutzerdefinierten Aufgaben nicht verwendet.	Sie können die Einstellungen für die Ausführung von geplanten Aufgaben anpassen.
Registrierung der Ausführung der Untersuchung und Aktualisierung des Schutzstatus des Geräts	Der Schutzstatus des Geräts wird wöchentlich nach Ausführung der Aufgabe Untersuchung wichtiger Bereiche aktualisiert.	Sie können die Einstellungen für die Registrierung der Aufgabe zur Untersuchung wichtiger Bereiche folgendermaßen konfigurieren: • durch Änderung der Einstellungen im Zeitplan für den Aufgabenstart der Aufgabe Untersuchung wichtiger Bereiche • durch Änderung des Untersuchungsbereichs der Aufgabe zur Untersuchung wichtiger Bereiche

		• durch Erstellung von benutzerdefinierten Aufgaben für die Untersuchung auf Befehl

Aufgaben zur Untersuchung auf Befehl über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Aufgabeneinstellungen für einen oder alle geschützten Geräte im Netzwerk konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen

Um eine neue benutzerdefinierte Aufgabe zur Untersuchung auf Befehl zu erstellen, gehen Sie wie folgt vor:

1. Für das Erstellen einer lokalen Aufgabe:
   a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Verwaltungskonsole von Kaspersky Security Center.
   b. Wählen Sie die Administrationsgruppe aus, zu der das geschützte Gerät gehört.
   c. Öffnen Sie auf der Registerkarte **Geräte** im Ergebnisbereich das Kontextmenü des geschützten Geräts.
   d. Wählen Sie den Punkt **Eigenschaften** aus.
   e. Klicken Sie im nächsten Fenster auf die Schaltfläche **Hinzufügen** im Abschnitt **Aufgaben**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.
2. Für das Erstellen einer Gruppenaufgabe:
   a. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
   b. Wählen Sie die Administrationsgruppe aus, für die Sie eine Aufgabe erstellen möchten.
   c. Öffnen Sie die Registerkarte **Aufgaben**.
   d. Klicken Sie auf die Schaltfläche **Aufgabe erstellen**.

   Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.
3. Um eine Aufgabe für eine benutzerdefinierte Gruppe von geschützten Geräten zu erstellen, gehen Sie wie folgt vor:

a. Klicken Sie im Knoten **Geräteauswahlen** in der Verwaltungskonsole von Kaspersky Security Center auf die Schaltfläche **Auswahl ausführen**, um eine Geräteauswahl durchzuführen.

b. Öffnen Sie die Registerkarte **Auswahlergebnisse Auswahlname**.

c. Wählen Sie in der Dropdown-Liste **Auswahl durchführen** die Option **Aufgabe für ein Auswahlergebnis erstellen** aus.

Daraufhin wird das Fenster **Assistent für neue Aufgabe** geöffnet.

4. Wählen Sie die Aufgabe **Untersuchung auf Befehl** aus der Liste der für Kaspersky Embedded Systems Security verfügbaren Aufgaben aus.

5. Klicken Sie auf **Weiter**.

   Das Fenster **Einstellungen** wird geöffnet.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

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

Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben von Kaspersky Security Center.

Das Fenster **Eigenschaften: Untersuchung auf Befehl** wird geöffnet.

Aufgabeneigenschaften für die Untersuchung auf Befehl öffnen

Um die Programmeinstellungen für die Aufgabe zur Untersuchung auf Befehl für ein einzelnes geschütztes Gerät zu öffnen, gehen wie folgt vor:

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

2. Wählen Sie die Administrationsgruppe aus, zu der das geschützte Gerät gehört.

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

4. Doppelklicken Sie auf den Namen des geschützten Geräts, für das Sie den Untersuchungsbereich anpassen möchten.

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.

5. Wählen Sie den Abschnitt **Aufgaben** aus.

6. Wählen Sie in der Liste der für das Gerät erstellten Aufgaben die Aufgabe zur Untersuchung auf Befehl aus, die Sie erstellt haben.

7. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Eigenschaften: Untersuchung auf Befehl** wird geöffnet.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

Erstellen einer Aufgabe zur Untersuchung auf Befehl

Um eine benutzerdefinierte Aufgabe zur Untersuchung auf Befehl zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Einstellungen** im Assistenten für neue Aufgaben.
2. Wählen Sie die gewünschte **Methode für die Aufgabenerstellung** aus.
3. Klicken Sie auf **Weiter**.
4. Erstellen Sie im Fenster **Untersuchungsbereich** einen Untersuchungsbereich:

   Standardmäßig gehören zum Untersuchungsbereich wichtige Bereiche des geschützten Geräts. Untersuchungsbereiche sind in der Tabelle mit dem Symbol ☑ gekennzeichnet. Bereiche, die vom Untersuchungsbereich ausgenommen sind, werden in der Tabelle mit dem Symbol ☐ markiert.

   Sie können den Untersuchungsbereich ändern: Einzelne vordefinierte Bereiche, Datenträger, Ordner, Netzwerkobjekte oder Dateien in den Untersuchungsbereich aufnehmen und individuelle Sicherheitseinstellungen für die hinzugefügten Bereiche festlegen.

   - Um 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 geschützten Geräts, einen Ordner, ein Netzwerkobjekt oder eine Datei auf dem geschützten Gerät oder auf einem anderen geschützten Gerät 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 Dateien** und **Untergeordnete Ordner**.

   - 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 anpassen** 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.

- Um eingebettete Objekte in hinzugefügten Untersuchungsbereich zu überspringen, gehen Sie wie folgt vor:

  a. Öffnen Sie das Kontextmenü für die Tabelle **Untersuchungsbereich** und wählen Sie **Ausnahme hinzufügen**.

  b. Geben Sie die Objekte an, die ausgeschlossen werden sollen: Wählen Sie den vordefinierten Gültigkeitsbereich in der Liste **Vordefinierter Bereich** aus, geben Sie das Gerätelaufwerk, den Ordner, das Netzwerkobjekt bzw. die Datei auf dem geschützten Gerät oder einem anderen geschützten Gerät im Netzwerk an.

  c. Klicken Sie auf die Schaltfläche **OK**.

5. Passen Sie im Fenster **Einstellungen** die heuristische Analyse und Integration mit anderen Komponenten an:

   - Passen Sie die Verwendung der heuristischen Analyse an.
   - Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie Objekte, die zur Liste der vertrauenswürdigen Zonen hinzugefügt wurden, vom Untersuchungsbereich der Aufgabe ausschließen möchten.
   - Aktivieren Sie das Kontrollkästchen **KSN bei der Untersuchung verwenden**, wenn Sie die Cloud-Dienste von Kaspersky Security Network für die Aufgabe nutzen möchten.
   - Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Priorität *Niedrig* zuzuweisen, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**.

     Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

   - Um die erstellte Aufgabe als Untersuchung wichtiger Bereiche zu verwenden, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten**.

6. Klicken Sie auf **Weiter**.
7. Legen Sie im Fenster **Zeitplan** die Einstellungen für den Zeitplan für den Aufgabenstart fest.
8. Klicken Sie auf **Weiter**.
9. Legen Sie im Fenster **Konto für das Ausführen der Aufgabe auswählen** das Konto fest, das Sie verwenden möchten.
10. Klicken Sie auf **Weiter**.
11. Geben Sie einen Aufgabennamen an.
12. Klicken Sie auf **Weiter**.

Der Aufgabenname darf nicht länger als 100 Zeichen sein und darf folgende Symbole nicht enthalten: " * < > & \ : |

Das Fenster **Erstellung der Aufgabe fertig stellen** wird geöffnet.

13. Sie können die Aufgabe optional ausführen, nachdem der Assistent abgeschlossen wurde, indem Sie das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten** aktivieren.

14. Klicken Sie auf **Fertig stellen**, um die Erstellung der Aufgabe abzuschließen.

Die neue Aufgabe zur Untersuchung auf Befehl wird für das ausgewählte geschützte Gerät oder eine Gruppe von geschützten Geräten erstellt.

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

In der Grundeinstellung weist Kaspersky Security Center einem geschützten Gerät den Status *Warnung* zu, wenn die Aufgabe zur Untersuchung wichtiger Bereiche seltener ausgeführt wird als durch die Einstellung *Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt* in Kaspersky Embedded Systems Security angegeben ist.

So konfigurieren Sie die Untersuchung aller geschützten Geräte, 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 angegebenen Aufgabeneinstellungen (der Untersuchungsbereich und die Sicherheitseinstellungen) werden für alle geschützten Geräte in der Gruppe übernommen. Passen Sie den Aufgabenzeitplan ein.

   Sie können das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten** aktivieren, wenn Sie die Aufgabe zur Untersuchung auf Befehl für eine Gruppe von geschützten Geräten erstellen, oder später im Fenster **Eigenschaften: <Aufgabenname>**.

3. Deaktivieren Sie mit Hilfe einen neuen oder vorhandenen Richtlinie den Start von lokalen Systemaufgaben zur Untersuchung auf Befehl auf den geschützten Geräten der Gruppe.

Von diesem Zeitpunkt an berücksichtigt der Kaspersky Security Center-Administrationsserver bei der Bewertung des Sicherheitszustands des geschützten Geräts und bei der Benachrichtigung darüber die Ergebnisse der letzten Ausführung einer Aufgabe mit dem Status "Untersuchung wichtiger Bereiche" und nicht die Ausführungsergebnisse der lokalen Systemaufgabe "Untersuchung wichtiger Bereiche".

Sie können den Status *Untersuchung wichtiger Bereiche* nicht nur Gruppenaufgaben, sondern auch Aufgaben für Gruppen von geschützten Geräten zur Untersuchung auf Befehl zuweisen.

In der Programmkonsole können Sie überprüfen, ob eine Aufgabe zur Untersuchung auf Befehl als Aufgabe zur Untersuchung wichtiger Bereiche betrachtet wird.

In der Programmkonsole wird das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten** in den Aufgabeneigenschaften nur angezeigt und kann nicht geändert werden.

Ausführung einer Aufgabe im Hintergrund zur Untersuchung auf Befehl

Prozesse, in denen Aufgaben von Kaspersky Embedded Systems Security ausgeführt werden, besitzen die Priorität *Mittel (Normal)*.

Sie können einem Prozess, in dem eine Aufgabe zur Untersuchung auf Befehl ausgeführt wird, die Priorität *Niedrig* (Low) zuweisen. Wenn die Priorität eines Prozesses gesenkt wird, erhöht sich dadurch die Ausführungsdauer der Aufgabe und die Leistung der Prozesse anderer aktiver Anwendungen wird gesteigert.

In einem aktiven Prozess mit niedriger Priorität können mehrere Aufgaben im Hintergrundmodus ausgeführt werden. Sie können die maximale Anzahl der Prozesse von Hintergrundaufgaben zur Untersuchung auf Befehl angeben.

Um die Priorität einer bestehenden Aufgabe zur Untersuchung auf Befehl zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl**.
2. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**.
3. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe werden gespeichert und unverzüglich während der Ausführung der Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Registrierung der Ausführung der Untersuchung wichtiger Bereiche

Standardmäßig wird der Schutzstatus des Geräts im Ergebnisbereich des Knotens **Kaspersky Embedded Systems Security** angezeigt und wöchentlich nach Abschluss der Aufgabe Untersuchung wichtiger Bereiche aktualisiert.

Der Zeitpunkt, zu dem der Schutzstatus des Geräts aktualisiert wird, ist mit dem Zeitplan der Aufgabe zur Untersuchung auf Befehl verknüpft, für die das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten** aktiviert ist. Standardmäßig ist das Kontrollkästchen nur für die Aufgabe zur Untersuchung wichtiger Bereiche aktiviert und kann für diese Aufgabe nicht geändert werden.

Sie können die Aufgabe zur Untersuchung auf Befehl, die mit dem Schutzstatus des Geräts verknüpft ist, nur aus Kaspersky Security Center auswählen.

Untersuchungsbereich der Aufgabe anpassen

Wenn Sie den Untersuchungsbereich in den Aufgaben "Untersuchung beim Hochfahren des Betriebssystems" und "Untersuchung wichtiger Bereiche" geändert haben, können Sie in diesen Aufgaben den standardmäßigen Untersuchungsbereich wiederherstellen. Führen Sie dazu die Wiederherstellung von Kaspersky Embedded Systems Security aus (**Start** > **Programme** > **Kaspersky Embedded Systems Security** > **Kaspersky Embedded Systems Security ändern oder löschen**). Wählen Sie im Installationsassistent die Option **Installierte Komponenten reparieren** aus und klicken Sie auf **Weiter**. Aktivieren Sie dann das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**.

Um einen Untersuchungsbereich einer bestehenden Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl**.
2. Wählen Sie die Registerkarte **Untersuchungsbereich** aus.
3. Um Objekte in den Untersuchungsbereich einzuschließen, gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü in einem leeren Bereich der Liste der Untersuchungsbereiche.
   b. Wählen Sie aus dem Kontextmenü die Option **Bereich hinzufügen** aus.
   c. Wählen Sie im geöffneten Fenster **Zum Untersuchungsbereich hinzufügen** den Typ des Objektes aus, das Sie hinzufügen möchten:
      - **Vordefinierter Bereich** – wenn Sie einen der vordefinierten Bereiche auf dem geschützten Gerät hinzufügen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Untersuchungsbereich aus.
      - **Laufwerk, Ordner oder Netzwerkobjekt** – wenn Sie in den Untersuchungsbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Bereich über die Schaltfläche **Durchsuchen** aus.
      - **Datei** – wenn Sie in den Untersuchungsbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Bereich über die Schaltfläche **Durchsuchen** aus.

   Sie können ein Objekt nicht zum Untersuchungsbereich hinzufügen, wenn es bereits als Ausnahme aus dem Untersuchungsbereich hinzugefügt wurde.
4. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten, oder führen Sie folgenden Aktionen aus:
   a. Öffnen Sie das Kontextmenü des Untersuchungsbereichs mit der rechten Maustaste.
   b. Wählen Sie im Kontextmenü den Punkt **Ausnahme hinzufügen**.
   c. Wählen Sie im geöffneten Fenster **Ausnahme hinzufügen** den Typ des Objektes aus, das Sie als Ausnahme aus dem Untersuchungsbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Untersuchungsbereich.
5. Um den Untersuchungsbereich oder eine hinzugefügte Ausnahme im Kontextmenü des entsprechenden Untersuchungsbereichs, den Sie ändern möchten, zu ändern, wählen Sie den Punkt **Bereich ändern**.
6. Um die Anzeige eines zuvor hinzugefügten Untersuchungsbereichs bzw. einer zuvor hinzugefügten Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des zu verbergenden Untersuchungsbereichs den Punkt **Bereich löschen** aus.

Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

7. Klicken Sie auf die Schaltfläche **OK**.

Das Fenster Untersuchungsbereich - Einstellungen wird geschlossen. Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen

Sie können eine der folgenden drei vordefinierten Sicherheitsstufen für einen in der Liste der Dateiressourcen des geschützten Geräts ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen** und **Maximale Sicherheit**.

Um eine der vordefinierten Sicherheitsstufen auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl**.
2. Wählen Sie die Registerkarte **Untersuchungsbereich** aus.
3. Wählen Sie in der Liste des geschützten Geräts ein Element aus dem Untersuchungsbereich aus, um eine vordefinierte Sicherheitsstufe festzulegen.
4. Klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Untersuchung auf Befehl anpassen** wird geöffnet.
5. Wählen Sie auf der Registerkarte **Sicherheitsstufe** die Sicherheitsstufe aus, die Sie übernehmen möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
6. Klicken Sie auf die Schaltfläche **OK**.
7. Klicken Sie auf die Schaltfläche **OK** im Fenster **Eigenschaften: Untersuchung auf Befehl**.

   Die Einstellungen der Aufgabe werden gespeichert und unverzüglich auf eine ausgeführte Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Sicherheitseinstellungen manuell anpassen

Standardmäßig werden in den Aufgaben zur Untersuchung auf Befehl die gleichen Sicherheitsparameter verwendet wie für den gesamten Untersuchungsbereich.

Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**.

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Untersuchungsbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des geschützten Geräts oder den Nodes in der Struktur festlegen.

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

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl**.
2. Wählen Sie die Registerkarte **Untersuchungsbereich** aus.
3. Wählen Sie die Elemente in der Liste der Untersuchungsbereiche aus, für die Sie Parameter für Sicherheit anpassen möchten.

   Für einen ausgewählten Knoten oder ein Element im Untersuchungsbereich kann eine vordefinierte Vorlage mit Sicherheitseinstellungen übernommen werden.

4. Klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Untersuchung auf Befehl anpassen** wird geöffnet.

5. Passen Sie auf den folgenden Registerkarten die Sicherheitseinstellungen des ausgewählten Knotens oder Elements entsprechend ihren Anforderungen an:

   - **Allgemein**
   - **Aktionen**
   - **Optimierung**
   - **Hierarchischer Speicher**

6. Klicken Sie im Fenster **Untersuchung auf Befehl anpassen** auf **OK**.
7. Klicken Sie im Fenster **Untersuchungsbereich** auf **OK**.

Die neuen Einstellungen des Untersuchungsbereichs werden gespeichert.

Allgemeine Aufgabeneinstellungen anpassen

Um allgemeine Einstellungen für Aufgaben zur Untersuchung auf Befehl anpassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl**.
2. Wählen Sie die Registerkarte **Untersuchungsbereich** aus.
3. Klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Untersuchung auf Befehl anpassen** wird geöffnet.

4. Klicken Sie auf die Schaltfläche **Einstellungen**.
5. Geben Sie auf der Registerkarte **Allgemein** im Gruppenfeld **Objekte untersuchen** das Objekt an, das Sie in den Untersuchungsbereich einschließen möchten:

   - **Untersuchungsobjekte**:
     - **Alle Objekte**
     - **Objekte, die nach Format untersucht werden**

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

- **Untergeordnete Ordner**
- **Untergeordnete Dateien**
- Bootsektoren und MBR
- Alternative NTFS-Ströme

6. Aktivieren oder deaktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen Nur neue und veränderte Dateien untersuchen.

   Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

7. Geben Sie im Gruppenfeld **Zusammengesetzte Objekte untersuchen** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - Alle / Nur neue Archive
   - Alle / Nur neue SFX-Archive
   - Alle / Nur neue E-Mail-Datenbanken
   - Alle / Nur neue gepackte Objekte
   - Alle / Nur neue E-Mails im Nur-Text-Format
   - Alle / Nur neue eingebettete OLE-Objekte

8. Klicken Sie auf **OK**.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

Um die Aktionen für infizierte und andere gefundene Objekte während der Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster Eigenschaften: Untersuchung auf Befehl.
2. Wählen Sie die Registerkarte **Untersuchungsbereich** aus.
3. Klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Untersuchung auf Befehl anpassen** wird geöffnet.
4. Klicken Sie auf die Schaltfläche **Einstellungen**.
5. Wählen Sie die Registerkarte **Aktionen** aus.

6. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:
   - **Nur informieren**.
   - **Desinfizieren**.
   - **Desinfizieren. Löschen, falls Desinfektion fehlschlägt**.
   - **Löschen**.
   - **Empfohlene Aktion ausführen**.
7. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - **Nur informieren**.
   - **Quarantäne**.
   - **Löschen**.
   - **Empfohlene Aktion ausführen**.
8. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktionen je nach Typ des erkannten Objekts ausführen**.
   b. Klicken Sie auf die Schaltfläche **Einstellungen**.
   c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts eine primäre und eine sekundäre Aktion aus (die auszuführen ist, falls die primäre Aktion nicht durchgeführt werden kann).
   d. Klicken Sie auf **OK**.
9. Wählen Sie die Aktion für nicht desinfizierbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann**.
10. Klicken Sie auf **OK**.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

So optimieren Sie die Leistung der Aufgabe Untersuchung auf Befehl:

1. Öffnen Sie das Fenster **Eigenschaften: Untersuchung auf Befehl**.
2. Wählen Sie die Registerkarte **Untersuchungsbereich** aus.
3. Klicken Sie auf die Schaltfläche **Anpassen**.
   Das Fenster **Untersuchung auf Befehl anpassen** wird geöffnet.
4. Klicken Sie auf die Schaltfläche **Einstellungen**.

5. Wählen Sie die Registerkarte **Optimierung** aus.

6. Im Abschnitt **Ausnahmen**:

   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Nicht erkennen**.
   - Klicken Sie für jede Einstellung auf die Schaltfläche **Ändern**, um Ausnahmen hinzuzufügen.

7. Im Abschnitt **Erweiterte Einstellungen**:

   - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
   - **Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)**
   - **iSwift-Technologie verwenden**
   - **iChecker-Technologie verwenden**

8. Klicken Sie auf **OK**.

Die neue Aufgabenkonfiguration wird gespeichert.

Untersuchung von Wechseldatenträgern anpassen

Um die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an das geschützte Gerät anzupassen, gehen Sie wie folgt vor:

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

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

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

4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.

   Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Zusätzlich**.

5. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Untersuchung von Wechseldatenträgern**.

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.

6. Im Abschnitt **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 automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)** und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste **Untersuchung starten mit Sicherheitsstufe** die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.

7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und übernommen.

Aufgabe zur Überwachung der Baseline-Integrität anpassen

Um die Gruppenaufgabe zur Überwachung der Baseline-Integrität zu konfigurieren, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center und wählen Sie die Administrationsgruppe, für die Sie die Anwendungsaufgaben konfigurieren möchten.

2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.

3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten.

4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:

   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und klicken Sie auf den Link **Aufgabe konfigurieren**.
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.

   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. Gehen Sie im Abschnitt **Untersuchungsbereich** wie folgt vor:

   a. Um Ordner in den Aufgabenbereich der Überwachung der Baseline-Integrität aufzunehmen:

      1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

         Das Fenster **Eigenschaften des Untersuchungsbereichs** wird geöffnet.

      2. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Diesen Bereich untersuchen**.

      3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um den Ordner anzugeben, der in den Aufgabenbereich der Überwachung der Baseline-Integrität aufgenommen werden soll.

      4. Aktivieren Sie das Kontrollkästchen **Unterordner ebenfalls untersuchen**, wenn Sie alle Unterordner in den Aufgabenbereich der Überwachung der Baseline-Integrität aufnehmen möchten.

   b. Um einen Ordner einzuschließen oder auszuschließen, der zuvor zum Aufgabenbereich der Überwachung der Baseline-Integrität hinzugefügt wurde, aktivieren oder deaktivieren Sie das Kontrollkästchen links neben dem Pfad des Ordners in der Tabelle für den **Untersuchungsbereich**.

   c. Um einen zuvor zum Aufgabenbereich der Überwachung der Baseline-Integrität hinzugefügten Ordner zu löschen, wählen Sie diesen Ordner in der Tabelle **Untersuchungsbereich** aus, und klicken Sie auf die Schaltfläche **Löschen**

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 die Aufgabe ausgeführt wird.

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 Abschnitten finden Sie im *Hilfesystem von Kaspersky Security Center*.

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

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Aufgaben zur Untersuchung auf Befehl über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und Aufgabeneinstellungen auf einem geschützten Gerät konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Aufgabeneinstellungen für die Untersuchung auf Befehl öffnen

Um die allgemeinen Einstellungen der Aufgabe zur Untersuchung auf Befehl über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe entspricht, die Sie konfigurieren möchten.

3. Klicken Sie im Ergebnisbereich des untergeordneten Knotens auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

Einstellungen des Gültigkeitsbereichs für die Aufgabe zur Untersuchung auf Befehl öffnen

Um die Einstellungen des Untersuchungsbereichs über die Programmkonsole zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe zur Untersuchung auf Befehl entspricht, deren Einstellungen Sie konfigurieren möchten.

3. Klicken Sie im Ergebnisbereich des ausgewählten Knotens auf den Link **Untersuchungsbereich anpassen**.

   Das Fenster **Untersuchungsbereich - Einstellungen** wird geöffnet.

Aufgabe zur Untersuchung auf Befehl erstellen und anpassen

Sie können im Knoten **Untersuchung auf Befehl** benutzerdefinierte Aufgaben für ein einzelnes geschütztes Gerät erstellen. Benutzerdefinierte Aufgaben können nicht in anderen funktionalen Komponenten von Kaspersky Embedded Systems Security erstellt werden.

Um eine neue Aufgabe zur Untersuchung auf Befehl zu erstellen und anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Untersuchung auf Befehl**.

2. Wählen Sie den Punkt **Aufgabe hinzufügen** aus.

   Das Fenster **Aufgabe hinzufügen** wird geöffnet.

3. Konfigurieren Sie folgende Aufgabeneinstellungen:

   - **Name** – Der Name der Aufgabe bestehend aus maximal 100 Zeichen. Folgende Zeichen dürfen nicht enthalten sein **" * < > & \ : |**.

     Ohne die Angabe des Aufgabennamens können Sie weder die neue Aufgabe speichern noch zur Konfiguration der Einstellungen der neuen Aufgabe auf den Registerkarten **Zeitplan**, **Erweitert** und **Mit folgenden Rechten starten** wechseln.

   - **Beschreibung** – Alle zusätzlichen Informationen über die Aufgabe. Nicht mehr als 2000 Zeichen. Diese Informationen werden im Fenster Eigenschaften der Aufgabe angezeigt.

   - **Heuristische Analyse verwenden**

   - **Aufgabe im Hintergrundmodus ausführen**

   - **Vertrauenswürdige Zone anwenden**

   - **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten**

   - **KSN bei der Untersuchung verwenden**

4. Passen Sie die Einstellungen für den Zeitplan für den Aufgabenstart auf den Registerkarten **Zeitplan** und **Erweitert** an.

5. Passen Sie auf der Registerkarte **Mit folgenden Rechten starten** die Einstellungen zum Starten der Aufgabe mit bestimmten Benutzerrechten an.

6. Klicken Sie im Fenster **Aufgabe hinzufügen** auf **OK**.

   Es wird eine neue benutzerdefinierte Aufgabe zur Untersuchung auf Befehl erstellt. Der Knoten mit dem Namen der neuen Aufgabe wird in der Programmkonsolenstruktur angezeigt. Die Operation wird im Systemaudit-Protokoll erfasst.

7. Wählen Sie bei Bedarf im Ergebnisbereich des ausgewählten Knotens **Untersuchungsbereich anpassen** aus.

   Das Fenster **Untersuchungsbereich - Einstellungen** wird geöffnet.

8. Wählen Sie in der Struktur oder Liste der Dateiressourcen des geschützten Geräts diejenigen Knoten oder Elemente aus, die Sie dem Untersuchungsbereich hinzufügen möchten.

9. Wählen Sie eine der voreingestellten Sicherheitsstufen aus oder passen Sie die Untersuchungseinstellungen manuell an.

10. Klicken Sie im Fenster **Untersuchungsbereich - Einstellungen** auf **Speichern**.

Die vorgenommenen Einstellungen werden beim nächsten Aufgabenstart übernommen.

Untersuchungsbereich in den Aufgaben zur Untersuchung auf Befehl

Dieser Abschnitt enthält Informationen über die Erstellung und Verwendung eines Untersuchungsbereichs in den Aufgaben zur Untersuchung auf Befehl.

Einstellungen für die Anzeige der freigegebenen Netzwerkordner anpassen

Um die Art der Anzeige der freigegebenen Netzwerkordner beim Anpassen von Einstellungen für den Untersuchungsbereich auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.

2. Öffnen Sie die Dropdown-Liste im oberen linken Abschnitt des Fensters und wählen Sie eine der folgenden Optionen aus:

   - Wählen Sie den Punkt **Als Baumstruktur anzeigen**, wenn Sie möchten, dass die freigegebenen Netzwerkordner als Baumstruktur angezeigt werden.
   - Wählen Sie den Punkt **Als Liste anzeigen**, wenn Sie möchten, dass die freigegebenen Netzwerkordner des geschützten Computers in Form einer Liste angezeigt werden.

   Standardmäßig werden die freigegebenen Netzwerkordner des geschützten Geräts als Liste angezeigt.

3. Klicken Sie auf die Schaltfläche **Speichern**.

Untersuchungsbereich erstellen

Wenn Sie Kaspersky Embedded Systems Security auf dem geschützten Gerät im Remote-Betrieb über die Programmkonsole verwalten, die an einem Administrator-Arbeitsplatz installiert ist, müssen Sie zur Gruppe der Administratoren auf dem geschützten Gerät gehören, um die dort befindlichen Ordner zu sehen.

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

Wenn Sie den Untersuchungsbereich in den Aufgaben "Untersuchung beim Hochfahren des Betriebssystems" und "Untersuchung wichtiger Bereiche" geändert haben, können Sie in diesen Aufgaben den standardmäßigen Untersuchungsbereich wiederherstellen. Führen Sie dazu die Wiederherstellung von Kaspersky Embedded Systems Security aus (**Start** > **Programme** > **Kaspersky Embedded Systems Security** > **Kaspersky Embedded Systems Security ändern oder löschen**). Wählen Sie im Installationsassistent die Option **Installierte Komponenten reparieren** aus und klicken Sie auf **Weiter**. Aktivieren Sie dann das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**.

Die Vorgehensweise beim Erstellen des Untersuchungsbereichs in der Aufgabe zur Untersuchung auf Befehl hängt von der ausgewählten Anzeige der freigegebenen Netzwerkordner ab. Sie können die freigegebenen Netzwerkordner als Baumstruktur oder Liste (Standardansicht) anzeigen lassen.

Um mithilfe der Liste der freigegebenen Netzwerkordner einen Untersuchungsbereich zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Öffnen Sie im linken Teil des geöffneten Fensters die Struktur mit den freigegebenen Netzwerkordnern des Computers, um alle Knoten und untergeordneten Knoten anzuzeigen.
3. Führen Sie folgende Aktionen aus:
   - Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten.
   - Deaktivieren Sie das Kontrollkästchen **Arbeitsplatz**, um einzelne Knoten in den Untersuchungsbereich einzuschließen, und gehen Sie wie folgt vor:
     - Um alle Laufwerke eines bestimmten Typs in den Untersuchungsbereich aufzunehmen, aktivieren Sie das Kontrollkästchen neben dem Namen des entsprechenden Datenträgertyps (z. B. um alle Wechseldatenträger auf dem geschützten Gerät einzuschließen, aktivieren Sie das Kontrollkästchen **Wechseldatenträger**).
     - Um einen einzelnen Datenträger eines bestimmten Typs in den Untersuchungsbereich aufzunehmen, öffnen Sie den Knoten, der die Liste dieses Datenträgertyps enthält, und aktivieren Sie das Kontrollkästchen neben dem Namen des entsprechenden Laufwerks. Um beispielsweise den Wechseldatenträger **F:** auszuwählen, erweitern Sie den Knoten **Wechseldatenträger** und aktivieren Sie das Kontrollkästchen für das Laufwerk **F:**.
     - Wenn Sie nur einen einzelnen Ordner oder eine einzelne Datei auf dem Laufwerk in den Schutzbereich einschließen möchten, aktivieren Sie das Kontrollkästchen neben dem Namen dieses Ordners bzw. dieser Datei.
4. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster **Untersuchungsbereich - Einstellungen** wird geschlossen. Die neu vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Um mithilfe der Liste der freigegebenen Netzwerkordner einen Untersuchungsbereich zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen **Arbeitsplatz**, um einzelne Knoten in den Untersuchungsbereich einzuschließen, und gehen Sie wie folgt vor:
   a. Öffnen Sie das Kontextmenü des Untersuchungsbereichs mit der rechten Maustaste.

b. Wählen Sie im Kontextmenü der Schaltfläche den Punkt **Untersuchungsbereich hinzufügen** aus.

c. Wählen Sie im geöffneten Fenster **Untersuchungsbereich hinzufügen** den Typ des Objektes aus, das Sie hinzufügen möchten:

- **Vordefinierter Bereich** – wenn Sie einen der vordefinierten Bereiche auf dem geschützten Gerät hinzufügen möchten. Wählen Sie danach in der Dropdown-Liste den gewünschten Untersuchungsbereich aus.
- **Laufwerk, Ordner oder Netzwerkobjekt** – wenn Sie in den Untersuchungsbereich ein separates Laufwerk, einen Ordner oder ein Netzwerkobjekt des gewünschten Typs aufnehmen möchten. Wählen Sie dann den gewünschten Bereich über die Schaltfläche **Durchsuchen** aus.
- **Datei** – wenn Sie in den Untersuchungsbereich nur eine separate Datei auf dem Laufwerk aufnehmen möchten. Wählen Sie dann den gewünschten Bereich über die Schaltfläche **Durchsuchen** aus.

Sie können ein Objekt nicht zum Untersuchungsbereich hinzufügen, wenn es bereits als Ausnahme aus dem Untersuchungsbereich hinzugefügt wurde.

3. Deaktivieren Sie die Kontrollkästchen neben den Namen derjenigen Knoten, die Sie aus dem Untersuchungsbereich ausschließen möchten, oder führen Sie folgenden Aktionen aus:

   a. Öffnen Sie das Kontextmenü des Untersuchungsbereichs mit der rechten Maustaste.

   b. Wählen Sie im Kontextmenü den Punkt **Ausnahme hinzufügen**.

   c. Wählen Sie im geöffneten Fenster **Ausnahme hinzufügen** den Typ des Objektes aus, das Sie als Ausnahme aus dem Untersuchungsbereich hinzufügen möchten, genauso wie beim Hinzufügen eines Objekts zum Untersuchungsbereich.

4. Um den hinzugefügten Untersuchungsbereich oder die hinzugefügte Ausnahme im Kontextmenü des Untersuchungsbereichs, den Sie ändern möchten, zu ändern, wählen Sie den Punkt **Bereich ändern**.

5. Um die Anzeige eines zuvor hinzugefügten Untersuchungsbereichs bzw. einer zuvor hinzugefügten Ausnahme in der Liste der freigegebenen Netzwerkordner auszublenden, wählen Sie im Kontextmenü des zu verbergenden Untersuchungsbereichs den Punkt **Aus Liste löschen** aus.

   Der Untersuchungsbereich wird bei seiner Löschung aus der Liste der freigegebenen Netzwerkordner aus dem Gültigkeitsbereich der Aufgabe zur Untersuchung auf Befehl ausgeschlossen.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Das Fenster **Untersuchungsbereich - Einstellungen** wird geschlossen. Die neu vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Netzwerkobjekte in den Untersuchungsbereich aufnehmen

Sie können Netzlaufwerke, Ordner und Dateien in den Untersuchungsbereich aufnehmen. Geben Sie dazu die Netzwerkpfade im UNC-Format (Universal Naming Convention) an.

Sie können keine Netzwerkordner untersuchen, wenn Sie unter dem Systemkonto arbeiten.

Um ein Netzwerkobjekt zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Öffnen Sie die Dropdown-Liste im oberen linken Bereich des Fensters und wählen Sie **Als Baumstruktur anzeigen** aus.
3. Gehen Sie im Kontextmenü des Knotens **Netzwerkumgebung** wie folgt vor:
   - Wählen Sie den Punkt **Netzwerkordner hinzufügen** aus, wenn Sie einen Netzwerkordner zum Untersuchungsbereich hinzufügen möchten.
   - Wählen Sie den Punkt **Netzwerkdatei hinzufügen** aus, wenn Sie eine Netzwerkdatei zum Untersuchungsbereich hinzufügen möchten.
4. Geben Sie den Pfad des Netzwerkordners oder der Netzwerkdatei im UNC-Format (Universal Naming Convention) an und drücken Sie die **EINGABE**-Taste.
5. Aktivieren Sie das Kontrollkästchen neben dem Namen des hinzugefügten Netzwerkobjekts, um es in den Untersuchungsbereich aufzunehmen.
6. Ändern Sie, falls erforderlich, die Sicherheitseinstellungen für das hinzugefügte Netzwerkobjekt.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Virtuelle Untersuchungsbereiche erstellen

Sie können in den Untersuchungsbereich virtuelle Laufwerke, Ordner und Dateien aufnehmen – einen virtuellen Untersuchungsbereich erstellen.

Sie können den Untersuchungsbereich erweitern, indem Sie separate virtuelle Festplatten, Ordner oder Dateien nur dann hinzufügen, wenn der Untersuchungsbereich als Struktur der Dateiressourcen angezeigt wird.

Um eine virtuelle Festplatte zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Öffnen Sie die Dropdown-Liste im oberen linken Bereich des Fensters und wählen Sie **Als Baumstruktur anzeigen** aus.
3. Öffnen Sie in der Dateistruktur des geschützten Geräts das Kontextmenü für den Knoten **Virtuelle Festplatten**, klicken Sie auf **Virtuelle Festplatte hinzufügen** und wählen Sie in der Liste der verfügbaren Namen den Namen für die virtuelle Festplatte.
4. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Laufwerk, um das Laufwerk in den Untersuchungsbereich aufzunehmen.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Um einen virtuellen Ordner oder eine virtuelle Datei zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Öffnen Sie die Dropdown-Liste im oberen linken Bereich des Fensters und wählen Sie **Als Baumstruktur anzeigen** aus.
3. Öffnen Sie in der Dateistruktur des geschützten Geräts das Kontextmenü des Knotens, zu dem Sie einen Ordner oder eine Datei hinzufügen möchten, und wählen Sie einen der folgenden Punkte aus:
   - **Virtuellen Ordner hinzufügen**, wenn Sie einen virtuellen Ordner zum Untersuchungsbereich hinzufügen möchten.
   - **Virtuelle Datei hinzufügen**, wenn Sie eine virtuelle Datei zum Untersuchungsbereich hinzufügen möchten.
4. Tragen Sie im Eingabefeld den Namen für den Ordner bzw. die Datei ein.
5. In der Zeile mit dem Namen des Ordners bzw. der Datei aktivieren Sie das Kontrollkästchen, um den Ordner bzw. die Datei in den Untersuchungsbereich zu übernehmen.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Die vorgenommenen Änderungen an den Aufgabeneinstellungen werden gespeichert.

Sicherheitseinstellungen anpassen

Standardmäßig werden in den Aufgaben zur Untersuchung auf Befehl die gleichen Sicherheitsparameter verwendet wie für den gesamten Untersuchungsbereich.

Diese Einstellungen entsprechen denen der vordefinierten Sicherheitsstufe **Empfohlen**.

Sie können die Werte der Standardsicherheitseinstellungen ändern, indem Sie entweder einheitliche Werte für den gesamten Untersuchungsbereich oder individuelle Werte für unterschiedliche Elemente in der Liste der Dateiressourcen des geschützten Geräts oder den Nodes in der Struktur festlegen.

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

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

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Wählen Sie im linken Bereich des Fensters den Knoten oder das Element aus, für den/dass Sie die Einstellungen anpassen möchten.

   Für einen ausgewählten Knoten oder ein Element im Untersuchungsbereich kann eine vordefinierte Vorlage mit Sicherheitseinstellungen übernommen werden.

   Links im Fenster können Sie die Anzeige der freigegebene Netzwerkordner auswählen, einen Untersuchungsbereich erstellen oder einen virtuellen Untersuchungsbereich erstellen.
3. Führen Sie im rechten Teil des Fensters eine der folgenden Aktionen aus:
   - Wählen Sie auf der Registerkarte **Sicherheitsstufe** die Sicherheitsstufe aus, die Sie übernehmen möchten.

- Passen Sie auf den folgenden Registerkarten die erforderlichen Sicherheitseinstellungen des ausgewählten Knotens oder Elements entsprechend ihren Anforderungen an:
  - Allgemein
  - Aktionen
  - Optimierung
  - Hierarchischer Speicher

4. Klicken Sie im Fenster **Untersuchungsbereich - Einstellungen** auf **Speichern**.

Die neuen Einstellungen des Untersuchungsbereichs werden gespeichert.

Vordefinierte Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl auswählen

Sie können eine der folgenden drei vordefinierten Sicherheitsstufen für einen in der Baumstruktur oder Liste der Dateiressourcen des geschützten Geräts ausgewählten Knoten anwenden: **Maximale Leistung**, **Empfohlen** und **Maximale Sicherheit**.

Um eine der vordefinierten Sicherheitsstufen auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen.
2. Wählen Sie in der Baumstruktur oder Liste der freigegebenen Netzwerkordner einen Knoten oder ein Element aus, um die vordefinierte Sicherheitsstufe festzulegen.
3. Vergewissern Sie sich, dass der ausgewählte Knoten bzw. das Element zum Untersuchungsbereich gehört.
4. Wählen Sie im rechten Teil des Fensters auf der Registerkarte **Sicherheitsstufe** die Sicherheitsstufe aus, die Sie anwenden möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
5. Klicken Sie auf die Schaltfläche **Speichern**.

   Die Einstellungen der Aufgabe werden gespeichert und unverzüglich während der Ausführung der Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Allgemeine Aufgabeneinstellungen anpassen

So passen Sie die allgemeinen Sicherheitseinstellungen der Untersuchung auf Befehl an:

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen.
2. Wählen Sie die Registerkarte **Allgemein** aus.

3. Geben Sie im Gruppenfeld **Objekte untersuchen** das Objekt an, das Sie in den Untersuchungsbereich einschließen möchten:

   - **Untersuchungsobjekte**:
     - Alle Objekte
     - Objekte, die nach Format untersucht werden
     - Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden
     - Objekte, die nach der angegebenen Erweiterungsliste untersucht werden
   - Bootsektoren und MBR
   - Alternative NTFS-Ströme

4. Aktivieren oder deaktivieren Sie im Abschnitt **Optimierung** das Kontrollkästchen Nur neue und veränderte Dateien untersuchen.

   Um zwischen den verfügbaren Optionen hin- und her zu wechseln, wenn das Kontrollkästchen deaktiviert ist, klicken Sie für jeden Typ der zusammengesetzten Objekte auf den Link **Alle** / **Nur neue**.

5. Geben Sie im Gruppenfeld **Zusammengesetzte Objekte untersuchen** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - Alle / Nur neue Archive
   - Alle / Nur neue SFX-Archive
   - Alle / Nur neue E-Mail-Datenbanken
   - Alle / Nur neue gepackte Objekte
   - Alle / Nur neue E-Mails im Nur-Text-Format
   - Alle / Nur neue eingebettete OLE-Objekte

6. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Aktionen anpassen

So passen Sie die Aktionen für infizierte und andere gefundene Objekte für die Untersuchung auf Befehl an:

1. Öffnen Sie das Fenster Untersuchungsbereich - Einstellungen.
2. Wählen Sie die Registerkarte **Aktionen** aus.
3. Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus:

- **Nur informieren**.
- **Desinfizieren**.
- **Desinfizieren. Löschen, falls Desinfektion fehlschlägt**.
- **Löschen**.
- **Empfohlene Aktion ausführen**.

4. Wählen Sie eine Aktion für möglicherweise infizierte Objekte:
   - **Nur informieren**.
   - **In Quarantäne verschieben**.
   - **Löschen**.
   - **Empfohlene Aktion ausführen**.
5. Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an:
   a. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Aktionen je nach Typ des erkannten Objekts ausführen**.
   b. Klicken Sie auf die Schaltfläche **Einstellungen**.
   c. Wählen Sie in dem sich öffnenden Fenster für jeden Typ des gefundenen Objekts eine primäre und eine sekundäre Aktion aus (die auszuführen ist, falls die primäre Aktion nicht durchgeführt werden kann).
   d. Klicken Sie auf **OK**.
6. Wählen Sie die Aktion für nicht desinfizierbare zusammengesetzte Dateien: Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann**.
7. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Leistung optimieren

So optimieren Sie die Leistung der Aufgabe Untersuchung auf Befehl:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Wählen Sie die Registerkarte **Optimierung** aus.
3. Im Abschnitt **Ausnahmen**:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Dateien ausschließen**.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Nicht erkennen**.

- Klicken Sie für jede Einstellung auf die Schaltfläche **Ändern**, um Ausnahmen hinzuzufügen.

4. Im Abschnitt **Erweiterte Einstellungen**:
   - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**
   - **Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)**
   - **iSwift-Technologie verwenden**
   - **iChecker-Technologie verwenden**
5. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Konfigurieren des hierarchischen Speichers

So passen Sie die Aktionen für infizierte und andere gefundene Objekte für die Untersuchung auf Befehl an:

1. Öffnen Sie das Fenster **Untersuchungsbereich - Einstellungen**.
2. Klicken Sie auf die Registerkarte **Hierarchischer Speicher**.
3. Wählen Sie eine Aktion für die Dateien aus:
   - **Nicht untersuchen**.
   - **Nur den residenten Teil einer Datei untersuchen**.
   - **Datei vollständig untersuchen**.

     Wenn diese Aktion ausgewählt ist, können Sie die folgenden Optionen festlegen:
     - Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Nur, wenn auf die Datei innerhalb des angegebenen Zeitraums zugegriffen wurde (Tage)** und geben Sie die Anzahl von Tagen an.
     - Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datei, wenn möglich, nicht auf die lokale Festplatte kopieren**.
4. Klicken Sie auf **Speichern**.

Die neue Aufgabenkonfiguration wird gespeichert.

Wechseldatenträger untersuchen

Um die Untersuchung von Wechseldatenträgern bei ihrem Anschluss an das geschützte Gerät in der Programmkonsole anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **Kaspersky Embedded Systems Security** und wählen Sie die Option **Untersuchung von Wechseldatenträgern anpassen** aus.

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.

2. Im Abschnitt **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 automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.

   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)** und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.

   - Geben Sie in der Dropdown-Liste **Untersuchung starten mit Sicherheitsstufe** die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.

3. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert und übernommen.

Statistik von Aufgaben zur Untersuchung auf Befehl

Während eine Aufgabe zur Untersuchung auf Befehl ausgeführt wird, können Sie Informationen über Anzahl der Objekte, die Kaspersky Embedded Systems Security seit dem Aufgabenstart verarbeitet hat, anzeigen.

Diese Informationen stehen auch zur Verfügung, wenn Sie eine Aufgabe anhalten. Sie können die Aufgabenstatistik im Bericht über Aufgabenausführung aufrufen.

So zeigen Sie die Statistik einer Aufgabe zur Untersuchung auf Befehl an:

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten **Untersuchung auf Befehl**.

2. Wählen Sie die Aufgabe zur Untersuchung auf Befehl, deren Statistik Sie anzeigen möchten.

Im Ergebnisfenster des ausgewählten Knotens wird im Abschnitt **Statistik** eine Statistik der Aufgabe angezeigt.

Informationen über Objekte, die Kaspersky Embedded Systems Security seit dem Aufgabenstart verarbeitet hat, werden in der nachfolgenden Tabelle angezeigt.

Statistik von Aufgaben zur Untersuchung auf Befehl

Feld	Beschreibung
Gefunden	Anzahl der Objekte, die von Kaspersky Embedded Systems Security gefunden wurden. Findet Kaspersky Embedded Systems Security beispielsweise in fünf Dateien ein und dasselbe schädliche Objekt, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Infizierte und andere gefundene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security als infiziert eingestuft hat, oder der gefundenen legalen Softwaredateien, die nicht aus dem Untersuchungsbereich ausgeschlossen wurden und die als legitime Software klassifiziert wurden, die von Eindringlingen verwendet werden kann, um das Gerät oder persönliche Daten zu beschädigen.
Möglicherweise infizierte Objekte gefunden	Anzahl der von Kaspersky Embedded Systems Security erkannten Objekte, die als möglicherweise infiziert eingestuft wurden.
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security aus folgenden Gründen nicht desinfiziert wurden: • Das erkannte Objekt ist von einem Typ, der nicht desinfiziert werden kann.

	• Bei der Desinfektion ist eine Störung aufgetreten.
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos versucht hat, in die Quarantäne zu verschieben, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Nicht gelöschte Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos zu entfernen versucht hat, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht untersuchte Objekte	Anzahl der zum Schutzbereich gehörenden Objekte, die Kaspersky Embedded Systems Security nicht untersuchen konnte, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Embedded Systems Security erfolglos ins Backup zu kopieren versucht hat, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Verarbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden.
In Quarantäne verschoben	Anzahl der Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Embedded Systems Security im Backup gespeichert wurden.
Gelöschte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security entfernt wurden.
Kennwortgeschützte Objekte	Anzahl der Objekte (z. B. Archive), die von Kaspersky Embedded Systems Security übersprungen wurden, weil sie kennwortgeschützt sind.
Beschädigte Objekte	Anzahl der Objekte, die von Kaspersky Embedded Systems Security übersprungen wurden, da ihr Format beschädigt war.
Verarbeitete Objekte	Objekte insgesamt, die von Kaspersky Embedded Systems Security verarbeitet wurden.

Sie können auch eine Statistik der Aufgaben zur Untersuchung auf Befehl im Bericht über die Ausführung der gewählten Aufgabe über den Link **Protokoll der Aufgabenausführung öffnen** im Abschnitt **Verwaltung** des Ergebnisbereichs anzeigen.

Wir empfehlen, dass Sie nach Aufgabenabschluss die im Protokoll der Aufgabenausführung registrierten Ereignisse auf der Registerkarte **Ereignisse** manuell bearbeiten.

Aufgabe zur Überwachung der Baseline-Integrität erstellen und anpassen

Um eine neue Aufgabe zur Überwachung der Baseline-Integrität zu erstellen oder anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des Knotens **System-Diagnose**.
2. Wählen die **Aufgabe zur Überwachung der Baseline-Integrität erstellen**.

Das Fenster **Aufgabe hinzufügen** wird geöffnet.

3. Wählen Sie in der Dropdown-Liste **Algorithmus zur Hash-Berechnung** eine der folgenden Optionen aus:

   - **MD5**
   - **SHA256**

4. Gehen Sie in der Tabelle **Untersuchungsbereiche** wie folgt vor:

   a. Um eine Datei oder einen Ordner in den Aufgabenbereich der Überwachung der Baseline-Integrität aufzunehmen:

      1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

         Das Fenster **Eigenschaften des Untersuchungsbereichs** wird geöffnet.

      2. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Diesen Bereich untersuchen**.

      3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um die Datei oder den Ordner anzugeben, die bzw. der in den Aufgabenbereich der Überwachung der Baseline-Integrität aufgenommen werden soll.

      4. Aktivieren Sie das Kontrollkästchen **Unterordner ebenfalls untersuchen**, wenn Sie alle Unterordner in den Aufgabenbereich der Überwachung der Baseline-Integrität aufnehmen möchten.

      5. Klicken Sie auf **OK**.

   b. Um zuvor zum Aufgabenbereich der Überwachung der Baseline-Integrität hinzugefügte Dateien bzw. Ordner zu ändern, gehen Sie wie folgt vor:

      1. Klicken Sie auf die Schaltfläche **Ändern**.

         Das Fenster **Eigenschaften des Untersuchungsbereichs** wird geöffnet.

      2. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Diesen Bereich untersuchen**.

      3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um die Datei oder den Ordner anzugeben, die bzw. der in den Aufgabenbereich der Überwachung der Baseline-Integrität aufgenommen werden soll.

      4. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Unterordner ebenfalls untersuchen**, wenn Sie alle Unterordner in den Aufgabenbereich der Überwachung der Baseline-Integrität aufnehmen oder aus diesem ausschließen möchten.

      5. Klicken Sie auf **OK**.

   c. Um einen zuvor zum Aufgabenbereich der Überwachung der Baseline-Integrität hinzugefügte Dateien oder Ordner zu löschen, wählen Sie die entsprechende Datei bzw. den Ordner in der Tabelle **Untersuchungsbereiche** aus, und klicken Sie auf die Schaltfläche **Löschen**.

5. Passen Sie die Einstellungen für den Zeitplan für den Aufgabenstart auf den Registerkarten **Zeitplan** und **Erweitert** an.

6. Passen Sie auf der Registerkarte **Mit folgenden Rechten starten** die Einstellungen zum Starten der Aufgabe mit bestimmten Benutzerrechten an.

7. Klicken Sie im Fenster **Aufgabe hinzufügen** auf **OK**.

Eine neue benutzerdefinierte Aufgabe zur Überwachung der Baseline-Integrität wird erstellt. Der Knoten mit dem Namen der neuen Aufgabe wird in der Programmkonsolenstruktur angezeigt. Die Operation wird im Systemaudit-Protokoll erfasst.

Um die Einstellungen der Aufgabe zur Überwachung der Baseline-Integrität zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Programmkonsole den Knoten **System-Diagnose**.
2. Wählen Sie den untergeordneten Knoten aus, welcher der Aufgabe entspricht, die Sie konfigurieren möchten.
3. Klicken Sie im Ergebnisbereich des untergeordneten Knotens auf den Link **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.

Aufgaben zur Untersuchung auf Befehl über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Web-Plug-ins nach einem oder allen geschützten Geräten im Netzwerk navigieren.

Assistent für die Aufgabe zur Untersuchung auf Befehl öffnen

Um eine neue lokale Aufgabe zur Untersuchung auf Befehl zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Verwaltete Geräte** aus.
2. Klicken Sie auf die Registerkarte **Gruppen**, um die Administrationsgruppe auszuwählen, zu der das geschützte Gerät gehört.
3. Klicken Sie auf den Namen des geschützten Geräts.
4. Wählen Sie im nächsten Fenster **<Name des Geräts>** den Abschnitt **Aufgaben** aus.
5. Klicken Sie auf **Hinzufügen**.

   Daraufhin wird das Fenster **Assistent zum Hinzufügen von Aufgaben** geöffnet.
6. Wählen Sie in der Dropdown-Liste **Programm** die Option **Kaspersky Embedded Systems Security** aus.
7. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Eintrag **Untersuchung auf Befehl** aus.
8. Klicken Sie auf **Weiter**.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

Um eine neue Gruppenaufgabe zur Untersuchung auf Befehl zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.
2. Klicken Sie auf die Registerkarte **Gruppen**, um die Administrationsgruppe auszuwählen, für die Sie eine Aufgabe erstellen möchten.
3. Klicken Sie auf **Hinzufügen**.

Daraufhin wird das Fenster **Assistent zum Hinzufügen von Aufgaben** geöffnet.

4. Wählen Sie in der Dropdown-Liste **Programm** die Option **Kaspersky Embedded Systems Security** aus.
5. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Eintrag **Untersuchung auf Befehl** aus.
6. Klicken Sie auf **Weiter**.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

Um eine neue Aufgabe zur Untersuchung auf Befehl für eine benutzerdefinierte Gruppe zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Geräteauswahl** aus.
2. Wählen Sie aus, wofür Sie eine Aufgabe erstellen möchten.
3. Klicken Sie auf **Start**.
4. Wählen Sie im Fenster **Auswahlergebnisse** die Geräte aus, für die Sie eine Aufgabe erstellen möchten.
5. Klicken Sie auf **Neue Aufgabe**.
6. Wählen Sie in der Dropdown-Liste **Programm** die Option **Kaspersky Embedded Systems Security** aus.
7. Wählen Sie in der Dropdown-Liste **Aufgabentyp** den Eintrag **Untersuchung auf Befehl** aus.
8. Klicken Sie auf **Weiter**.

Konfigurieren Sie die Aufgabeneinstellungen nach Bedarf.

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

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Aufgaben** aus.
2. Klicken Sie in der Liste der Aufgaben von Kaspersky Security Center auf den Aufgabennamen.

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

Aufgabeneigenschaften für die Untersuchung auf Befehl öffnen

Um die Programmeinstellungen für die Aufgabe zur Untersuchung auf Befehl für ein einzelnes geschütztes Gerät zu öffnen, gehen wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Verwaltete Geräte** aus.
2. Klicken Sie auf die Registerkarte **Gruppen**, um die Administrationsgruppe auszuwählen, zu der das geschützte Gerät gehört.
3. Klicken Sie auf den Namen des geschützten Geräts.
4. Wählen Sie im nächsten Fenster **<Name des Geräts>** den Abschnitt **Aufgaben** aus.

5. Wählen Sie in der Liste der für das Gerät erstellten Aufgaben die Aufgabe zur Untersuchung auf Befehl aus, die Sie erstellt haben.

6. Öffnen Sie die Registerkarte **Programmeinstellungen**.

Untersuchungsbereich der Aufgabe anpassen

Um einen Untersuchungsbereich einer bestehenden Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Aufgabeneigenschaften für die Untersuchung auf Befehl.

2. Wählen Sie den Abschnitt **Untersuchungsbereich** aus.

3. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel hinzuzufügen.
   - Wählen Sie eine bestehende Regel aus und klicken Sie auf die Schaltfläche **Bearbeiten**.

   Das Fenster **Bereich ändern** wird geöffnet.

4. Stellen Sie die Umschaltfläche auf **Aktiv** wählen Sie einen Objekttyp aus.

5. Passen Sie im Abschnitt **Schutz von Objekten** folgende Einstellungen an:

   - **Schutzmodus für Objekte**:
     - **Alle Objekte**
     - **Objekte, die nach Format untersucht werden**
     - **Objekte, die entsprechend der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden**
     - **Objekte, die nach der angegebenen Erweiterungsliste untersucht werden**
   - **Untergeordnete Ordner**
   - **Untergeordnete Dateien**
   - **Bootsektoren und MBR untersuchen**
   - **Alternative NTFS-Ströme untersuchen**
   - Nur neue und veränderte Dateien schützen

6. Geben Sie im Abschnitt **Schutz von zusammengesetzten Objekten** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - **Archive**
   - **SFX-Archive**

- Gepackte Objekte
- E-Mail-Datenbanken
- E-Mails im Nur-Text-Format
- Eingebettete OLE-Objekte

7. Legen Sie im Abschnitt **Aktion für infizierte und andere Objekte** fest, welche Aktion auf infizierte und andere Objekte angewendet werden soll:
   - Nur informieren.
   - **Desinfizieren**.
   - **Desinfizieren. Löschen, falls Desinfektion fehlschlägt**.
   - Löschen.
   - **Empfohlen**.
8. Legen Sie im Abschnitt **Aktion für möglicherweise infizierte Objekte** fest, welche Aktion auf möglicherweise infizierte Objekte angewendet werden soll:
   - Nur informieren.
   - **Quarantäne**.
   - Löschen.
   - Empfohlen.
9. Aktivieren oder deaktivieren Sie im Abschnitt **Aktion für möglicherweise infizierte Objekte** das Kontrollkästchen Zusammengesetzte Datei vollständig entfernen, wenn diese im Falle eines gefundenen eingebetteten Objektes vom Programm nicht modifiziert werden kann.
10. Konfigurieren Sie im Abschnitt **Ausnahmen** die folgenden Einstellungen:
    - Deaktivieren oder aktivieren Sie das Kontrollkästchen Dateien ausschließen.
    - Deaktivieren oder aktivieren Sie das Kontrollkästchen Nicht erkennen.
11. Passen Sie im Abschnitt **Erweiterte Einstellungen** folgende Einstellungen an:
    - Untersuchung beenden, wenn sie länger dauert als (Sek.)
    - Zusammengesetzte Objekte nicht untersuchen, wenn größer als (MB)
    - iSwift-Technologie verwenden
    - iChecker-Technologie verwenden
12. Legen Sie im Abschnitt **Aktionen für autonome Dateien** fest, welche Aktion auf die Dateien angewendet werden soll:
    - **Nicht untersuchen**.

- **Nur den residenten Teil einer Datei untersuchen**.
- **Datei vollständig untersuchen**.

  Wenn diese Aktion ausgewählt ist, können Sie die folgenden Optionen festlegen:

  - Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Nur, wenn auf die Datei innerhalb des angegebenen Zeitraums zugegriffen wurde (Tage)** und geben Sie die Anzahl von Tagen an.
  - Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Datei, wenn möglich, nicht auf die lokale Festplatte kopieren**.

13. Klicken Sie auf die Schaltfläche **OK**.

Passen Sie die Aufgabeneinstellungen an

Um die Einstellungen einer bestehenden Aufgabe zur Untersuchung auf Befehl anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie die Aufgabeneigenschaften für die Untersuchung auf Befehl.
2. Wählen Sie den Abschnitt **Einstellungen** aus.
3. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.
4. Legen Sie in der Dropdown-Liste **Ebene der heuristischen Analyse** die Stufe der Analyse fest, falls benötigt.
5. Konfigurieren Sie im Abschnitt **Integration mit anderen Komponenten** die folgenden Einstellungen:
   - Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie Objekte, die zur Liste der vertrauenswürdigen Zonen hinzugefügt wurden, vom Untersuchungsbereich der Aufgabe ausschließen möchten.
   - Aktivieren Sie das Kontrollkästchen **KSN zur Überprüfung verwenden**, wenn Sie die Cloud-Dienste von Kaspersky Security Network für die Aufgabe nutzen möchten.
   - Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Priorität *Niedrig* zuzuweisen, aktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**.

     Arbeitsprozesse, in denen Aufgaben für Kaspersky Embedded Systems Security ausgeführt werden, haben standardmäßig die Priorität *Mittel* (Normal).

   - Um die erstellte Aufgabe als Untersuchung wichtiger Bereiche zu verwenden, aktivieren Sie das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten**.

Vertrauenswürdige Zone

Dieser Abschnitt enthält Informationen über die vertrauenswürdige Zone in Kaspersky Embedded Systems Security, Anweisungen zum Hinzufügen von Objekten in die vertrauenswürdige Zone sowie zur Anwendung der vertrauenswürdigen Zone beim Ausführen von Aufgaben.

Über die vertrauenswürdige Zone

Die vertrauenswürdige Zone ist eine Liste mit Ausschlüssen aus dem Schutz- oder Untersuchungsbereich, den Sie erstellen und auf folgende Aufgaben anwenden können: Untersuchung auf Befehl, Echtzeitschutz für Dateien mit Ausnahme der Untersuchung von Quarantäne-Objekten.

In den Aufgaben zum Echtzeitschutz für Dateien und zur Untersuchung auf Befehl wird die vertrauenswürdige Zone standardmäßig übernommen.

Sie können die Liste mit den Regeln für die Erstellung einer vertrauenswürdigen Zone in eine XML-Konfigurationsdatei exportieren, um sie später auf ein anderes geschütztes Gerät in Kaspersky Embedded Systems Security zu importieren.

Vertrauenswürdige Prozesse

Wird in den Aufgaben zum Echtzeitschutz für Dateien verwendet.

Bestimmte Programme auf dem geschützten Gerät können instabil werden, wenn Dateien, auf die das Programm zugreift, von Kaspersky Embedded Systems Security abgefangen werden. Zu diesen Anwendungen zählen beispielsweise Systemprogramme von Domain-Controllern.

Damit solche Programme nicht negativ beeinflusst werden, können Sie den Schutz für jene Dateien deaktivieren, auf welche die aktiven Prozesse dieser Programme zugreifen. Dazu wird in der vertrauenswürdigen Zone eine Liste mit vertrauenswürdigen Prozessen angelegt.

Microsoft empfiehlt, bestimmte Dateien des Betriebssystems Microsoft Windows und Programmdateien der Firma Microsoft als nicht infizierbar vom Echtzeitschutz für Dateien auszuschließen. Eine Auswahl der empfohlenen Ausnahmen finden Sie auf der Microsoft-Website (Artikelcode: KB822158).

Sie können das Übernehmen von vertrauenswürdigen Prozessen in der vertrauenswürdigen Zone aktivieren und deaktivieren.

> Wenn eine ausführbare Datei beispielsweise durch ein Update verändert wird, schließt Kaspersky Embedded Systems Security diese Datei aus der Liste vertrauenswürdiger Prozesse aus.

Das Programm übernimmt den Dateipfad auf einem geschützten Gerät nicht für die Kennzeichnung des Prozesses als vertrauenswürdig. Der Dateipfad auf dem geschützten Gerät wird nur für die Suche der Datei und die Berechnung ihrer Prüfsumme verwendet, sowie für das Informieren des Benutzers über die Quelle der ausführbaren Datei.

Backup-Operationen

Wird in den Aufgaben zum Echtzeit-Computerschutz verwendet.

Sie können den Schutz für Objekte, auf die beim Verschieben von Festplattendaten ins Backup auf externe Geräte zugegriffen wird, während der Backup-Operationen ausschalten. Kaspersky Embedded Systems Security untersucht Objekte, die vom Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden.

Ausnahmen

- Werden beim Echtzeitschutz für Dateien verwendet.
- Alle erkennbaren Objekte in den angegebenen Bereichen des geschützten Geräts.
- Festgelegte gefundene Objekte nach Name oder Namensmaske in allen Schutzbereichen bzw. Untersuchungsbereichen.

Vertrauenswürdige Zone über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie durch die Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und die vertrauenswürdige Zone für ein oder alle geschützten Geräte im Netzwerk konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Richtlinieneinstellungen der vertrauenswürdigen Zone öffnen

Um die vertrauenswürdige Zone über die Richtlinie für Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Zusätzlich**.
6. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Vertrauenswürdige Zone**.
   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

Konfigurieren Sie die vertrauenswürdige Zone nach Bedarf.

Wenn ein geschütztes Gerät durch eine aktive Richtlinie von Kaspersky Security Center verwaltet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht über die Programmkonsole geändert werden.

Einstellungsfenster der vertrauenswürdigen Zone öffnen

Um die vertrauenswürdige Zone im Fenster "Eigenschaften des Programms" zu verwalten, gehen Sie wie folgt vor:

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

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.
5. Wählen Sie im Abschnitt **Programme** die Option **Kaspersky Embedded Systems Security 3.1** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.
   Das Fenster mit den **Programmeinstellungen für Kaspersky Embedded Systems Security 3.1** geöffnet.
7. Wählen Sie den Abschnitt **Zusätzlich**.
8. Klicken Sie auf die Schaltfläche **Einstellungen** im Unterabschnitt **Vertrauenswürdige Zone**.
   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

Konfigurieren Sie die vertrauenswürdige Zone nach Bedarf.

Einstellungen der vertrauenswürdigen Zone über das Verwaltungs-Plug-in anpassen

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

So passen Sie die Einstellungen der vertrauenswürdigen Zone an:

1. Zu überspringende Objekte festlegen, mithilfe von Kaspersky Embedded Systems Security während der Aufgabenausführung auf der Registerkarte **Ausnahmen**.
2. Zu überspringende Prozesse festlegen mithilfe von Kaspersky Embedded Systems Security während der Aufgabenausführung auf der Registerkarte **Vertrauenswürdige Prozesse**.

3. Not-a-virus-Maske anwenden.

Ausnahme hinzufügen

Um eine Ausnahme zur vertrauenswürdigen Zone über die Richtlinie für Kaspersky Security Center hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Vertrauenswürdige Zone**.

2. Geben Sie auf der Registerkarte **Ausnahmen** die Objekte an, die Kaspersky Embedded Systems Security von der Untersuchung und vom Schutz ausnehmen soll:

   - Klicken Sie auf die Schaltfläche Empfohlene Ausnahmen hinzufügen, wenn Sie die empfohlenen Ausnahmen hinzufügen möchten.

   - Um vorkonfigurierte Ausnahmen zu importieren, klicken Sie auf die Schaltfläche **Import** und wählen Sie im neuen Fenster die Konfigurationsdatei im xml-Format auf Ihrem Gerät aus.

     Die Ausnahmen aus der xml-Datei werden zur Liste mit Ausnahmen hinzugefügt.

   - Wenn Sie die Bedingungen, bei deren Vorliegen ein Objekt als vertrauenswürdig eingestuft werden soll, manuell angeben möchten, klicken Sie auf **Hinzufügen** und fahren Sie mit den folgenden Schritten fort.

     Das Fenster **Ausnahme** wird geöffnet.

3. Wenn Sie im Abschnitt **Das Objekt wird unter folgenden Bedingungen nicht untersucht** auf die Schaltfläche **Hinzufügen** geklickt haben, geben Sie die Objekte an, die Sie aus dem Schutzbereich bzw. Untersuchungsbereich ausschließen möchten, und die Objekte, die Sie aus der Erkennung ausschließen möchten:

   - Wenn Sie ein Objekt aus dem Schutzbereich oder Untersuchungsbereich ausschließen möchten, gehen Sie wie folgt vor:

     a. Aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt**.

     b. Klicken Sie auf die Schaltfläche **Ändern**.

     Das Fenster **Wählen Sie ein Objekt aus** wird geöffnet.

     c. Geben Sie das Objekt an, das Sie aus dem Untersuchungsbereich ausschließen möchten.

     > Bei der Angabe der Objekte können Sie Namensmasken (über die Zeichen ? und *) und alle Arten von Umgebungsvariablen verwenden. Die Auflösung von Umgebungsvariablen (Ersetzen von Variablen durch ihre Werte) wird von Kaspersky Embedded Systems Security beim Starten einer Aufgabe oder beim Anwenden neuer Einstellungen auf eine ausgeführte Aufgabe durchgeführt (gilt nicht für Aufgaben zur Untersuchung auf Befehl). Kaspersky Embedded Systems Security löst Umgebungsvariablen unter dem Konto auf, mit dem die Aufgabe gestartet wurde. Weitere Informationen zu Umgebungsvariablen finden Sie in der Wissensdatenbank von Microsoft.

     d. Klicken Sie auf **OK**.

     e. Aktivieren Sie das Kontrollkästchen **Für Unterordner übernehmen**, wenn Sie alle untergeordneten Dateien und Order des angegebenen Objekts vom Schutzbereich oder Untersuchungsbereich ausschließen möchten.

- Wenn Sie den Namen eines erkennbaren Objekts angeben wollen:

  a. Aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**.

  b. Klicken Sie auf die Schaltfläche **Ändern**.

  Das Fenster **Liste der gefundenen Objekte** wird geöffnet.

  c. Geben Sie den Namen oder die Namensmaske des erkennbaren Objekts gemäß der Klassifizierung der Viren-Enzyklopädie an.

  d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

  e. Klicken Sie auf **OK**.

4. Aktivieren Sie im Abschnitt **Gültigkeitsbereich der Ausnahme** die Kontrollkästchen neben den Namen der Aufgaben, auf welche die Ausnahme angewendet werden soll.

5. Klicken Sie auf **OK**.

Die Ausnahme wird in der Liste in der Registerkarte **Ausnahmen** des Fensters **Vertrauenswürdige Zone** angezeigt.

Vertrauenswürdige Prozesse hinzufügen

Um einen oder mehrere Prozesse zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Vertrauenswürdige Zone**.

2. Wählen Sie die Registerkarte **Vertrauenswürdige Prozesse** aus.

3. Aktivieren Sie das Kontrollkästchen Datei-Aktivität beim Erstellen eines Backups nicht untersuchen, um die Untersuchung von Lesevorgängen für Dateien zu überspringen.

4. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**, um die Untersuchung von Dateivorgängen für vertrauenswürdige Prozesse zu überspringen.

5. Der Liste der vertrauenswürdigen Prozesse können auf zwei Arten Prozesse hinzugefügt werden:

   - Um vorkonfigurierte vertrauenswürdige Prozesse zu importieren, klicken Sie auf die Schaltfläche **Import** und wählen Sie im neuen Fenster die Konfigurationsdatei im xml-Format auf Ihrem Gerät aus.

     Prozesse aus der XML-Datei werden der Liste mit vertrauenswürdigen Prozessen hinzugefügt.

   - Um den Prozess manuell anzugeben, klicken Sie auf die Schaltfläche **Hinzufügen** und fahren Sie mit den folgenden Schritten fort.

6. Wenn Sie im Kontextmenü der Schaltfläche die Option **Hinzufügen** angeklickt haben, wählen Sie eine der drei Optionen aus:

   - **Mehrere Prozesse.**

     Nehmen Sie im nächsten Fenster **Vertrauenswürdige Prozesse hinzufügen** folgende Einstellungen vor:

     a. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**.

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

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 Gerät, auf dem Kaspersky Embedded Systems Security installiert ist, über Administratorrechte verfügen, damit die Liste der aktiven Prozesse angezeigt werden kann. Sie können die Prozesse in der Liste der aktiven Prozesse nach Dateinamen, Prozess-ID (PID) oder Pfad der ausführbaren Prozessdatei auf dem geschützten Gerät sortieren. Beachten Sie, dass Sie laufende Prozesse auswählen können, indem Sie auf die Schaltfläche **Prozesse** klicken und nur die Programmkonsole auf einem geschützten Gerät oder in den angegebenen Host-Einstellungen über Kaspersky Security Center verwenden.

- **Einen Prozess aufgrund von Dateiname und Pfad**.

  Gehen Sie im nächsten Fenster **Hinzufügen eines Prozesses** wie folgt vor:

  a. Geben Sie einen Pfad zu einer ausführbaren Datei (inklusive Dateiname) an.

  > Bei der Angabe der Objekte können Sie Namensmasken (über die Zeichen ? und *) und alle Arten von Umgebungsvariablen verwenden. Die Auflösung von Umgebungsvariablen (Ersetzen von Variablen durch ihre Werte) wird von Kaspersky Embedded Systems Security beim Starten einer Aufgabe oder beim Anwenden neuer Einstellungen auf eine ausgeführte Aufgabe durchgeführt (gilt nicht für Aufgaben zur Untersuchung auf Befehl). Kaspersky Embedded Systems Security löst Umgebungsvariablen unter dem Konto auf, mit dem die Aufgabe gestartet wurde. Weitere Informationen zu Umgebungsvariablen finden Sie in der Wissensdatenbank von Microsoft.

  b. Klicken Sie auf **OK**.

- **Einen Prozess aufgrund der Objekteigenschaften**.

  Nehmen Sie im nächsten Fenster **Hinzufügen eines vertrauenswürdigen Prozesses** folgende Einstellungen vor:

  a. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie einen Prozess aus.

  b. Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden.

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

  d. Klicken Sie auf **OK**.

Um den ausgewählten Prozess zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, muss mindestens ein Kriterium für Vertrauenswürdigkeit ausgewählt sein.

7. Klicken Sie im Fenster **Vertrauenswürdige Zone** 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, die Untersuchung legitimer Softwaredateien und Webressourcen, die als schädlich eingestuft werden, zu überspringen. Die Maske wirkt sich auf folgende Aufgaben aus:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl

Wenn die Maske nicht zur Liste mit Ausnahmen hinzugefügt wird, wendet Kaspersky Embedded Systems Security die Aktion an, die in den Aufgabeneinstellungen der Software, die zu dieser Kategorie gehört, festgelegt ist.

Um die Not-a-virus-Maske zu verwenden, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Vertrauenswürdige Zone**.
2. Scrollen Sie auf der Registerkarte **Ausnahmen** in der Spalte **Zu erkennende Objekte** in der Liste nach unten und wählen Sie die Zeile mit dem Wert not-a-virus:* aus, wenn das Kontrollkästchen deaktiviert ist.
3. Klicken Sie auf OK.

   Die neue Konfiguration wird übernommen.

Vertrauenswürdige Zone über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie durch die Benutzeroberfläche der Programmkonsole navigieren und die vertrauenswürdige Zone auf einem geschützten Gerät konfigurieren.

Vertrauenswürdige Zone für Aufgaben in der Programmkonsole übernehmen

Die vertrauenswürdige Zone wird standardmäßig in der Aufgabe "Echtzeitschutz für Dateien", in vom Benutzer neu erstellten Aufgaben zur Untersuchung auf Befehl sowie in allen Systemaufgaben zur Untersuchung auf Befehl angewendet. Eine Ausnahme bildet die Aufgabe zur Untersuchung von Quarantäne-Objekten.

Nachdem die vertrauenswürdige Zone aktiviert bzw. deaktiviert wurde, werden die für sie festgelegten Ausnahmen in den laufenden Aufgaben sofort wirksam bzw. unwirksam.

Um die Übernahme der vertrauenswürdigen Zone für die Aufgaben von Kaspersky Embedded Systems Security zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü der Aufgabe, für die Sie die Verwendung der vertrauenswürdigen Zone anpassen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

   Das Fenster **Aufgabeneinstellungen** wird geöffnet.
3. Wählen Sie im nächsten Fenster auf der Registerkarte **Allgemein** eine der folgenden Aktionen aus:

   - Wenn Sie die vertrauenswürdige Zone in der Aufgabe übernehmen möchten, aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**.
   - Wenn Sie die Übernahme der vertrauenswürdigen Zone in der Aufgabe deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**.
4. Wenn Sie die Einstellungen der vertrauenswürdigen Zone anpassen möchten, klicken Sie auf den Link im Namen des Kontrollkästchens **Vertrauenswürdige Zone anwenden**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

   Konfigurieren Sie im Fenster **Vertrauenswürdige Zone** die Ausnahmen und vertrauenswürdigen Prozesse und klicken Sie auf **OK**.
5. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**, um die Änderungen zu speichern.

Einstellungen der vertrauenswürdigen Zone in der Programmkonsole konfigurieren

So passen Sie die Einstellungen der vertrauenswürdigen Zone an:

1. Zu überspringende Objekte festlegen, mithilfe von Kaspersky Embedded Systems Security während der Aufgabenausführung auf der Registerkarte **Ausnahmen**.
2. Zu überspringende Prozesse festlegen mithilfe von Kaspersky Embedded Systems Security während der Aufgabenausführung auf der Registerkarte **Vertrauenswürdige Prozesse**.
3. Vertrauenswürdige Zone für die Programmaufgaben übernehmen.
4. Not-a-virus-Maske anwenden.

Ausnahme zur vertrauenswürdigen Zone hinzufügen

Um eine Ausnahme über die Programmkonsole manuell zur vertrauenswürdigen Zone hinzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.
2. Wählen Sie die Menüoption **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
3. Wählen Sie die Registerkarte **Ausnahmen** aus.

4. Legen Sie die Objekte fest, die von Kaspersky Embedded Systems Security während der Untersuchung und vom Schutz ausgenommen werden sollen:

   - Um vorkonfigurierte Ausnahmen zu importieren, klicken Sie auf die Schaltfläche **Import** und wählen Sie im neuen Fenster die Konfigurationsdatei im xml-Format auf Ihrem Gerät aus.

     Die Ausnahmen aus der xml-Datei werden zur Liste mit Ausnahmen hinzugefügt.

   - Wenn Sie die Bedingungen, bei deren Vorliegen ein Objekt als vertrauenswürdig eingestuft werden soll, manuell angeben möchten, klicken Sie auf **Hinzufügen** und fahren Sie mit den folgenden Schritten fort.

     Das Fenster **Ausnahme** wird geöffnet.

5. Wenn Sie im Abschnitt **Das Objekt wird unter folgenden Bedingungen nicht untersucht** auf die Schaltfläche **Hinzufügen** geklickt haben, geben Sie die Objekte an, die Sie aus dem Schutzbereich bzw. Untersuchungsbereich ausschließen möchten, und die Objekte, die Sie aus der Erkennung ausschließen möchten:

   - Wenn Sie ein Objekt aus dem Schutzbereich oder Untersuchungsbereich ausschließen möchten, gehen Sie wie folgt vor:

     a. Aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt**.

     b. Klicken Sie auf die Schaltfläche **Ändern**.

        Das Fenster **Wählen Sie ein Objekt aus** wird geöffnet.

     c. Geben Sie das Objekt an, das Sie aus dem Untersuchungsbereich ausschließen möchten.

        Bei der Angabe der Objekte können Sie Namensmasken (über die Zeichen ? und *) und alle Arten von Umgebungsvariablen verwenden. Die Auflösung von Umgebungsvariablen (Ersetzen von Variablen durch ihre Werte) wird von Kaspersky Embedded Systems Security beim Starten einer Aufgabe oder beim Anwenden neuer Einstellungen auf eine ausgeführte Aufgabe durchgeführt (gilt nicht für Aufgaben zur Untersuchung auf Befehl). Kaspersky Embedded Systems Security löst Umgebungsvariablen unter dem Konto auf, mit dem die Aufgabe gestartet wurde. Weitere Informationen zu Umgebungsvariablen finden Sie in der Wissensdatenbank von Microsoft.

     d. Klicken Sie auf **OK**.

     e. Aktivieren Sie das Kontrollkästchen **Für Unterordner übernehmen**, wenn Sie alle untergeordneten Dateien und Order des angegebenen Objekts vom Schutzbereich oder Untersuchungsbereich ausschließen möchten.

   - Wenn Sie den Namen eines erkennbaren Objekts angeben wollen:

     a. Aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**.

     b. Klicken Sie auf die Schaltfläche **Ändern**.

        Das Fenster **Liste der gefundenen Objekte** wird geöffnet.

     c. Geben Sie den Namen oder die Namensmaske des erkennbaren Objekts gemäß der Klassifizierung der Viren-Enzyklopädie an.

     d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

     e. Klicken Sie auf **OK**.

6. Aktivieren Sie im Abschnitt **Gültigkeitsbereich der Ausnahme** die Kontrollkästchen neben den Namen der Aufgaben, auf welche die Ausnahme angewendet werden soll.

7. Klicken Sie auf **OK**.

Die Ausnahme wird in der Liste in der Registerkarte **Ausnahmen** des Fensters **Vertrauenswürdige Zone** angezeigt.

Vertrauenswürdige Prozesse hinzufügen

Ein Prozess kann der Liste der vertrauenswürdigen Prozesse auf zwei Arten hinzugefügt werden:

- Prozess aus der Liste der Prozesse auswählen, die auf dem geschützten Gerät aktiv sind.
- Die ausführbare Datei des Prozesses auswählen, unabhängig davon, ob der Prozess gerade aktiv ist oder nicht.

> Wenn die ausführbare Datei eines Prozesses verändert wird, löscht Kaspersky Embedded Systems Security den Prozess aus der Liste der vertrauenswürdigen Prozesse.

Um einen oder mehrere Prozesse zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.

2. Wählen Sie die Menüoption **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

3. Wählen Sie die Registerkarte **Vertrauenswürdige Prozesse** aus.

4. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität beim Erstellen eines Backups nicht untersuchen**, um die Untersuchung von Lesevorgängen für Dateien zu überspringen.

5. Aktivieren Sie das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**, um die Untersuchung von Dateivorgängen für vertrauenswürdige Prozesse zu überspringen.

6. Der Liste der vertrauenswürdigen Prozesse können auf zwei Arten Prozesse hinzugefügt werden:

   - Um vorkonfigurierte vertrauenswürdige Prozesse zu importieren, klicken Sie auf die Schaltfläche **Import** und wählen Sie im neuen Fenster die Konfigurationsdatei im xml-Format auf Ihrem Gerät aus.

     Prozesse aus der XML-Datei werden der Liste mit vertrauenswürdigen Prozessen hinzugefügt.

   - Um den Prozess manuell anzugeben, klicken Sie auf die Schaltfläche **Hinzufügen** und fahren Sie mit den folgenden Schritten fort.

7. Wenn Sie im Kontextmenü der Schaltfläche die Option **Hinzufügen** angeklickt haben, wählen Sie eine der drei Optionen aus:

   - **Mehrere Prozesse.**

     Nehmen Sie im nächsten Fenster **Vertrauenswürdige Prozesse hinzufügen** folgende Einstellungen vor:

     a. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**.

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

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 Gerät, auf dem Kaspersky Embedded Systems Security installiert ist, über Administratorrechte verfügen, damit die Liste der aktiven Prozesse angezeigt werden kann. Sie können die Prozesse in der Liste der aktiven Prozesse nach Dateinamen, Prozess-ID (PID) oder Pfad der ausführbaren Prozessdatei auf dem geschützten Gerät sortieren. Beachten Sie, dass Sie laufende Prozesse auswählen können, indem Sie auf die Schaltfläche **Prozesse** klicken und nur die Programmkonsole auf einem geschützten Gerät oder in den angegebenen Host-Einstellungen über Kaspersky Security Center verwenden.

- **Einen Prozess aufgrund von Dateiname und Pfad**.

  Gehen Sie im nächsten Fenster **Hinzufügen eines Prozesses** wie folgt vor:

  a. Geben Sie einen Pfad zu einer ausführbaren Datei (inklusive Dateiname) an.

  Bei der Angabe der Objekte können Sie Namensmasken (über die Zeichen `?` und `*`) und alle Arten von Umgebungsvariablen verwenden. Die Auflösung von Umgebungsvariablen (Ersetzen von Variablen durch ihre Werte) wird von Kaspersky Embedded Systems Security beim Starten einer Aufgabe oder beim Anwenden neuer Einstellungen auf eine ausgeführte Aufgabe durchgeführt (gilt nicht für Aufgaben zur Untersuchung auf Befehl). Kaspersky Embedded Systems Security löst Umgebungsvariablen unter dem Konto auf, mit dem die Aufgabe gestartet wurde. Weitere Informationen zu Umgebungsvariablen finden Sie in der Wissensdatenbank von Microsoft.

  b. Klicken Sie auf **OK**.

- **Einen Prozess aufgrund der Objekteigenschaften**.

  Nehmen Sie im nächsten Fenster **Hinzufügen eines vertrauenswürdigen Prozesses** folgende Einstellungen vor:

  a. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie einen Prozess aus.

  b. Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden.

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

  d. Klicken Sie auf **OK**.

Um den ausgewählten Prozess zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, muss mindestens ein Kriterium für Vertrauenswürdigkeit ausgewählt sein.

8. Klicken Sie im Fenster **Vertrauenswürdige Zone** 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, die Untersuchung legitimer Softwaredateien und Webressourcen, die als schädlich eingestuft werden, zu überspringen. Die Maske wirkt sich auf folgende Aufgaben aus:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl

Wenn die Maske nicht zur Liste mit Ausnahmen hinzugefügt wird, wendet Kaspersky Embedded Systems Security die Aktion an, die in den Aufgabeneinstellungen der Software oder der Webressource, die zu dieser Kategorie gehört, festgelegt ist.

Um die Not-a-virus-Maske zu verwenden, gehen Sie wie folgt vor:

1. Öffnen Sie in der Struktur der Programmkonsole das Kontextmenü des **Kaspersky Embedded Systems Security** Hauptknotens.
2. Wählen Sie die Menüoption **Einstellungen der vertrauenswürdigen Zone anpassen** aus.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
3. Wählen Sie die Registerkarte **Ausnahmen** aus.
4. Scrollen Sie in der Liste nach unten und suchen Sie den Wert *Not-a-virus:**.
5. Aktivieren Sie das entsprechende Kontrollkästchen, wenn es nicht aktiviert ist.
6. Klicken Sie auf **OK**.

Die neue Konfiguration wird übernommen.

Vertrauenswürdige Zone über das Web-Plug-in verwalten

So konfigurieren Sie die vertrauenswürdige Zone über das Web-Plug-in:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Zusätzlich**.

5. Klicken Sie im Unterabschnitt **Vertrauenswürdige Zone** auf **Einstellungen**.

6. Konfigurieren Sie die vertrauenswürdige Zone nach Bedarf.

Exploit-Prävention

Dieser Abschnitt enthält eine Anleitung für die Konfiguration des Schutzes des Prozess-Speichers vor der Ausnutzung von Schwachstellen.

Über die Exploit-Prävention

Kaspersky Embedded Systems Security bietet eine Möglichkeit zum Schutz des Prozess-Speichers vor Exploits. Diese Funktion ist in der Komponente "Exploit-Prävention" implementiert. Sie können den Status der Aktivität der Komponente ändern und die 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, 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 das geschützte Gerät neu gestartet werden (z. B. wenn der Systemprozess geschützt ist).

Wenn Anzeichen für einen Exploit-Angriff auf den geschützten Prozess gefunden werden, führt Kaspersky Embedded Systems Security eine der folgenden Aktionen aus:

- Prozess wird bei einem Exploit-Versuch beendet
- Benachrichtigung über die Ausnutzung einer Schwachstelle im Prozess wird ausgelöst

Sie können den Schutz von Prozessen auf eine der folgenden Weisen beenden:

- Komponente deinstallieren
- Prozess aus der Liste der geschützten Prozesse entfernen und neu starten

Kaspersky Security Exploit Prevention Service

Um eine möglichst effektive Nutzung der Funktionen der Komponente "Exploit-Prävention" zu gewährleisten, muss auf dem geschützten Gerät Kaspersky Security Exploit Prevention Service vorhanden sein. Dieser Dienst ist zusammen mit der Komponente "Exploit-Prävention" Bestandteil der empfohlenen Installation. Während der Installation des Dienstes auf dem geschützten Gerät wird der Prozess kavfswh erstellt und gestartet. Auf diese Art werden Informationen über geschützte Prozesse von der Komponente an den Security Agenten gesendet

Nach dem Beenden von Kaspersky Security Exploit Prevention Service schützt Kaspersky Embedded Systems Security auch weiterhin die Prozesse, die zur Liste der geschützten Prozesse hinzugefügt wurden. Darüber hinaus wird das Programm in neu hinzugefügte Prozesse geladen und wendet alle verfügbaren Verfahren zur Exploit-Prävention an, um den Prozess-Speicher zu schützen.

Wenn Ihr Gerät unter dem Betriebssystem Windows 10 oder höher läuft, wird das Programm nach dem Beenden von Kaspersky Security Exploit Prevention Service die Prozesse und den Prozess-Speicher nicht länger schützen.

Sollte Kaspersky Security Exploit Prevention Service beendet werden, erhält das Programm nicht länger Daten zu Ereignissen, die für geschützte Prozesse auftreten (darunter auch Daten über Exploit-Angriffe und das Beenden von Prozessen). Der Agent kann auch nicht länger Daten über neue Schutzeinstellungen und über das Hinzufügen neuer Prozesse zur Liste der geschützten Prozesse erhalten.

Modus der Exploit-Prävention

Sie können die getroffenen Aktionen zur Minderung der Risiken einer Ausnutzung von Schwachstellen in geschützten Prozessen anpassen, indem Sie einen von zwei Modi auswählen:

- **Bei Exploit beenden**: Wenden Sie diesen Modus an, um den Prozess beim Versuch der Ausnutzung einer Schwachstelle zu beenden.

  Wenn eine versuchte Ausnutzung einer Schwachstelle in einem geschützten Prozess gefunden wird, die im Betriebssystem als kritisch eingestuft ist, beendet Kaspersky Embedded Systems Security den Prozess nicht – unabhängig vom Modus, der in den Einstellungen der Komponente "Exploit-Prävention" angegeben ist.

- **Nur informieren**: Wenden Sie diesen Modus an, um mithilfe von Ereignissen im Sicherheitsprotokoll Daten über Exploits in geschützten Prozessen zu erhalten.

  Wenn dieser Modus ausgewählt ist, erstellt Kaspersky Embedded Systems Security Ereignisse, um alle Versuche zu protokollieren, mit denen Schwachstellen aufgedeckt werden sollen.

Exploit-Prävention über das Verwaltungs-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Verwaltungs-Plug-ins navigieren und Komponenteneinstellungen für einen oder alle geschützte Geräte im Netzwerk konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Richtlinieneinstellungen für die Exploit-Prävention öffnen

Um die Einstellungen der Exploit-Prävention über die Richtlinie von Kaspersky Security Center zu öffnen, gehen Sie wie folgt vor:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Richtlinie** aus.
4. Doppelklicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
5. Wählen Sie im nächsten Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Echtzeit-Computerschutz** aus.
6. Klicken Sie im Unterabschnitt **Exploit-Prävention** auf die Schaltfläche **Einstellungen**.

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

Konfigurieren Sie die Exploit-Prävention nach Bedarf.

Einstellungsfenster der Exploit-Prävention öffnen

So öffnen Sie das Eigenschaftsfenster für die Exploit-Prävention:

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Wählen Sie die Administrationsgruppe aus, für die Sie die Aufgabe konfigurieren möchten.
3. Wählen Sie die Registerkarte **Geräte** aus.
4. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Name des geschützten Geräts>** zu öffnen:

   - Doppelklicken Sie auf den Namen des geschützten Geräts.
   - Wählen Sie das Element **Eigenschaften** aus dem Kontextmenü des geschützten Geräts aus.

   Das Fenster **Eigenschaften: <Name des geschützten Geräts>** wird geöffnet.
5. Wählen Sie im Abschnitt **Programme** die Option **Kaspersky Embedded Systems Security 3.1** aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster mit den **Programmeinstellungen für Kaspersky Embedded Systems Security 3.1** geöffnet.
7. Wählen Sie den Unterabschnitt **Echtzeit-Computerschutz** aus.
8. Klicken Sie im Unterabschnitt **Exploit-Prävention** auf die Schaltfläche **Einstellungen**.

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

Konfigurieren Sie die Exploit-Prävention nach Bedarf.

Einstellungen zum Schutz des Prozess-Speichers anpassen

Um die Einstellungen zum Schutz des Prozess-Speichers für die Prozesse anzupassen, die zur Liste mit geschützten Prozessen hinzugefügt wurden, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Exploit-Prävention**.
2. Konfigurieren Sie im Block **Modus der Exploit-Prävention** die folgenden Einstellungen:
   - **Exploit von Prozessen mit Schwachstellen verhindern**.
     - **Bei Exploit beenden**.
     - **Nur informieren**.
3. Konfigurieren Sie im Block **Aktionen zur Vorbeugung** die folgenden Einstellungen:
   - **Mittels Terminaldienst über missbräuchlich verwendete Prozesse benachrichtigen**.
   - **Exploit von Prozessen mit Schwachstellen auch verhindern, wenn Kaspersky Security Service deaktiviert ist**.
4. Klicken Sie im Fenster **Exploit-Prävention** auf **OK**.

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

Hinzufügen eines Prozesses zum Schutzbereich

Die Komponente "Exploit-Prävention" schützt standardmäßig mehrere Prozesse. Sie können diesen Prozess vom Schutzbereich ausschließen, indem Sie die entsprechenden Kontrollkästchen in der Liste deaktivieren.

Um einen Prozess zur Liste mit geschützten Prozessen hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Exploit-Prävention**.
2. Klicken Sie auf der Registerkarte **Geschützte Prozesse** auf die Schaltfläche **Durchsuchen**.

   Ein Microsoft-Windows-Explorer-Fenster wird geöffnet.
3. Wählen Sie den Prozess aus, den Sie zur Liste hinzufügen möchten.
4. Klicken Sie auf **Öffnen**.

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

   Der angegebene Prozess wird zur Liste der geschützten Prozesse hinzugefügt.
6. Wählen Sie den hinzugefügten Prozess aus.

7. Klicken Sie auf **Verfahren zur Exploit-Prävention angeben**.

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

8. Wählen Sie eine der Varianten zur Anwendung der Verfahren zur Risikominderung aus:

   - **Alle verfügbaren Methoden zur Exploit-Prävention anwenden**.

     Wenn diese Einstellung ausgewählt ist, kann die Liste nicht geändert werden. Standardmäßig werden alle verfügbaren Techniken für einen Prozess angewendet.

   - **Folgende Verfahren zur Exploit-Prävention anwenden.**

     Wenn diese Variante ausgewählt ist, können Sie die Liste der angewendeten Verfahren zur Risikominderung bearbeiten:

     a. Aktivieren Sie die Kontrollkästchen der Verfahren, die Sie zum Schutz des ausgewählten Prozesses anwenden möchten.

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

9. Passen Sie die Einstellungen 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 URL**
     - **Verbotene URL**
     - **Computer**

     Diese Einstellungen gelten nur für Internet Explorer®.

10. Klicken Sie auf **OK**.

    Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Exploit-Prävention über die Programmkonsole verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche der Programmkonsole navigieren und die Komponenteneinstellungen auf einem geschützten Gerät konfigurieren.

Navigation

Erfahren Sie, wie Sie mit der ausgewählten Benutzeroberfläche zu den gewünschten Aufgabeneinstellungen navigieren.

Allgemeine Einstellungen der Exploit-Prävention öffnen

*Um das Fenster **Einstellungen zur Exploit-Prävention** zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Echtzeitschutz für Dateien**.
2. Wählen Sie den Knoten **Exploit-Prävention**.
3. Klicken Sie in dem Bereich Einstellungen zum Schutz von Prozessen auf den Link **Eigenschaften**.
   Das Fenster **Einstellungen zur Exploit-Prävention** wird geöffnet.

Passen Sie die allgemeinen Einstellungen für die Exploit-Prävention nach Bedarf an.

Einstellungen der Exploit-Prävention für den Schutz von Prozessen öffnen

*Um das Fenster ***Einstellungen zum Schutz von Prozessen*** zu öffnen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Programmkonsole den Knoten **Echtzeitschutz für Dateien**.
2. Wählen Sie den Knoten **Exploit-Prävention**.

In dem Bereich Einstellungen zum Schutz von Prozessen klicken Sie auf den Link **Parameter des Prozess-Schutzes**.

Das Fenster Einstellungen zum Schutz von Prozessen wird geöffnet.

Passen Sie die Einstellungen der Exploit-Prävention für den Schutz von Prozessen nach Bedarf an.

Einstellungen zum Schutz des Prozess-Speichers anpassen

Um einen Prozess zur Liste mit geschützten Prozessen hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster Einstellungen zur Exploit-Prävention.
2. Konfigurieren Sie im Block **Modus der Exploit-Prävention** die folgenden Einstellungen:
   - Exploit von Prozessen mit Schwachstellen verhindern.
     - Bei Exploit beenden.
     - Nur informieren.
3. Konfigurieren Sie im Block **Aktionen zur Vorbeugung** die folgenden Einstellungen:
   - Mittels Terminaldienst über missbräuchlich verwendete Prozesse benachrichtigen.

- **Exploit von Prozessen mit Schwachstellen auch verhindern, wenn Kaspersky Security Service deaktiviert ist**.

4. Klicken Sie im Fenster **Einstellungen zur Exploit-Prävention** auf **OK**.

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

Hinzufügen eines Prozesses zum Schutzbereich

Die Komponente "Exploit-Prävention" schützt standardmäßig mehrere Prozesse. Sie können die Auswahl der Prozesse, die nicht geschützt werden sollen, in der Liste mit geschützten Prozesse aufheben.

Um einen Prozess zur Liste mit geschützten Prozessen hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Einstellungen zum Schutz von Prozessen**.
2. Um einen Prozess hinzuzufügen, um ihn vor Missbrauch zu schützen und die möglichen Auswirkungen eines Exploits zu beschränken, gehen Sie wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Durchsuchen**.
      Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.
   b. Wählen Sie im folgenden Fenster den Prozess aus, den Sie zur Liste hinzufügen möchten.
   c. Klicken Sie auf **Öffnen**.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.
      Der angegebene Prozess wird zur Liste der geschützten Prozesse hinzugefügt.
3. Wählen Sie einen hinzugefügten Prozess in der Liste aus.
4. Die aktuelle Konfiguration wird auf der Registerkarte **Einstellungen zum Schutz von Prozessen** angezeigt:
   - **Prozessname**.
   - **Wird ausgeführt**.
   - **Angewendete Verfahren zur Exploit-Prävention.**
   - **Reduzierung des Handlungsbereichs des Prozesses (Einstellungen der Technologie Attack Surface Reduction).**
5. Um die auf den gegebenen Prozess angewendeten Verfahren zur Exploit-Prävention zu bearbeiten, wählen Sie die Registerkarte **Laden von Modulen verbieten**.
6. Wählen Sie eine der Varianten zur Anwendung der Verfahren zur Risikominderung aus:
   - **Alle verfügbaren Methoden zur Exploit-Prävention anwenden**.
     Wenn diese Einstellung ausgewählt ist, kann die Liste nicht geändert werden. Standardmäßig werden alle verfügbaren Techniken für einen Prozess angewendet.
   - **Angeführte Verfahren zur Exploit-Prävention für den Prozess anwenden**.

Wenn diese Variante ausgewählt ist, können Sie die Liste der angewendeten Verfahren zur Risikominderung bearbeiten:

a. Aktivieren Sie die Kontrollkästchen der Verfahren, die Sie zum Schutz des ausgewählten Prozesses anwenden möchten.

7. Passen Sie die Einstellungen 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 Abschnitt **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 URL**
  - **Verbotene Websites**
  - **Computer**

Diese Einstellungen gelten nur für Internet Explorer®.

8. Klicken Sie auf **Speichern**.

Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Exploit-Prävention über das Web-Plug-in verwalten

In diesem Abschnitt erfahren Sie, wie Sie in der Benutzeroberfläche des Web-Plug-ins navigieren und die Komponenteneinstellungen auf einem geschützten Gerät konfigurieren.

Einstellungen zum Schutz des Prozess-Speichers anpassen

Um die Einstellungen zum Schutz des Prozess-Speichers für die Prozesse anzupassen, die zur Liste mit geschützten Prozessen hinzugefügt wurden, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Unterabschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Exploit-Prävention** auf **Einstellungen**.

6. Öffnen Sie die Registerkarte **Einstellungen zur Exploit-Prävention**.
7. Konfigurieren Sie im Block **Modus der Exploit-Prävention** die folgenden Einstellungen:
   - **Exploit von Prozessen mit Schwachstellen verhindern**.
     - **Bei Exploit beenden**.
     - **Nur informieren**.
8. Konfigurieren Sie im Block **Aktionen zur Vorbeugung** die folgenden Einstellungen:
   - **Mittels Terminaldienst über missbräuchlich verwendete Prozesse benachrichtigen**.
   - **Exploit von Prozessen mit Schwachstellen auch verhindern, wenn Kaspersky Security Service deaktiviert ist**.
9. Klicken Sie im Fenster **Exploit-Prävention** auf **OK**.

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

Hinzufügen eines Prozesses zum Schutzbereich

Um die Einstellungen zum Schutz des Prozess-Speichers für die Prozesse anzupassen, die zur Liste mit geschützten Prozessen hinzugefügt wurden, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster der Web-Konsole **Geräte** → **Richtlinien & Profile** aus.
2. Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten.
3. Wählen Sie im Fenster **<Name der Richtlinie>** die Registerkarte **Programmeinstellungen** aus.
4. Wählen Sie den Abschnitt **Echtzeitschutz für Computer** aus.
5. Klicken Sie im Unterabschnitt **Exploit-Prävention** auf **Einstellungen**.
6. Öffnen Sie die Registerkarte **Geschützte Prozesse**.
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.
8. Das Fenster **Verfahren zur Exploit-Prävention** wird geöffnet.
9. Geben Sie den Prozessnamen an.
10. 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. Standardmäßig werden alle verfügbaren Techniken für einen Prozess angewendet.
    - **Folgende Verfahren zur Exploit-Prävention anwenden.**

      Wenn diese Variante ausgewählt ist, können Sie die Liste der angewendeten Verfahren zur Risikominderung bearbeiten:

a. Aktivieren Sie die Kontrollkästchen der Verfahren, die Sie zum Schutz des ausgewählten Prozesses anwenden möchten.

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

11. 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 URL**
  - **Verbotene URL**
  - **Computer**

Diese Einstellungen gelten nur für Internet Explorer®.

12. Klicken Sie auf **OK**.

Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Exploit-Präventionstechniken

Exploit-Präventionstechniken

Verfahren zur Exploit-Prävention	Beschreibung
Data Execution Prevention (DEP)	Verhinderung einer Ausführung von Daten – Verbot der Ausführung eines zufälligen Codes im geschützten Speicherbereich.
Address Space Layout Randomization (ASLR)	Zufallsgestaltung der Datenstruktur im Adressraum des Prozesses.
Structured Exception Handler Overwrite Protection (SEHOP)	Auswechslung des Eintrags in der Struktur der Ausnahmen oder Auswechslung des Ausnahmehandlers.
Null Page Allocation	Verhinderung der Umorientierung des Nullregisters.
LoadLibrary Network Call Check (Anti ROP)	Schutz vor dem Download dynamischer Bibliotheken von Netzwerkpfaden.
Executable Stack (Anti ROP)	Verbot der unbefugten Verwendung des Stapelbereichs.
Anti RET Check (Anti ROP)	Untersuchung des sicheren Aufrufs von Funktionen durch eine CALL-Anweisung.
Anti Stack Pivoting (Anti ROP)	Schutz vor einer Verschiebung des ESP-Registerstapels zur exploitierten Adresse.

Simple Export Address Table Access Monitor (EAT Access Monitor & EAT Access Monitor via Debug Register)	Schutz vor Lesezugriff auf die Exportadresstabelle (Export Address Table) für die Module kernel32.dll, kernelbase.dll, ntdll.dll
Heapspray Allocation (Heapspray)	Schutz vor Speicherbelegung unter Verwendung von schädlichem Code.
Execution Flow Simulation (Anti Return Oriented Programming)	Erkennen potenziell gefährlicher Anweisungsketten (mögliches ROP-Gadget) in der Komponente Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Schutz vor der Ausweitung von Privilegien durch eine Schwachstelle im AFD-Treiber (Ausführen eines zufälligen Codes auf dem Nullring durch den Anruf von QueryIntervalProfile).
Attack Surface Reduction (ASR)	Blockierung des Starts von Modulen mit etwaigen Schwachstellen über den geschützten Prozess.
Anti Process Hollowing (Hollowing)	Schutz gegen das Erstellen und Ausführen von schädlichen Kopien vertrauenswürdiger Prozesse.
Anti AtomBombing (APC)	Globaler Atomtabellen-Exploit über Asynchrone Prozeduraufrufe (APC).
Anti CreateRemoteThread (RThreadLocal)	Ein anderer Prozess hat einen Thread in einem geschützten Prozess erstellt.
Anti CreateRemoteThread (RThreadRemote)	Ein geschützter Prozess hat einen Thread in einem anderen Prozess erstellt.

Integration mit Drittherstellersystemen

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

Leistungsindikatoren für das Programm Systemmonitor

Dieser Abschnitt enthält Informationen über Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows, die von Kaspersky Embedded Systems Security während der Installation registriert werden.

Über Leistungsindikatoren in Kaspersky Embedded Systems Security

Die Komponente "Leistungsindikatoren" gehört zu den standardmäßig installierten Komponenten von Kaspersky Embedded Systems Security. Während der Installation registriert Kaspersky Embedded Systems Security seine Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows.

Mit den Indikatoren von Kaspersky Embedded Systems Security können Sie die Leistung des Programms bei der Ausführung von Aufgaben zum Echtzeit-Computerschutz kontrollieren. Sie können Engstellen beim Zusammenwirken mit anderen Anwendungen und bei ungenügenden Ressourcen identifizieren. Sie können Abstürze von Kaspersky Embedded Systems Security untersuchen und so ungewünschte Einstellungen identifizieren.

Sie können die Leistungsindikatoren für Kaspersky Embedded Systems Security aufrufen, indem Sie die Konsole **Optimierung** im Abschnitt **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 empfohlene Konfigurationen von Kaspersky Embedded Systems Security bei Grenzwertüberschreitungen angegeben.

Gesamtzahl der abgelehnten Anfragen (Total number of requests denied)

Gesamtzahl der abgelehnten Anfragen (Total number of requests denied)

Name	Gesamtzahl der abgelehnten Anfragen (Total number of requests denied)
Definition	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die nicht von den Programmprozessen angenommen wurden. Es wird ab dem letzten Start von Kaspersky Embedded Systems Security gezählt. Das Programm überspringt Objekte, für die Verarbeitungsanfragen von Prozessen durch Kaspersky Embedded Systems Security zurückgewiesen werden.
Ziel	Ein Indikator kann überwachen: • Senkung des Echtzeit-Computerschutzes, weil die Prozesse von Kaspersky Embedded Systems Security überlastet sind. • Unterbrechung des Echtzeit-Computerschutzes aufgrund von Fehlern in den File-Interception-Dispatchern.
Normalwert / Grenzwert	0 / 1

Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Summe der abgelehnten Verarbeitungsanfragen entspricht der Summe der übersprungenen Objekte. Folgende Situationen sind abhängig vom "Verhalten" des Indikators möglich: • Der Indikator zeigt mehrere abgelehnte Anfrage im Laufe einer längeren Zeit: Alle Prozesse von Kaspersky Embedded Systems Security waren vollständig ausgelastet, deshalb konnte Kaspersky Embedded Systems Security die Objekte nicht untersuchen. Um das Überspringen von Objekten auszuschließen, erhöhen Sie die Menge an Programmprozessen für Aufgaben zum Echtzeit-Computerschutz. Sie können die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** von Kaspersky Embedded Systems Security verwenden. • Die Summe der abgelehnten Anfragen übersteigt den kritischen Schwellenwert erheblich und steigt schnell an: Der File-Interception-Dispatcher ist ausgefallen. Kaspersky Embedded Systems Security untersucht Objekte nicht, wenn darauf zugegriffen wird. Kaspersky Embedded Systems Security neu starten

Gesamtzahl der übersprungenen Anfragen (Total number of requests skipped).

Gesamtzahl der übersprungenen Anfragen (Total number of requests skipped).

Name	Gesamtzahl der übersprungenen Anfragen (Total number of requests skipped).
Definition	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die von Kaspersky Embedded Systems Security angenommen wurden, über die aber kein Ereignis über den Verarbeitungsabschluss gesendet wurde. Es wird ab dem letzten Programmstart gezählt. Wenn eine Anfrage zur Verarbeitung eines Objekts, das von einem aktiven Prozess angenommen wurde, kein Ereignis über den Verarbeitungsabschluss gesendet hat, übergibt der Treiber diese Anfrage an einen anderen Prozess und der Wert des Indikators **Anzahl der übersprungenen Anfragen** wird um 1 erhöht. Wenn der Treiber alle aktiven Prozesse aufgerufen hat und die Verarbeitungsanfrage von keinem der Prozesse angenommen wurde (wegen Überlastung) oder keine Ereignisse über den Verarbeitungsabschluss gesendet wurden, überspringt Kaspersky Embedded Systems Security das Objekt und erhöht den Wert des Indikators **Gesamtzahl der übersprungenen Anfragen** um 1.
Ziel	Der Indikator kann einen Produktivitätsverlust wegen ausbleibender Datenströme von File-Interception-Dispatchern überwachen.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Ein Indikator, der ungleich null ist, bedeutet, dass ein oder mehrere Datenströme des File-Interception-Dispatchers hängen geblieben sind und stillstehen. Der Indikatorwert entspricht der Anzahl der Datenströme, die zurzeit stillstehen.

	Wenn das Untersuchungstempo nicht befriedigt, starten Sie Kaspersky Embedded Systems Security neu, um die angehaltenen Datenströme wiederherzustellen.

Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Name	Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden (Number of requests not processed due to lack of resources).
Definition	Gesamtzahl der Anfragen des File-Interception-Treibers, die aufgrund ungenügender Systemressourcen (beispielsweise des Arbeitsspeichers) nicht verarbeitet wurden. Es wird ab dem letzten Start von Kaspersky Embedded Systems Security gezählt. Kaspersky Embedded Systems Security überspringt Anfragen zur Verarbeitung von Objekten, die nicht vom File-Interceptor-Treiber verarbeitet werden.
Ziel	Der Indikator kann mögliche Qualitätsverluste des Echtzeit-Computerschutzes erkennen und beseitigen, die aufgrund eines Mangels an Systemressourcen eintreten.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert ungleich null ist, brauchen die Prozesse von Kaspersky Embedded Systems Security für die Anfragenbearbeitung einen größeren Arbeitsspeicher. Es ist möglich, dass es andere aktive Prozesse gibt, die den ganzen Arbeitsspeicher in Anspruch nehmen.

Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Name	Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden (Number of requests sent to be processed).
Definition	Anzahl der Objekte, die auf Verarbeitung durch aktive Prozesse warten.
Ziel	Dieser Indikator kann verwendet werden, um die Belastung der Arbeitsprozesse von Kaspersky Embedded Systems Security und Gesamtstufe der Dateiaktivität auf dem geschützten Gerät zu überwachen.
Normalwert / Grenzwert	Der Indikator kann je nach Stufe der Dateiaktivität auf dem geschützten Gerät schwanken.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	N/V

Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

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 Aufgaben zum Echtzeit-Computerschutz beteiligt sind.
Ziel	Dieser Indikator erlaubt es, mögliche Qualitätsverluste des Echtzeit-Computerschutzes zu erkennen und zu beseitigen, die auf vollständige Auslastung der Prozesse von Kaspersky Embedded Systems Security zurückgehen.
Normalwert / Grenzwert	Variiert / 40.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	In jedem aktiven Prozess können bis zu 60 Datenströme des File-Interception-Dispatchers angelegt werden. Wenn sich der Indikator der Zahl 60 nähert, besteht das Risiko, dass kein aktiver Prozess mehr die Verarbeitung einer in der Warteschlange stehenden Anfrage vom File-Interception-Treiber abnimmt und Kaspersky Embedded Systems Security überspringt das Objekt. Vergrößern Sie die Anzahl der Prozesse von Kaspersky Embedded Systems Security für die Aufgaben zum Echtzeit-Computerschutz. Sie können die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** von Kaspersky Embedded Systems Security verwenden.

Maximale Anzahl der Datenströme des File-Interception-Dispatchers

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 Aufgaben zum Echtzeit-Computerschutz 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 Indikator **Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers** abweicht, verteilt Kaspersky Embedded Systems Security die Belastung ungleichmäßig auf die ausführenden Prozesse. Kaspersky Embedded Systems Security neu starten

Anzahl der Elemente in der Warteschlange für infizierte Objekte

Anzahl der Elemente in der Warteschlange für infizierte Objekte

Name	Anzahl der Elemente in der Warteschlange für infizierte Objekte.
Definition	Anzahl der infizierten Objekte, die momentan auf die Verarbeitung (Desinfektion oder Löschen) warten.
Ziel	Ein Indikator kann überwachen: • Unterbrechung des Echtzeit-Computerschutzes aufgrund von möglichen Fehlern in den File-Interception-Dispatchern. • Überlastung der Prozesse wegen ungleichmäßiger Verteilung der Prozessorzeit zwischen den anderen laufenden Programmen und Kaspersky Embedded Systems Security. • Virenepidemien.
Normalwert / Grenzwert	Der Indikatorwert kann von Null abweichen, wenn Kaspersky Embedded Systems Security gefundene infizierte oder möglicherweise infizierte Objekte verarbeitet, aber nicht sofort nach Bearbeitungsschluss zur Null zurückkehrt. / Der Indikatorwert bleibt längere Zeit nicht auf Null.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert längere Zeit nicht auf Null bleibt: • Kaspersky Embedded Systems Security verarbeitet keine Objekte (möglicherweise aufgrund eines Absturzes des File-Interception-Dispatchers) Kaspersky Embedded Systems Security neu starten • Möglicherweise steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Belastung am geschützten Gerät durch andere Anwendungen senken). • Es ist eine Virenepidemie eingetreten. Vom Eintreten einer Virenepidemie zeugt außerdem eine große Menge an gefundenen infizierten oder möglicherweise infizierten Objekten in der Aufgabe Echtzeitschutz für Dateien. Informationen über die Anzahl der gefundenen Objekte können Sie der Aufgabenstatistik oder dem Protokoll der Aufgabenausführung entnehmen.

Anzahl der pro Sekunde verarbeiteten Objekte

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 geschützten Geräts erkannt und beseitigt werden, die wegen der Zuweisung zu geringer Prozessorzeit an die Arbeitsprozesse von Kaspersky Embedded Systems Security oder wegen Fehler bei der Ausführung von Kaspersky Embedded Systems Security eingetreten sind.
Normalwert / Grenzwert	Variiert / Nein.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Die Indikatorwerte hängen von den aktivierten Werten der Einstellungen für Kaspersky Embedded Systems Security und von der Belastung des geschützten Geräts durch Prozesse anderer Programme ab. Beobachten Sie längere Zeit das mittlere Anzeige-Niveau des Indikators. Wenn der allgemeine Indikatorwert gesunken ist, kann diese auf eine der folgenden Situationen hinweisen: • Den aktiven Prozessen von Kaspersky Embedded Systems Security steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Embedded Systems Security zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Belastung am geschützten Gerät durch andere Anwendungen senken). • Kaspersky Embedded Systems Security ist abgestürzt (mehrere Datenströme stehen still). Kaspersky Embedded Systems Security neu starten

SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält Informationen zu den Indikatoren und Traps in Kaspersky Embedded Systems Security.

Über SNMP-Indikatoren und -Traps in Kaspersky Embedded Systems Security

Wenn Sie SNMP-Indikatoren und -Traps zu den Komponenten von Anti-Virus hinzugefügt haben, die installiert werden sollen, können Sie Indikatoren und Traps für Kaspersky Embedded Systems Security mithilfe des SNMP-Protokolls (Simple Network Management Protocol) anzeigen.

Um die Indikatoren und Traps für Kaspersky Embedded Systems Security am Administrator-Arbeitsplatz anzuzeigen, starten Sie auf dem geschützten Gerät den SNMP-Dienst und am Administrator-Arbeitsplatz den SNMP-Dienst und den Dienst SNMP-Traps.

SNMP-Indikatoren in Kaspersky Embedded Systems Security

Dieser Abschnitt enthält eine Tabelle mit einer Beschreibung der Einstellungen der SNMP-Indikatoren von Kaspersky Embedded Systems Security.

Leistungsindikatoren

Leistungsindikatoren

Indikatoren	Definition
currentRequestsAmount	Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden
currentInfectedQueueLength	Anzahl der Elemente in der Warteschlange für infizierte Objekte
currentObjectProcessingRate	Anzahl der pro Sekunde verarbeiteten Objekte
currentWorkProcessesNumber	Aktuelle Anzahl von Arbeitsprozessen, die von Kaspersky Embedded Systems Security genutzt werden

Indikatoren für Quarantäne

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	Gesamtmenge der Daten im Quarantäne-Ordner (MB)

Indikator für Backup

Indikator für Backup

Indikatoren	Definition
currentBackupStorageSize	Gesamtmenge der Daten im Backup-Ordner (MB)

Allgemeine Indikatoren

Allgemeine Indikatoren

Indikatoren	Definition
lastCriticalAreasScanAge	Der seit der letzten vollständigen Untersuchung der wichtigen Bereiche des geschützten Geräts vergangene Zeitraum (in Sekunden angegebener Zeitraum seit dem letzten Abschluss der Aufgabe zur Untersuchung wichtiger Bereiche).
licenseExpirationDate	Lizenzablaufdatum. Wenn ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt wurden, wird das Ablaufdatum der Lizenz des Reserveschlüssels angezeigt.
currentApplicationUptime	Ausführungszeit von Kaspersky Embedded Systems Security seit dem letzten Start, in Hundertstelsekunden

Update-Indikatoren

Update-Indikatoren

Indikatoren	Definition
avBasesAge	"Alter" der Datenbanken (in Hundertstelsekunden angegebener Zeitraum seit Erstellungsdatum der zuletzt installierten Datenbanken-Updates).

Indikatoren für den Echtzeitschutz für Dateien

Indikatoren für den Echtzeitschutz für Dateien

Indikatoren	Definition
totalObjectsProcessed	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien untersuchten Objekte
totalInfectedObjectsFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen infizierten und anderen Objekte
totalSuspiciousObjectsFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen möglicherweise infizierten Objekte
totalVirusesFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen Objekte
totalObjectsQuarantined	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die von Kaspersky Embedded Systems Security in die Quarantäne verschoben wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien.
totalObjectsNotQuarantined	Anzahl der infizierten oder möglicherweise infizierten Objekte, die Kaspersky Embedded Systems Security erfolglos versuchte, in die Quarantäne zu verschieben. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsDisinfected	Anzahl der infizierten Objekte, die von Kaspersky Embedded Systems Security desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotDisinfected	Anzahl der infizierten und anderen Objekte, deren Desinfektion durch Kaspersky Embedded Systems Security fehlgeschlagen ist. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsDeleted	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die von Kaspersky Embedded Systems Security gelöscht wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotDeleted	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die Kaspersky Embedded Systems Security erfolglos zu löschen versuchte. Gezählt seit dem letzten Start der zum Aufgabe Echtzeitschutz für Dateien
totalObjectsBackedUp	Anzahl der infizierten oder anderen Objekte, die von Kaspersky Embedded Systems Security ins Backup verschoben wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotBackedUp	Anzahl der infizierten oder anderen Objekte, die Kaspersky Embedded Systems Security erfolglos versuchte, ins Backup zu verschieben. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien

SNMP-Traps und ihre Optionen in Kaspersky Embedded Systems Security

Die Optionen von SNMP-Traps in Kaspersky Embedded Systems Security sind wie folgt zusammengefasst:

- eventThreatDetected: Objekt gefunden.

  Der Trap verfügt über die folgenden Optionen:

  - eventDateAndTime
  - eventSeverity
  - computerName
  - UserName
  - objectName
  - threatName
  - detectType
  - detectCertainty

- eventBackupStorageSizeExceeds: Die maximale Größe des Backups wurde überschritten. Die Gesamtmenge der Daten im Backup-Ordner hat den Wert überschritten, der durch die Einstellung **Maximale Größe des Backups (MB)** festgelegt ist. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

  Der Trap verfügt über die folgenden Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdBackupStorageSizeExceeds: Maximale Größe des Backups ist erreicht. Der freie Speicherplatz im Backup beträgt weniger als oder ist gleich dem Wert **Grenzwert für verfügbaren Speicherplatz (MB)**. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

  Der Trap verfügt über die folgenden Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds: Die maximale Größe der Quarantäne wurde überschritten. Das Gesamtvolumen der Daten im Quarantäne-Ordner hat den Wert überschritten, der durch die Einstellung **Maximale Größe der Quarantäne (MB)** festgelegt ist. Kaspersky Embedded Systems Security verschiebt möglicherweise infizierte Objekte weiterhin in die Quarantäne.

  Der Trap verfügt über die folgenden Optionen:

- eventDateAndTime
- eventSeverity
- eventSource

- eventThresholdQuarantineStorageSizeExceeds: Maximale Größe der Quarantäne ist erreicht. Größe des freien Speicherplatzes in der Quarantäne, die in der Einstellung **Grenzwert für verfügbaren Speicherplatz (MB)** eingegeben wurde, ist gleich dem angegebenen Wert oder liegt darunter. Kaspersky Embedded Systems Security erstellt weiterhin Backups für infizierte Objekte.

  Der Trap verfügt über die folgenden Optionen:

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined: Quarantäne-Fehler.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - UserName
  - computerName
  - objectName
  - storageObjectNotAddedEventReason

- eventObjectNotBackuped: Fehler beim Speichern einer Kopie des Objekts im Backup.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - UserName
  - computerName
  - storageObjectNotAddedEventReason

- eventQuarantineInternalError: Interner Quarantäne-Fehler.

  Der Trap verfügt über die folgenden Optionen:

- eventSeverity
- eventDateAndTime
- eventSource
- eventReason

- eventBackupInternalError: Backup-Fehler.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason

- eventAVBasesOutdated: Antiviren-Datenbanken sind veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Update der Programm-Datenbanken zum letzten Mal ausgeführt wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von geschützten Geräten).

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated: Antiviren-Datenbanken sind stark veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Update der Programm-Datenbanken zum letzten Mal ausgeführt wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von geschützten Geräten).

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted: Kaspersky Embedded Systems Security läuft

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown: Kaspersky Embedded Systems Security wurde beendet

Der Trap verfügt über die folgenden Optionen:

- eventSeverity
- eventDateAndTime
- eventSource

- eventCriticalAreasScanWasntPerformForALongTime: Untersuchung wichtiger Bereiche liegt lange zurück. Anzahl der Tage, seitdem die Aufgabe "Untersuchung wichtiger Bereiche" zum letzten Mal abgeschlossen wurde.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired: Lizenz ist abgelaufen.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon: Lizenz läuft bald ab. Es werden die Tage gezählt, die bis zum Ablauf der Lizenz verbleiben.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventTaskInternalError: Fehler bei Ausgabenausführung.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName

- eventUpdateError: Fehler beim Ausführen der Update-Aufgabe.

  Der Trap verfügt über die folgenden Optionen:

  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

Beschreibungen und mögliche Werte der Optionen von SNMP-Traps in Kaspersky Embedded Systems Security

Beschreibungen der Trap-Optionen und ihrer möglichen Werte werden nachfolgend aufgeführt:

- eventDateAndTime: Datum und Uhrzeit des Ereignisses.
- eventSeverity: Prioritätsstufe.

  Diese Option kann folgende Werte annehmen:

  - critical (1) – kritisch
  - warning (2) – Warnung
  - info (3) – informativ
- userName: Benutzername (beispielsweise der Name eines Benutzers, der versucht hat auf eine infizierte Datei zuzugreifen).
- computerName: Name des geschützten Geräts (beispielsweise Name eines geschützten Geräts, von dem ein Benutzer versucht hat, Zugriff auf eine infizierte Datei zu bekommen).
- eventSource: Funktionale Komponente, die das Ereignis generiert hat.

  Diese Option kann folgende Werte annehmen:

  - unknown (0) – Die Komponente ist unbekannt
  - quarantine (1) – Quarantäne
  - backup (2) – Backup
  - reporting (3) – Protokolle der Aufgabenausführung
  - updates (4) – Update
  - realTimeProtection (5) – Echtzeitschutz für Dateien
  - onDemandScanning (6) – Untersuchung auf Befehl
  - product (7) – Ereignis, das nichts mit einzelnen Komponenten, sondern mit Kaspersky Embedded Systems Security als Ganzem zu tun hat

- systemAudit (8) – Systemaudit-Protokoll

- eventReason: Ereignisauslöser: Grund für Ereigniseintritt.

  Diese Option kann folgende Werte annehmen:

  - reasonUnknown (0) – der Grund ist unbekannt.

  - reasonInvalidSettings (1) – nur für Ereignisse des Backups und der Quarantäne; wird angezeigt, wenn der Quarantäne-Ordner oder der Backup-Ordner nicht verfügbar sind (unzureichende Zugriffsrechte oder Ordner wurde in den Quarantäneparametern falsch angegeben, z.B. ein Netzwerkpfad wurde angegeben). In diesem Fall verwendet Kaspersky Embedded Systems Security den Standardordner für Backup oder Quarantäne.

- objectName: Objektname (beispielsweise der 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, die Kaspersky Embedded Systems Security beim Fund eines Objekts zurückgibt. Sie können den vollständigen Namen eines gefundenen Objekts im Protokoll der Aufgabenausführung einsehen.

- detectType: Typ des gefundenen Objekts.

  Diese Option kann folgende Werte annehmen:

  - undefined (0) – nicht definiert

  - virware – klassische Viren und Netzwerkwürmer

  - trojware – Trojaner

  - malware – sonstige Schadsoftware

  - adware – Adware

  - pornware – pornografische Programme

  - riskware – legale Programmen, die von Angreifern genutzt werden können, um das Gerät oder persönliche Daten des Benutzers zu schädigen

- detectCertainty: Gewissheit für Erkennung einer Bedrohung.

  Diese Option kann folgende Werte annehmen:

  - Suspicion (möglicherweise infiziert) – Kaspersky Embedded Systems Security hat erkannt, dass ein Codeabschnitt des Objekts teilweise mit einem bekannten Schadcode übereinstimmt.

  - Sure (infiziert)– Kaspersky Embedded Systems Security hat erkannt, dass ein Codeabschnitt des Objekts vollständig mit einem bekannten Schadcode übereinstimmt.

- days: Anzahl von Tagen (z. B. Anzahl der Tage bis zum Ablauf einer Lizenz).

- errorCode: Ein Fehlercode.

- knowledgeBaseId: Adresse des Artikels in der Wissensdatenbank (beispielsweise Adresse des Artikels, der einen Fehler beschreibt).

- taskName: Ein Aufgabenname.

- updaterErrorEventReason: Der Grund, aus dem das Update nicht übernommen wurde.

  Diese Option kann folgende Werte annehmen:

  - reasonUnknown(0) – der Grund ist unbekannt.
  - reasonAccessDenied – Zugriff verweigert.
  - reasonUrlsExhausted – das Ende der Liste mit Update-Quellen wurde erreicht.
  - reasonInvalidConfig – ungültige Konfigurationsdatei.
  - reasonInvalidSignature – ungültige Signatur.
  - reasonCantCreateFolder – der Ordner kann nicht angelegt werden.
  - reasonFileOperError – Dateifehler.
  - reasonDataCorrupted – das Objekt ist beschädigt.
  - reasonConnectionReset – Verbindungstrennung.
  - reasonTimeOut – Zeitüberschreitung bei Verbindung.
  - reasonProxyAuthError – Fehler bei Authentifizierung auf dem Proxyserver.
  - reasonServerAuthError – Fehler bei Authentifizierung auf dem Server.
  - reasonHostNotFound – Gerät nicht gefunden.
  - reasonServerBusy – Server nicht verfügbar.
  - reasonConnectionError – Verbindungsfehler.
  - reasonModuleNotFound – das Objekt wurde nicht gefunden.
  - reasonBlstCheckFailed(16) – Fehler bei der Untersuchung der Deny-Liste für Schlüssel. Möglicherweise wurden während des Updatevorgangs Datenbanken-Updates veröffentlicht. Wiederholen Sie bitte das Update in einigen Minuten.

- storageObjectNotAddedEventReason: Der Grund für das Nichtverschieben eines Objektes in das Backup oder die Quarantäne.

  Diese Option kann folgende Werte annehmen:

  - reasonUnknown (0) – der Grund ist unbekannt.
  - reasonStorageInternalError – Datenbankfehler; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
  - reasonStorageReadOnly – Datenbank ist schreibgeschützt; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
  - reasonStorageIOError – Ein-/Ausgabefehler: a) Kaspersky Embedded Systems Security ist beschädigt, Kaspersky Embedded Systems Security muss wiederhergestellt werden; b) das Laufwerk mit Kaspersky Embedded Systems Security ist beschädigt.

- reasonStorageCorrupted – Speicher ist beschädigt; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
- reasonStorageFull – Datenbank ist voll; freier Speicherplatz ist erforderlich.
- reasonStorageOpenError – Datenbankdatei konnte nicht geöffnet werden; Kaspersky Embedded Systems Security muss wiederhergestellt werden.
- reasonStorageOSFeatureError – Einige Funktionen des Betriebssystems entsprechen nicht den Anforderungen von Kaspersky Embedded Systems Security.
- reasonObjectNotFound – Das in die Quarantäne zu verschiebende Objekt ist nicht auf dem Datenträger vorhanden.
- reasonObjectAccessError – unzureichende Rechte für die Verwendung der Backup-API: Das Benutzerkonto, mit dessen Rechten der Vorgang ausgeführt wird, hat nicht die Berechtigung Backup Operator.
- reasonDiskOutOfSpace – zu wenig Platz auf dem Datenträger.

Integration mit WMI

Kaspersky Embedded Systems Security unterstützt die Integration mit Windows-Verwaltungsinstrumentation (WMI): Sie können Client-Systeme verwenden, die WMI zum Empfangen von Daten über den Web-Based Enterprise Management-Standard (WBEM) nutzen, um Informationen über den Status von Kaspersky Embedded Systems Security und seine Komponenten zu erhalten.

Wenn Kaspersky Embedded Systems Security installiert ist, werden eigene Module im System registriert, um einen Namensraum von Kaspersky Embedded Systems Security auf dem geschützten Gerät zu erstellen. Ein Namensraum von Kaspersky Embedded Systems Security ermöglicht die Nutzung von Klassen und Exemplarklassen für Kaspersky Embedded Systems Security sowie deren Eigenschaften.

Die Werte einiger Eigenschaften von Exemplarklassen hängen von Aufgabentypen ab.

Eine *Nicht-periodische Aufgabe* ist eine Programmaufgabe, die zeitlich nicht beschränkt ist und entweder dauernd ausgeführt oder beendet werden kann. Bei diesen Aufgaben wird kein Ausführungsfortschritt angezeigt. Die Ergebnisse der Aufgabe werden während der Ausführung der Aufgabe fortlaufend als einzelne Ereignisse protokolliert (beispielsweise Fund eines infizierten Objekts durch Aufgaben zum Echtzeit-Computerschutz). Dieser Aufgabentyp wird über Richtlinien von Kaspersky Security Center verwaltet.

Eine *Periodische Aufgabe* ist eine Programmaufgabe, die zeitlich beschränkt ist und 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). Mehrere periodische Aufgaben desselben Typs können auf einem einzelnen geschützten Gerät gleichzeitig ausgeführt werden (drei Aufgaben zur Untersuchung auf Befehl mit unterschiedlichen Untersuchungsbereichen). Periodische Aufgaben können über Kaspersky Security Center als Gruppenaufgaben verwaltet werden.

Wenn Sie Werkzeuge für die Erstellung von WMI-Namensraumabfragen verwenden und dynamische Daten aus WMI-Namensräume in Ihrem Unternehmensnetzwerk empfangen, haben Sie die Möglichkeit, Informationen über den aktuellen Zustand des Programms zu empfangen (siehe Tabelle unten).

Informationen über den Zustand des Programms

Eigenschaft der Exemplarklasse	Beschreibung	Werte

ProductName	Name des installierten Programms.	Vollständiger Name des Programms ohne Versionsnummer.
ProductVersion	Vollständige Versionsnummer des installierten Programms.	Vollständige Versionsnummer des Programms einschließlich Nummer des Builds
InstalledPatches	Übersicht der Anzeigenamen der installierten Patches.	Liste von kritischen Fehlerbehebungen, die für das Programm installiert wurden.
IsLicenseInstalled	Status der Aktivierung des Programms.	Status des Schlüssels, der zur Aktivierung des Programms verwendet wurde. Mögliche Werte: • Falsch – Dem Programm wurde kein Lizenzschlüssel hinzugefügt. • Wahr – Dem Programm wurde ein Lizenzschlüssel hinzugefügt.
LicenseDaysLeft	Zeigt an, wie viele Tage bis zum Ablauf einer aktuellen Lizenz übrig sind.	Anzahl der Tage, die bis zum Ablauf der aktuellen Lizenz verbleiben. Mögliche nicht-positive Werte: • 0 – Die Lizenz ist abgelaufen. • -1 – Es können keine Informationen über den aktuellen Schlüssel abgerufen werden oder der angegebene Schlüssel kann nicht zur Aktivierung des Programms verwendet werden (beispielsweise, wenn er auf der Grundlage einer Deny-Liste für Schlüssel gesperrt ist).
AVBasesDatetime	Zeitstempel für die aktuelle Version der Antiviren-Datenbanken.	Datum und Uhrzeit der Erstellung der derzeit verwendeten Antiviren-Datenbanken. Wenn das installierte Programm keine Antiviren-Datenbanken verwendet, weist das Feld den Wert "Nicht installiert" auf.
IsExploitPreventionEnabled	Status der Komponente "Exploit-Prävention".	Status der Komponente "Exploit-Prävention". Mögliche Werte: • Wahr – Die Komponente "Exploit-Prävention" ist aktiviert und bietet Schutz. • Falsch – Die Komponente "Exploit-Prävention" bietet keinen Schutz. Beispielsweise deaktiviert, nicht installiert, der Lizenzvertrag wurde verletzt.
ProtectionTasksRunning	Zusammenstellung von Schutzaufgaben, die derzeit ausgeführt werden.	Liste der Aufgaben zum Schutz, zur Kontrolle und Überwachung, die derzeit ausgeführt werden. In diesem Feld sollten alle ausgeführten nicht periodischen Aufgaben angeführt sein. Wenn keine nicht periodische Aufgabe ausgeführt wird, weist das Feld den Wert "Keine" auf.

IsAppControlRunning	Status der Aufgabe zur Kontrolle des Programmstarts.	Status der Aufgabe zur Kontrolle des Programmstarts. • Wahr – Die Aufgabe zur Kontrolle des Programmstarts wird derzeit nicht ausgeführt. • Falsch – Die Kontrolle des Programmstarts wird derzeit nicht ausgeführt oder die Komponente "Kontrolle des Programmstarts" ist nicht installiert.
AppControlMode	Modus der Aufgabe zur Kontrolle des Programmstarts.	Beschreibt den aktuellen Status der Komponente "Kontrolle des Programmstarts" und beschreibt den ausgewählten Modus für die zugehörige Aufgabe. Mögliche Werte: • Aktiv – In den Aufgabeneinstellungen ist der Modus **Aktiv** ausgewählt. • Nur Statistik – In den Aufgabeneinstellungen ist der Modus **Nur Statistik** ausgewählt. • Nicht installiert – Die Komponente "Kontrolle des Programmstarts" ist nicht installiert.
AppControlRulesNumber	Gesamtanzahl der Regeln für die Kontrolle des Programmstarts.	Anzahl der derzeit in den Einstellungen der Kontrolle des Programmstarts festgelegten Regeln.
AppControlLastBlocking	Zeitstempel für den letzten von der Aufgabe zur Kontrolle des Programmstarts in einem beliebigen Modus blockierten Programmstart.	Datum und Uhrzeit des letzten von der Komponente "Kontrolle des Programmstarts" blockierten Programmstarts. Dieses Feld beinhaltet alle blockierten Programme unabhängig vom Aufgabenmodus. Wenn zum Zeitpunkt der Verarbeitung der WMI-Abfrage keine Exemplarklassen von blockierten Programmstarts registriert sind, wird dem Feld der Wert "Keine" zugewiesen.
PeriodicTasksRunning	Zusammenstellung von periodischen Aufgaben, die derzeit ausgeführt werden.	Liste von Aufgaben zur Untersuchung auf Befehl, zum Update und zur Inventarisierung, die derzeit ausgeführt werden. Dieses Feld sollte alle ausgeführten periodischen Aufgaben beinhalten. Wenn derzeit keine periodischen Aufgaben ausgeführt werden, weist das Feld den Wert "Keine" auf.
ConnectionState	Status der Verbindung zwischen der WMI-Anbieterkomponente und dem Kaspersky Security Service (KAVFS).	Informationen über den Status der Verbindung zwischen der WMI-Anbieterkomponente und dem Kaspersky Security Service. Mögliche Werte: • Erfolg – Die Verbindung wurde erfolgreich hergestellt: der WMI-Client kann Informationen über den Programmstatus empfangen. • Fehler. Fehlercode: <code> – Die Verbindung konnte aufgrund eines Fehlers mit dem

		angegebenen Code nicht hergestellt werden.

Diese Daten repräsentieren Eigenschaften von Exemplarklassen KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, wobei:

- KasperskySecurity_ProductInfo der Name der Klasse von Kaspersky Embedded Systems Security ist
- .ProductName=Kaspersky Embedded Systems Security die Schlüsseleinstellungen für Kaspersky Embedded Systems Security sind

Die Exemplarklasse wird im Namensraum ROOT\Kaspersky\Security erstellt.

Arbeiten mit Kaspersky Embedded Systems Security aus der Befehlszeile

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

Befehle

Sie können die Basisbefehle zur Verwaltung von Kaspersky Embedded Systems Security aus der Befehlszeile des geschützten Geräts anhand des Befehlszeilen-Tools erteilen, das zum Paket der Programmkomponenten von Kaspersky Embedded Systems Security gehört.

Mithilfe von Befehlen können Sie nur Funktionen steuern, für die Sie in Kaspersky Embedded Systems Security zugriffsberechtigt sind.

Bestimmte Befehle von Kaspersky Embedded Systems Security werden in folgenden Modi ausgeführt:

- Synchronmodus: Die Kontrolle kehrt sofort nach Abschluss der Befehlsausführung zur Konsole zurück.
- Asynchronmodus: Die Kontrolle kehrt sofort nach dem Befehlsstart zur Konsole zurück.

Um die Ausführung eines im Synchronmodus ausgeführten Befehls zu unterbrechen,

drücken Sie die Tasten **Strg+C**.

Gehen Sie gemäß diesen Regeln vor, wenn Sie Befehle für Kaspersky Embedded Systems Security eingeben:

- Beachten Sie bei der Eingabe von Schlüsseln und Befehlen die Groß- und Kleinschreibung.
- Trennen Sie Schlüssel für Befehle mit einem Leerzeichen ab.
- Sollte der Pfad von Dateien/Ordnern als Wert in einem Feld eingegeben sein und Leerzeichen enthalten, fügen Sie dem Pfad Anführungszeichen hinzu, z. B.: `"C:\TEST\test cpp.exe"`.
- Bei Bedarf können Sie für Dateinamen oder Pfade Platzhalter verwenden. Beispiele: `"C:\Temp\Temp*\"`, `"C:\Temp\Temp???.doc"`, `"C:\Temp\Temp*.doc"`.

Mithilfe der Befehlszeile können Sie das gesamte Spektrum an Operationen zur Steuerung und Verwaltung von Kaspersky Embedded Systems Security ausführen (siehe Tabelle unten).

Befehle für Kaspersky Embedded Systems Security

Befehl	Beschreibung
KAVSHELL APPCONTROL	Aktualisieren Sie die Regelliste mit der ausgewählten Importregel.
KAVSHELL APPCONTROL /CONFIG	Einstellung des Ausführungsmodus der Aufgabe zur Kontrolle des Programmstarts.
KAVSHELL APPCONTROL /GENERATE	Startet die Aufgabe zum Erstellen von Regeln für die Kontrolle des Programmstarts.
KAVSHELL VACUUM	Defragmentiert die Log-Dateien für Kaspersky Embedded Systems Security.

KAVSHELL PASSWORD	Verwaltet die Einstellungen für den Kennwortschutz.
KAVSHELL HELP	Die Hilfe für Befehle in Kaspersky Embedded Systems Security anzeigen.
KAVSHELL START	Starten von Kaspersky Security Service.
KAVSHELL STOP	Beenden von Kaspersky Security Service.
KAVSHELL SCAN	Erstellt und startet eine temporäre Aufgabe zur Untersuchung auf Befehl mit einem Untersuchungsbereich und Sicherheitsparametern, die durch Befehlszeilenoptionen vorgegeben werden.
KAVSHELL SCANCRITICAL	Starten der lokalen Systemaufgabe "Untersuchung wichtiger Bereiche".
KAVSHELL TASK	Startet, hält an / setzt fort, beendet die angegebene Aufgabe im asynchronen Modus, gibt den aktuellen Aufgabenstatus / eine Statistik für die Aufgabe zurück.
KAVSHELL RTP	Startet oder beendet alle Aufgaben zum Echtzeit-Computerschutz.
KAVSHELL UPDATE	Starten Sie die Aufgabe zum Update der Programm-Datenbanken mit den durch die Befehlszeilenoptionen angegebenen Einstellungen.
KAVSHELL ROLLBACK	Kehrt zur vorherigen Version der Datenbanken zurück.
KAVSHELL LICENSE	Fügt die Schlüssel hinzu oder löscht sie. Zeigt Informationen über die hinzugefügten Schlüssel an.
KAVSHELL TRACE	Ablaufverfolgung aktivieren oder deaktivieren. Verwaltet Parameter der Ablaufverfolgung.
KAVSHELL DUMP	Das Erstellen von Dump-Dateien aktivieren oder deaktivieren, wenn Prozesse von Kaspersky Embedded Systems Security mit einem Absturz beendet werden.
KAVSHELL IMPORT	Importiert die allgemeinen Einstellungen, Funktionen und Aufgaben für Kaspersky Embedded Systems Security aus einer Konfigurationsdatei.
KAVSHELL EXPORT	Exportiert alle Einstellungen und vorhandene Aufgaben von Kaspersky Embedded Systems Security in eine Konfigurationsdatei.
KAVSHELL DEVCONTROL	Ergänzt die Liste der erstellten Regeln für die Gerätekontrolle entsprechend dem ausgewählten Prinzip für das Hinzufügen.

Hilfe für Befehle in Kaspersky Embedded Systems Security anzeigen: KAVSHELL HELP

Um eine Liste aller Befehle für Kaspersky Embedded Systems Security anzuzeigen, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Um die Beschreibung und Syntax eines Befehls anzuzeigen, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL HELP <Befehl>

KAVSHELL <Befehl> /?
```

Beispiele für 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 beim Hochfahren des Betriebssystems" sowie andere Aufgaben, für deren Zeitplan die Startfrequenz **Bei Programmstart** gilt.

Um Kaspersky Security Service zu beenden, 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 `[/pwd:<password>]`.

Einen ausgewählten Bereich untersuchen: KAVSHELL SCAN

Um eine Aufgabe zur Untersuchung bestimmter Bereiche des geschützten Geräts zu starten, verwenden Sie den Befehl `KAVSHELL SCAN`. Die Befehlszeilenoptionen 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 (ihre Aufgabeneinstellungen können nicht in der Programmkonsole angezeigt werden). Es wird jedoch ein Leistungsprotokoll generiert und unter dem Knoten **Protokolle der Aufgabenausführung** in der Programmkonsole angezeigt.

Wenn Sie den Pfad in einer Aufgabe zur Untersuchung bestimmter Bereiche angeben, können Sie Umgebungsvariablen verwenden. Wenn eine Umgebungsvariable verwendet wird, führen Sie den Befehl `KAVSHELL SCAN` als entsprechender Benutzer aus.

Der Befehl `KAVSHELL SCAN` wird im Synchronmodus ausgeführt.

Um eine bestehenden Aufgabe zur Untersuchung auf Befehl aus der Befehlszeile zu starten, verwenden Sie den Befehl KAVSHELL TASK.

Syntax des Befehls KAVSHELL SCAN

```
KAVSHELL SCAN <Untersuchungsbereiche>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< Name der Datei mit einer
Liste der Untersuchungsbereiche >] [/F<A|C|E>] [/NEWONLY] [/AI:
<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>]
[/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"Masken">] [/ES:<Größe>] [/ET:<Dauer in
Sekunden>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<Tage>] [NORECALL]>] [/NOICHECKER]
[/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<Dateiname für Protokoll der
Aufgabenausführung>] [/ANSI] [/ALIAS:<Alias des Aufgabenamens>]
```

Der Befehl KAVSHELL SCAN enthält sowohl obligatorische als auch Parameter/Optionen, deren Verwendung optional ist (s. Tabelle unten).

Beispiele des Befehls KAVSHELL APPCONTROL

```
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
```

`KAVSHELL SCAN` Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
Untersuchungsbereich. Obligatorischer Parameter.	
<Dateien>	Untersuchungsbereich – Liste mit Dateien, Ordnern, Netzwerkpfaden und vordefinierten Bereichen. Geben Sie den Netzwerkpfad im UNC-Format (Universal Naming Convention) an. Im folgenden Beispiel wird der Ordner "Folder4" ohne einen Pfad angegeben, was darauf schließen lässt, dass er sich in dem Ordner befindet, in dem der KAVSHELL-Befehl ausgeführt wird: KAVSHELL SCAN Folder4 Wenn der Name des zu untersuchenden Objekts Leerzeichen beinhaltet, muss dieser von Anführungszeichen umschlossen sein. Wenn ein Ordner angegeben ist, untersucht Kaspersky Embedded Systems Security auch alle enthaltenen Unterordner. Um eine Gruppe der Datei zu untersuchen, können Sie die Zeichen * und ? verwenden.
<Ordner>	
<Netzwerkpfad>	
/MEMORY	Objekte im Arbeitsspeicher untersuchen.
/SHARED	Freigegebene Ordner auf dem geschützten Gerät untersuchen
/STARTUP	Autostart-Objekte untersuchen
/REMDRIVES	Wechseldatenträger untersuchen.
/FIXDRIVES	Festplatten untersuchen.

/MYCOMP	Alle Bereiche des geschützten Geräts untersuchen
/L:<Pfad zur Datei mit einer Liste der Untersuchungsbereiche>	Vollständiger Pfad zur Datei mit einer Liste der Untersuchungsbereiche. Verwenden Sie Zeilenumbrüche, um die Untersuchungsbereiche in der Datei voneinander zu trennen. Sie können wie im nachfolgenden Beispiel zum Inhalt einer Datei mit einer Liste für die Untersuchungsbereiche vordefinierte Untersuchungsbereiche angeben. C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Objekte untersuchen (Dateitypen). Wenn Sie diese Option nicht angeben, untersucht Kaspersky Embedded Systems Security die Objekte nach Format.	
/FA	Alle Objekte untersuchen.
/FC	Objekte, die nach Format untersucht werden (Standard). Kaspersky Embedded Systems Security untersucht nur Objekte, deren Formate in der Liste der als infizierbar geltenden Objekte enthalten sind.
/FE	Objekte nach Erweiterung untersuchen. Kaspersky Embedded Systems Security untersucht nur Objekte, die der Erweiterung nach als infizierbar gelten.
/NEWONLY	Nur neue und veränderte Dateien untersuchen. Wenn Sie diese Option nicht angeben, untersucht Kaspersky Embedded Systems Security alle Objekte.
Aktion für infizierte und andere Objekte. Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Embedded Systems Security die Aktion **Überspringen** aus.	
DISINFECT	Desinfizieren, irreparable Objekte überspringen Die Einstellungen DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Embedded Systems Security beibehalten, um die Kompatibilität mit den vorherigen Versionen zu gewährleisten. Diese Optionen können anstelle der Optionen "/AI" und "/AS" verwendet werden. In diesem Fall werden möglicherweise infizierte Objekte nicht durch Kaspersky Embedded Systems Security verarbeitet.
DISINFDEL	Desinfizieren, irreparable Objekte überspringen
DELETE	Löschen Die Einstellungen DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Embedded Systems Security gespeichert, um die Kompatibilität mit den vorherigen Versionen zu gewährleisten. Diese Optionen können anstelle der Optionen "/AI" und "/AS" verwendet werden. In diesem Fall werden möglicherweise infizierte Objekte nicht durch Kaspersky Embedded Systems Security verarbeitet.
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
/AS: **Aktion für möglicherweise infizierte Objekte**. Wenn Sie diese Option nicht angeben, führt Kaspersky Embedded Systems Security die Aktion **Überspringen** aus.	
QUARANTINE	Quarantäne
DELETE	Löschen

REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
Ausnahmen	
/E:ABMSPO	Die folgenden Typen an zusammengesetzten Objekten ausschließen: A – SFX-Archive B – E-Mail-Datenbanken M – Dateien in 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 die festgelegte <Anzahl der Sekunden>. Standardmäßig ist keine Zeitbeschränkung vorgesehen.
/ES:<Größe>	Zusammengesetzte Objekte, deren Größe den in MB festgelegten Wert <size> überschreitet, von der Untersuchung ausschließen. Standardmäßig untersucht Kaspersky Embedded Systems Security Objekte jeglicher Größe.
/TZOFF	Ausnahmen der vertrauenswürdigen Zone verschieben.
Erweiterte Einstellungen (Options)	
/NOICHECKER	iChecker-Technologie deaktivieren (standardmäßig aktiviert).
/NOISWIFT	iSwift-Technologie deaktivieren (standardmäßig aktiviert).
/ANALYZERLEVEL: <Ebene der heuristischen Analyse>	Verwendung der heuristischen Analyse aktivieren, Analyseniveau einstellen. Die folgenden Ebenen der heuristischen Analyse verfügbar: 1 – oberflächlich; 2 – mittel; 3 – tief Wenn Sie diese Option auslassen, verwendet Kaspersky Embedded Systems Security die heuristische Analyse nicht.
/ALIAS:<Alias des Aufgabenamens>	Ordnet einen temporären Namen für eine Aufgabe zur Untersuchung auf Befehl zu und ermöglicht es Ihnen auf diese zu verweisen, während diese ausgeführt wird, beispielsweise um ihre Statistiken mit dem Befehl TASK abzurufen. Der Alias des Aufgabenamens muss unter den alternativen Namen für die Aufgaben aller Komponenten von Kaspersky Embedded Systems Security einmalig sein. Wenn diese Option nicht vorgegeben ist, wird der Aufgabe ein temporärer Name im Format "scan_<kavshell_pid>", z.B. "scan_1234". In der Programmkonsole erhält die Aufgabe den Namen "Scan objects <Datum und Uhrzeit>", z. B. Scan objects 8/16/2007 5:13:14 PM.
Einstellungen des Protokolls der Aufgabenausführung (Berichteinstellungen)	
/W:<Name des Protokolls der Aufgabenausführung>	Wenn Sie diesen Parameter angeben, speichert Kaspersky Embedded Systems Security das Protokoll der Aufgabenausführung mit dem durch diesen Parameter vorgegebenen Namen.

	Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse, die während der Aufgabe auftraten. Im Protokoll werden die Ereignisse aufgezeichnet, die durch die Einstellungen des Protokolls der Aufgabenausführung und Einstellungen des Ereignisprotokolls von Kaspersky Embedded Systems Security in der "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten "Protokolle der Aufgabenausführung" der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security die Protokolldatei nicht erstellen kann, wird eine Fehlermeldung angezeigt, der Befehl wird aber dennoch ausgeführt.
/ANSI	Mit dieser Option wird die ANSI-Kodierung verwendet, um Ereignisse im Protokoll der Aufgabenausführung zu registrieren. Die ANSI-Option wird nicht verwendet, wenn der W-Parameter nicht festgelegt wird. Wenn die ANSI-Option nicht festgelegt wurde, wird UNICODE verwendet, um das Protokoll der Aufgabenausführung zu generieren.

Aufgabe "Untersuchung wichtiger Bereiche" starten: KAVSHELL SCANCRITICAL

Verwenden Sie den Befehl `KAVSHELL SCANCRITICAL`, um die Systemaufgabe zur Untersuchung wichtiger Bereiche mit den Einstellungen zu starten, die in der Programmkonsole festgelegt wurden.

Syntax des Befehls KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<Dateiname für das Protokoll der Aufgabenausführung>]
```

Beispiele für den Befehl KAVSHELL SCANCRITICAL

Um die Aufgabe zur Untersuchung wichtiger Bereiche auszuführen und das Protokoll der Aufgabenausführung im aktuellen Ordner in der Datei scancritical.log zu speichern, führen Sie folgenden Befehl aus:

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

Sie können den Parameter /W verwenden, um den Speicherort des Protokolls der Aufgabenausführung zu definieren (siehe nachfolgende Tabelle).

Syntax des Parameters `/W` des Befehls `KAVSHELL SCANCRITICAL`

Parameter/Option	Beschreibung

/W:<Name des Protokolls der Aufgabenausführung>	Wenn Sie diesen Parameter angeben, speichert Kaspersky Embedded Systems Security das Protokoll der Aufgabenausführung mit dem durch diesen Parameter vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse, die während der Aufgabe auftraten. Im Protokoll werden die Ereignisse aufgezeichnet, die durch die Einstellungen des Protokolls der Aufgabenausführung und Einstellungen des Ereignisprotokolls von Kaspersky Embedded Systems Security in der "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten **Protokolle der Aufgabenausführung** der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security die Protokolldatei nicht erstellen kann, wird eine Fehlermeldung angezeigt, der Befehl wird aber dennoch ausgeführt.

Aufgaben asynchron verwalten: 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 `[/pwd:<password>]`.

Syntac des Befehls KAVSHELL TASK

```
KAVSHELL TASK [<Alias des Aufgabenamens> </START | /STOP | /PAUSE | /RESUME | /STATE |
/STATISTICS >]
```

Beispiele des Befehls KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

Der Befehl `KAVSHELL TASK` kann ohne Parameter/Optionen oder mit einem oder mehreren Parametern/Optionen ausgeführt werden (siehe nachfolgende Tabelle).

KAVSHELL TASK Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
Keine Parameter	Zeigt die Liste aller vorhandenen Aufgaben von Kaspersky Embedded Systems Security an. Die Liste umfasst die folgenden Felder: Alias des Aufgabennamens, Aufgabenkategorie (System oder benutzerdefiniert) und aktueller Status der Aufgabe.
<Alias des Aufgabenamens>	Verwenden Sie anstatt des Aufgabennamens im Befehl SCAN TASK einen alternativen Namen (Task alias). Dies ist ein zusätzlicher Kurzname, den Kaspersky Embedded Systems Security an Aufgaben vergibt. Um die alternativen Namen der Aufgaben von Kaspersky Embedded Systems Security anzuzeigen, geben Sie den Befehl KAVSHELL TASK ohne einen Parameter ein.
/START	Starten der angegebenen Aufgabe im asynchronen Modus.
/STOP	Beenden einer angegebenen Aufgabe.
/PAUSE	Anhalten einer angegebenen Aufgabe.
/RESUME	Asynchrones Fortsetzen einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (z. B. *Läuft*, *Abgeschlossen*, *Angehalten*, *Beendet*, *Fehlgeschlagen*, *Wird gestartet*, *Wird fortgesetzt*).
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Aufgabenstart verarbeitet wurden

Beachten Sie, dass nicht alle Aufgaben von Kaspersky Embedded Systems Security die Schlüssel /PAUSE, /RESUME und /STATE unterstützen.

Rückgabecodes für den Befehl KAVSHELL TASK.

Das PPL-Attribut entfernen: KAVSHELL CONFIG

Mit dem Befehl `KAVSHELL CONFIG` können Sie das PPL-Attribut (Protected Process Light) für Kaspersky Security Service unter Verwendung des ELAM-Treibers entfernen, der während der Programminstallation installiert wurde.

Syntax des Befehls KAVSHELL CONFIG

```
KAVSHELL CONFIG /PPL:<OFF>
```

KAVSHELL CONFIG Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
/PPL:OFF	PPL-Attribut für Kaspersky Security Service entfernen.

Aufgaben zum Echtzeit-Computerschutz starten und beenden: KAVSHELL RTP

Mit dem Befehl `KAVSHELL RTP` können Sie alle Aufgaben zum Echtzeit-Computerschutz starten oder beenden.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Beispiele des Befehls KAVSHELL RTP

Um alle Aufgaben zum Echtzeit-Computerschutz zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL RTP /START
```

Der Befehl `KAVSHELL RTP` kann eine beliebige der beiden obligatorischen Optionen enthalten (s. Tabelle unten).

KAVSHELL RTP Befehlszeilenoptionen

Parameter/Optionen	Beschreibung
/START	Startet alle Aufgaben zum Echtzeit-Computerschutz: Echtzeitschutz für Dateien und Verwendung von KSN.
/STOP	Beendet alle Aufgaben zum Echtzeit-Computerschutz.

Aufgabe "Kontrolle des Programmstarts" verwalten: 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 Laden des DLL-Moduls zu überwachen, 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).

`KAVSHELL APPCONTROL /CONFIG` Befehlszeilenparameter/-optionen

Parameter/Option	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 • Statistik – Nur Statistik generieren
`/dll:<no|yes>`	Deaktivieren oder Aktivieren von "Upload von DLL-Modulen überwachen".
`/savetofile: <vollständiger Pfad der xml-Datei>`	Festgelegte Regeln in die angegebene Datei im XML-Format exportieren.
`/savetofile: <vollständiger Name der xml-Datei>`	Liste der Regeln in einer Datei speichern.
`/savetofile: <vollständiger Name der xml-Datei> /sdc`	Liste der Regeln für die Kontrolle für Installationspakete in einer Datei speichern.
`/clearsdc`	Alle Regeln für die Kontrolle für Installationspakete aus der Liste löschen.

Erstellen von Regeln für die Kontrolle des Programmstarts: KAVSHELL APPCONTROL /GENERATE

Mithilfe des Befehls `KAVSHELL APPCONTROL/GENERATE` können Sie die Listen der Regeln für die Kontrolle des Programmstarts erstellen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie `[/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 beliebiger 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 /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

Sie können Befehlszeilenparameter/-optionen verwenden, um die Einstellungen für das automatische Erstellen von Regeln der Aufgaben zur Kontrolle des Programmstarts zu konfigurieren (sieh nachfolgende Tabelle).

`KAVSHELL APPCONTROL /GENERATE` Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
Gültigkeitsbereich der Erlaubnisregeln	
<Ordnerpfad>	Geben Sie den Pfad zu dem Ordner mit den ausführbaren Dateien an, für welche die Erlaubnisregeln automatisch generiert werden.
/source:<Pfad der Datei mit der Ordnerliste>	Geben Sie den Pfad zu einer TXT-Datei mit einer Liste der Ordner an, die ausführbare Dateien enthalten, für welche die Erlaubnisregeln automatisch generiert werden.
/masks: <edms>	Geben Sie die Dateierweiterungen der ausführbaren Dateien an, für welche die Erlaubnisregeln automatisch generiert werden. Sie können Dateien mit den folgenden Erweiterungen in den Regelbereich aufnehmen: • e – Dateien mit der Erweiterung exe • d – Dateien mit der Erweiterung dll • m – Dateien mit der Erweiterung msi • s – Skripte
/runapp	Wenn Sie Erlaubnisregeln generieren, berücksichtigen Sie auch Programme, die derzeit auf dem geschützten Gerät ausgeführt werden.
Verhalten bei der automatischen Erstellung von Erlaubnisregeln	
/rules: <ch|cp|h>	Geben Sie Aktionen an, die während der Erstellung von Regeln für die Aufgabe 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 der Parameter /rules: <ch|cp> angegeben wird.
/user: <Benutzer oder Benutzergruppe>	Benutzername oder Name der Benutzergruppe angeben, für welche die Regeln angewendet werden sollen. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer und/oder die angegebene Benutzergruppe.
Verhalten nach Abschluss des Erstellens von Regeln für die Kontrolle des Programmstarts	
/export:	Speichert die generierten Regeln in einer XML-Datei.

<vollständiger Pfad der xml-Datei>	
/unique	Informationen über das geschützte Gerät mit installierten Programmen hinzufügen, die Grundlage für die Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts sind.
\prefix: <Präfix für die Regelnamen>	Geben Sie ein Präfix für die Namen von Erlaubnisregeln der Kontrolle des Programmstarts an.
/import: <a|r|m>	Importiert die generierten Regeln in die angegebene Liste der Regel für die Kontrolle des Programmstarts gemäß der ausgewählten Importregel: • a – **Zu den bestehenden Regeln hinzufügen** (Regeln mit identischen Einstellungen werden verdoppelt) • r – **Bestehende Regeln ersetzen** (Regeln mit identischen Einstellungen werden nicht hinzugefügt; es wird eine Regel hinzugefügt, wenn mindestens eine Regeleinstellung eindeutig ist) • m – **Mit bestehenden Regeln zusammenführen** (Regeln mit identischen Einstellungen werden nicht hinzugefügt; es wird eine Regel hinzugefügt, wenn mindestens eine Regeleinstellung eindeutig ist)

Regelliste für die Kontrolle des Programmstarts füllen: KAVSHELL APPCONTROL

Mithilfe des Befehls `KAVSHELL APPCONTROL` können Sie Regeln aus einer XML-Datei zur Regelliste der Aufgabe zur Kontrolle des Programmstarts gemäß der ausgewählten Importregel hinzufügen sowie alle bestehenden 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 `[/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 der Importregel "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
```

Sie können die Befehlszeilenparameter verwenden, um das Prinzip auszuwählen, das zum Hinzufügen neuer Regeln aus der angegebenen XML-Datei in die festgelegte Liste der Regeln für die Kontrolle des Programmstarts verwendet wird (siehe nachfolgende Tabelle).

KAVSHELL APPCONTROL Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
/append <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts basierend auf der angegebenen XML-Datei aktualisieren. Importregel – **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 basierend auf der angegebenen XML-Datei aktualisieren. Importregel – **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. Importregel – **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 für die Gerätekontrolle füllen: 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 `[/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 von einer XML-Datei zu den vorhandenen Regeln der Gerätekontrollaufgabe hinzuzufügen gemäß der Importregel "Zu den bestehenden Regeln hinzufügen", führen Sie den folgenden Befehl aus:

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Sie können die Befehlszeilenparameter verwenden, um die zu verwendende Importregel auszuwählen, die zum Hinzufügen neuer Regeln aus der angegebenen XML-Datei in die festgelegte Liste der Regeln für die Gerätekontrolle verwendet wird (siehe nachfolgende Tabelle).

KAVSHELL DEVCONTROL Befehlszeilenparameter/-optionen

Schlüssel	Beschreibung
/append <vollständiger	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen XML-Datei ergänzen. Importregel – **Zu den bestehenden Regeln hinzufügen** (Regeln mit identischen Einstellungen werden verdoppelt).

Pfad der xml-Datei>	
/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 Parametern 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. Importregel – **Mit bestehenden Regeln zusammenführen** (neue Regeln werden nicht dupliziert, wenn identische Regeln bereits vorhanden sind).
/clear	Liste der Regeln zur Gerätekontrolle leeren.

Die Aufgabe "Update der Programm-Datenbanken" starten: KAVSHELL UPDATE

Mit dem Befehl `KAVSHELL UPDATE` können Sie die Aufgabe zum Update der Programm-Datenbanken von Kaspersky Embedded Systems Security im Synchronmodus starten.

Eine Aufgabe zum Update der Programm-Datenbanken, die mit dem Befehl `KAVSHELL UPDATE` gestartet wurde, ist temporär. Sie wird nur während ihrer Ausführung in der Programmkonsole angezeigt. Es wird jedoch ein Protokoll der Aufgabenausführung generiert und unter **Protokolle der Aufgabenausführung** in 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 zur Verwendung von Kaspersky Security Center zur Verwaltung von Kaspersky Security für Windows Server auf geschützten Geräten finden Sie im Abschnitt "Verwaltung von Kaspersky Security für Windows Server über das Kaspersky Security Center".

Wenn Sie in dieser Aufgabe den Pfad eine Update-Quelle angeben, können Sie Umgebungsvariablen verwenden. Wenn eine Umgebungsvariable verwendet wird, führen Sie den Befehl `KAVSHELL UPDATE` als entsprechender Benutzer aus.

Syntax des Befehls KAVSHELL UPDATE

```
KAVSHELL UPDATE < Update-Quelle | /AK | /KL> [/NOUSEKL] [/PROXY:<Adresse>:<Port>]
[/AUTHTYPE:<0-2>] [/PROXYUSER:<Benutzername>] [/PROXYPWD:<Kennwort>] [/NOPROXYFORKL]
[/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE] [/TIMEOUT:<Sekunden>] [/REG:
<Code iso3166>] [/W:<Name des Protokolls der Aufgabenausführung>] [/ALIAS:<Alias des
Aufgabennamens>]
```

Der Befehl KAVSHELL UPDATE enthält sowohl obligatorische als auch Parameter/Optionen, deren Verwendung optional ist (s. Tabelle unten).

Beispiel für den Befehl KAVSHELL UPDATE

Um eine benutzerdefinierte Aufgabe zum Update der Programm-Datenbanken zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL UPDATE
```

Um eine Aufgabe zum Update der Programm-Datenbanken zu starten, dessen Updatedateien im Netzwerkordner \\server\bases gespeichert sind, führen Sie folgenden Befehl aus:

```
KAVSHELL UPDATE \\server\bases
```

Um eine Aufgabe zum Update der Programm-Datenbanken vom FTP-Server ftp://dnl-ru1.kaspersky-labs.com/ zu starten und alle Ereignisse der Aufgabe in die 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 Updates der Programm-Datenbanken für Kaspersky Embedded Systems Security von dem Kaspersky-Update-Server herunterzuladen, stellen Sie eine Verbindung zu der Update-Quelle her. Verwenden Sie dazu einen Proxyserver (Proxyserver-Adresse: proxy.company.com, Port: 8080). Führen Sie den folgenden Befehl aus, um über die integrierte Microsoft Windows NTLM-Authentifizierung mit dem Benutzernamen "inetuser" und dem Kennwort "123456" auf das geschützte Gerät zuzugreifen:

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

KAVSHELL UPDATE Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
Update-Quelle (obligatorischer Parameter). Geben Sie eine oder mehrere Quellen an. Kaspersky Embedded Systems Security greift der angegebenen Reihenfolge nach auf die Update-Quellen zu. Trennen Sie die Quellen durch Leerzeichen.	
<Pfad im Format UNC>	Benutzerdefinierte Update-Quelle Pfad des Netzwerk-Update-Ordners im UNC-Format.
<URL>	Benutzerdefinierte Update-Quelle Adresse eines HTTP- oder FTP-Servers, auf dem sich der Update-Ordner befindet.
<Lokaler Ordner>	Benutzerdefinierte Update-Quelle Ordner auf dem geschützten Gerät.
/AK	Geben Sie den Kaspersky Security Center-Administrationsserver als Update-Quelle an.
/KL	Geben Sie als Update-Quelle die Kaspersky-Update-Server an.
/NOUSEKL	Die Kaspersky-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 Parameter nicht angegeben ist, stellt Kaspersky Embedded Systems Security automatisch die Einstellungen des Proxyservers fest, der im lokalen Netzwerk verwendet wird.
/AUTHTYPE:<0-2>	Dieser Parameter bestimmt die Authentifizierungsmethode für den Zugriff auf den Proxyserver. Folgende Werte sind möglich: **0** – Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Embedded Systems Security greift unter dem Benutzerkonto **Lokales System** (**SYSTEM**) auf den Proxyserver zu; **1** – Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Embedded Systems Security greift unter dem Benutzernamen und Kennwort, die durch die Parameter /PROXYUSER und /PROXYPWD angegeben werden, auf den Proxyserver zu;

	2 – Authentifizierung mit Benutzername und Kennwort, die durch die Parameter /PROXYUSER und /PROXYPWD (basic authentication) angegeben werden. Wenn der Proxyserver keine Authentifizierung erfordert, muss dieser Parameter nicht festgelegt werden.
/PROXYUSER: <Benutzername>	Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn Sie /AUTHTYPE:0 angeben, werden die Parameter /PROXYUSER: <Benutzername> und /PROXYPWD:<Kennwort> ignoriert.
/PROXYPWD:<Kennwort>	Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn Sie /AUTHTYPE:0 angeben, werden die Parameter /PROXYUSER: <Benutzername> und /PROXYPWD:<Kennwort> ignoriert. Wenn der Parameter "/PROXYUSER" angegeben ist und der Parameter "/PROXYPWD" ausgelassen wurde, wird das Passwort als leere Zeichenkette angesehen.
/NOPROXYFORKL	Proxyserver-Einstellungen für die Verbindung zu den Kaspersky-Update-Servern nicht verwenden (werden standardmäßig verwendet).
/USEPROXYFORCUSTOM	Proxyserver-Parameter für die Verbindung zu benutzerdefinierten Update-Quellen verwenden (werden standardmäßig nicht verwendet).
/USEPROXYFORLOCAL	Proxyserver-Parameter für die Verbindung zu lokalen Update-Quellen verwenden. Wenn keine Einstellung angegeben wurde, wird die Einstellung **Für lokale Adressen keinen Proxyserver verwenden** verwendet.
Allgemeine Parameter eines FTP- und HTTP-Servers	
/NOFTPPASSIVE	Wenn dieser Schlüssel angegeben ist, verwendet Kaspersky Embedded Systems Security den FTP-Server im aktiven Modus für eine Verbindung zum geschützten Gerät. Wenn dieser Schlüssel nicht angegeben ist, verwendet Kaspersky Embedded Systems Security nach Möglichkeit den passiven Modus des FTP-Servers.
/TIMEOUT:<Anzahl der Sekunden>	Wartezeit für Verbindung mit einem FTP- oder HTTP-Server. Wenn Sie diesen Parameter nicht festlegen, verwendet Kaspersky Embedded Systems Security den Standardwert von 10 Sekunden. Der Wert muss als Ganzzahl eingegeben werden.
/REG:<Code iso3166>	Regionale Einstellungen Dieser Parameter wird beim Update-Download von den Update-Servern von Kaspersky verwendet. Kaspersky Embedded Systems Security optimiert den Update-Download auf das geschützte Gerät, indem der geografisch am nächsten liegenden Update-Server ausgewählt wird. Der Wert dieses Parameters sollte nach ISO 3166-1 als Alpha-2-Code für das Land angegeben werden, in dem sich das geschützte Gerät befindet, beispielsweise "/REG: gr" oder "/REG:US". Wenn dieser Schlüssel nicht angegeben oder ein ungültiger Landescode angegeben wird, erkennt Kaspersky Embedded Systems Security den Ort des geschützten Geräts entsprechend den regionalen Einstellungen des geschützten Geräts, auf dem die Programmkonsole installiert ist.
/ALIAS:<Alias des Aufgabenamens>	Mit diesem Parameter können Sie der Aufgabe einen alternativen Namen zuordnen, mit dem Sie auf die Aufgabe verweisen können, 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 Komponenten von Kaspersky Embedded Systems Security einmalig sein. Wenn dieser Schlüssel nicht festgelegt ist, erhält die Aufgabe einen alternativen Namen im Format update_<kavshell_pid> (z.B. update_1234). In der Programmkonsole erhält die Aufgabe den Namen "Update-databases <Datum und Uhrzeit>" (z. B. Update-databases 8/16/2007 5:41:02 PM).
/W:<Name des Protokolls	Wenn Sie diesen Parameter angeben, speichert Kaspersky Embedded Systems

der Aufgabenausführung>	Security das Protokoll der Aufgabenausführung mit dem durch diesen Parameter vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse, die während der Aufgabe auftraten. Im Protokoll werden die Ereignisse aufgezeichnet, die durch die Einstellungen des Protokolls der Aufgabenausführung und Einstellungen des Ereignisprotokolls von Kaspersky Embedded Systems Security in der "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten **Protokolle der Aufgabenausführung** der Programmkonsole angezeigt. Wenn Kaspersky Embedded Systems Security die Protokolldatei nicht erstellen kann, wird eine Fehlermeldung angezeigt, der Befehl wird aber dennoch ausgeführt.

Rückgabecodes für den Befehl KAVSHELL UPDATE

Rollback von Datenbanken-Updates von Kaspersky Embedded Systems Security ausführen: KAVSHELL ROLLBACK

Mit dem Befehl `KAVSHELL ROLLBACK` können Sie die lokale Systemaufgabe zum Rollback des Datenbanken-Updates von Kaspersky Embedded Systems Security ausführen. Dadurch werden die Datenbanken von Kaspersky Embedded Systems Security mit den zuvor installierten Updates wiederhergestellt. Der Befehl wird synchron ausgeführt.

Syntax des Befehls

```
KAVSHELL ROLLBACK
```

Rückgabecodes für den Befehl KAVSHELL ROLLBACK.

Protokollanalyse verwalten: 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
```

KAVSHELL TASK LOG-INSPECTOR zum Ändern der Befehlszeilenoptionen

Einstellung	Beschreibung
/START	Starten der angegebenen Aufgabe im asynchronen Modus.
/STOP	Beenden einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (z. B. *Läuft*, *Abgeschlossen*, *Angehalten*, *Beendet*, *Fehlgeschlagen*, *Wird gestartet*, *Wird fortgesetzt*).
/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.

Programm aktivieren: KAVSHELL LICENSE

Mit dem Befehl `KAVSHELL LICENSE` können Sie in Kaspersky Embedded Systems Security Schlüssel und Aktivierungscodes verwalten.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<Schlüsseldatei | Aktivierungscode> [/R] | /DEL:<Schlüssel |
Nummer des Aktivierungscodes>]
```

Beispiel 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).

KAVSHELL LICENSE Befehlszeilenparameter/-optionen

Parameter	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 Status * ist, wurde der Schlüssel als Reserveschlüssel hinzugefügt.
/ADD:<Name der Schlüsseldatei oder Aktivierungscode>	Fügt den Schlüssel mithilfe der angegebenen Datei oder eines 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 mit dem angegebenen Aktivierungscode.

Rückgabecodes für den Befehl KAVSHELL LICENSE.

Erstellung von Protokollen zur Ablaufverfolgung aktivieren, anpassen und deaktivieren: KAVSHELL TRACE

Mit dem Befehl `KAVSHELL TRACE` können Sie das Anlegen eines Ablaufverfolgungsberichts für alle Subsysteme von Kaspersky Embedded Systems Security aktivieren oder deaktivieren, und die entsprechende Protokollierungsstufe festlegen.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet.

Syntax des Befehls KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<path to trace log file folder> [/S:<Maximale Größe einer Log-Datei in MB>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Wenn die Ablaufverfolgung aktiviert ist und Sie die Einstellungen ändern möchten, geben Sie den Befehl `KAVSHELL TRACE` mit der Option "ON" ein und verwenden Sie die Parameter "/S" und "/LVL", um die Einstellungen für die Ablaufverfolgung festzulegen (siehe nachfolgende Tabelle).

Schlüssel des Befehls KAVSHELL TRACE

Schlüssel	Beschreibung
/ON	Führen eines Protokolls zur Ablaufverfolgung aktivieren
/F:<Ordner für Log-Dateien des Ablaufverfolgungsprotokolls>	Dieser Parameter gibt den vollständigen Pfad des Ordners an, in dem die Log-Dateien des Ablaufverfolgungsprotokolls gespeichert werden (obligatorischer Schlüssel). Wenn Sie den Pfad eines nicht vorhandenen Ordners angeben, wird kein Protokoll zur Ablaufverfolgung erstellt. Pfade zu Ordnern auf Netzlaufwerken von anderen nicht geschützten Geräten können nicht angegeben werden.

	Wenn der durch den Parameter angegebene Pfad ein Leerzeichen beinhaltet, muss dieser von Anführungszeichen umschlossen sein, beispielsweise /F:"C:\Trace Folder". Wenn Sie den Pfad von Log-Dateien des Ablaufverfolgungsberichts 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 Ablaufverfolgungsberichts. Sobald eine Log-Datei den Grenzwert erreicht, beginnt Kaspersky Embedded Systems Security, die Daten in eine neue Datei zu schreiben. Die bisherige Log-Datei wird gespeichert. Wenn Sie diesen Parameter nicht angeben, beträgt die maximale Größe für eine Log-Datei 50 MB.
/LVL:debug|info|warning|error|critical	Dieser Parameter 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 Parameter nicht angegeben ist, werden Ereignisse mit der Genauigkeitsstufe **Alle Debug-Informationen** im Protokoll zur Ablaufverfolgung aufgezeichnet.
/OFF	Diese Option 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 aktivieren 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 aktivieren 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.

Log-Dateien für Kaspersky Embedded Systems Security defragmentieren: KAVSHELL VACUUM

Mithilfe des Befehls `KAVSHELL VACUUM` können Sie Log-Dateien für Ereignisse des Programms defragmentieren. Dies hilft dabei, System- und Programmfehler zu vermeiden, die durch das Speichern einer großen Anzahl an Protokolldateien mit Programmereignissen verursacht werden.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie `[/pwd:<password>]`.

Wir empfehlen, dass Sie den Befehl `KAVSHELL VACUUM` verwenden, um den Potokolldateispeicher zu optimieren, wenn Untersuchungen auf Befehl und Update-Aufgaben in regelmäßigen Abständen ausgeführt werden. Dieser Befehl sorgt dafür, dass Kaspersky Embedded Systems Security die logische Struktur der Protokolldateien des Programms aktualisiert, die in dem angegebenen Pfad auf einem geschützten Gerät gespeichert sind.

Standardmäßig werden die Log-Dateien der Ereignisse bei der Ausführung des Programms im Pfad "C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Reports" gespeichert. Wenn Sie manuell einen anderen Pfad zum Speichern von Protokollen angegeben haben, defragmentiert der Befehl `KAVSHELL VACUUM` die Dateien im Ordner, der in den Einstellungen der Protokolle von Kaspersky Embedded Systems Security angegeben ist.

Die erforderliche Zeit für die Ausführung des Befehls `KAVSHELL VACUUM` und dem Abschluss der Defragmentierung steigt mit der Größe der Dateien.

Während der Ausführung des Befehls `KAVSHELL VACUUM` ist die Ausführung der Aufgaben Echtzeitschutz und Computer-Kontrolle unmöglich. Der Defragmentierungsvorgang sperrt den Zugang auf das Protokoll von Kaspersky Embedded Systems Security und verhindert ein Protokollieren von Ereignissen. Um den Schutz nicht zu beeinträchtigen, empfehlen wir, dass Sie im Voraus planen, zu welchem Zeitpunkt Sie den Befehl `KAVSHELL VACUUM` ausführen.

Um eine Defragmentierung der Log-Dateien für Ereignisse bei der Ausführung von Kaspersky Embedded Systems Security durchzuführen, führen Sie den folgenden Befehl aus:

```
KAVSHELL VACUUM
```

Für diesen Befehl sind Rechte des lokalen Systemkontos erforderlich.

iSwift-Basis bereinigen: KAVSHELL FBRESET

Kaspersky Embedded Systems Security verwendet die iSwift-Technologie, um eine erneute Untersuchung einer Datei zu vermeiden, wenn die Datei seit der vorherigen Untersuchung nicht verändert wurde (**iSwift-Technologie verwenden**).

Kaspersky Embedded Systems Security erstellt die Dateien "klamfb.dat" und "klamfb2.dat" im Ordner "%SYSTEMDRIVE%\System Volume Information". Diese Dateien enthalten Informationen über virenfreie Objekte, die bereits untersucht wurden. Je größer die Anzahl der Dateien, die von Kaspersky Embedded Systems Security untersucht worden sind, desto größer ist die Datei klamfb.dat (klamfb2.dat). Diese Datei enthält nur aktuelle Informationen über Dateien im System: Wenn eine Datei im System gelöscht wird, löscht Kaspersky Embedded Systems Security die entsprechenden Informationen aus der Datei klamfb.dat.

Um eine Datei zu leeren, verwenden Sie den Befehl `KAVSHELL FBRESET`.

Berücksichtigen Sie folgende Besonderheiten bei der Arbeit mit dem Befehl `KAVSHELL FBRESET`:

- Wenn Sie den Befehl "KAVSHELL FBRESET" verwenden, um die Datei "klamfb.dat" zu löschen, wird der Schutz von Kaspersky Embedded Systems Security nicht unterbrochen (im Gegensatz dazu wird der Schutz unterbrochen, wenn die Datei "klamfb.dat" manuell gelöscht wird).

- Nachdem die Datei klamfb.dat geleert wurde, kann sich die durch Kaspersky Embedded Systems Security verursachte Belastung des geschützten Geräts erhöhen. Dabei untersucht Kaspersky Embedded Systems Security alle Dateien, auf die nach dem Leeren der Datei klamfb.dat zum ersten Mal zugegriffen wird. Nach der Untersuchung speichert Kaspersky Embedded Systems Security Informationen zu jedem untersuchten Objekt wieder in die Datei "klamfb.dat". Wenn neue Versuche unternommen werden, um auf ein Objekt zuzugreifen, verhindert die iSwift-Technologie eine erneute Untersuchung der Datei, wenn sie nicht verändert wurde.

Zur Ausführung des Befehls `KAVSHELL FBRESET` muss der Kommandozeileninterpreter im Benutzerkonto SYSTEM gestartet werden.

Anlegen von Dump-Dateien aktivieren und deaktivieren: KAVSHELL DUMP

Sie können den Befehl `KAVSHELL DUMP` verwenden, um die Erstellung von Snapshots (Dump-Dateien) der Prozesse von Kaspersky Embedded Systems Security zu aktivieren oder zu deaktivieren, wenn diese mit einem Absturz abgeschlossen werden (siehe nachfolgende Tabelle). Zusätzlich können Sie zu jeder Zeit eine Dump-Datei der laufenden Prozesse von Kaspersky Embedded Systems Security erstellen.

Damit eine Dump-Datei erfolgreich erstellt werden kann, muss der Befehl `KAVSHELL DUMP` unter dem lokalen Systemkonto (SYSTEM) ausgeführt werden.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Embedded Systems Security unverschlüsselt aufgezeichnet.

Der Befehl KAVSHELL DUMP kann nicht für x64-Prozesse verwendet werden.

Syntax des Befehls KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<folder with the dump file>|/SNAPSHOT /F:<Ordner mit Dump-Datei> /
P:<pid> | /OFF>
```

KAVSHELL DUMP Befehlszeilenparameter/-optionen

Schlüssel	Beschreibung
/ON	Aktiviert die Erstellung einer Dump-Datei, wenn ein Prozess mit einem Absturz abgeschlossen wurde.
/F:<Pfad der Dump-Dateien>	Dieser Parameter ist obligatorisch. Er gibt den Pfad des Ordners an, in dem die Dump-Datei gespeichert wird. Pfade zu Ordnern auf Netzlaufwerken von anderen nicht geschützten Geräten sind nicht zulässig. Wenn Sie einen Pfad zum Ordner für die Dump-Datei angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariable sind dagegen nicht zulässig.
/SNAPSHOT	Nimmt ein Snapshot vom Speicher des laufenden Prozesses mit der angegebenen PID auf

	und speichert die Dump-Datei in den im Parameter "/F" angegebenen Ordner.
/P	Die Prozess-PID wird im Task-Manager von Microsoft Windows angezeigt.
/OFF	Deaktiviert die Erstellung einer Dump-Datei, wenn ein Prozess mit einem Absturz abgeschlossen wurde.

Rückgabecodes für den Befehl KAVSHELL DUMP

Beispiele des Befehls KAVSHELL DUMP

Um die Erstellung einer Dump-Datei zu aktivieren und die erstellte Dump-Datei im Ordner "C:\Dump-Ordner" zu speichern, führen Sie folgenden Befehl aus:

```
KAVSHELL DUMP /ON /F:"C:\Dump-Order"
```

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 deaktivieren, führen Sie folgenden Befehl aus:

```
KAVSHELL DUMP /OFF
```

Einstellungen importieren: KAVSHELL IMPORT

Mit dem Befehl `KAVSHELL IMPORT` können Sie die Einstellungen, von Kaspersky Embedded Systems Security und die aktuellen Aufgaben aus einer Konfigurationsdatei in Kaspersky Embedded Systems Security in eine Kopie von Kaspersky Embedded Systems Security auf dem geschützten Gerät 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 `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL IMPORT

```
KAVSHELL IMPORT <Name und Pfad der Konfigurationsdatei>
```

Biespiele des Befehls KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Befehlszeilenparameter KAVSHELL IMPORT

Parameter	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

Einstellungen exportieren: KAVSHELL EXPORT

Mit dem Befehl `KAVSHELL EXPORT` können Sie alle Einstellungen von Kaspersky Embedded Systems Security und die aktuellen Aufgaben in eine Konfigurationsdatei exportieren, um sie in ein anderes geschütztes Gerät in Kaspersky Embedded Systems Security zu importieren.

Syntax des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiele des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Befehlszeilenparameter KAVSHELL EXPORT

Parameter	Beschreibung
<Name und Pfad der Konfigurationsdatei>	Name der Konfigurationsdatei, in der die Einstellungen 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

Integration in Microsoft Operation Management Suite: KAVSHELL OMSINFO

Mithilfe des Befehls KAVSHELL OMSINFO können Sie den Programmstatus sowie Informationen über die von den Antiviren-Datenbanken und dem KSN-Dienst gefundenen Bedrohungen anzeigen. Die Informationen über Bedrohungen werden den verfügbaren Ereignisprotokollen entnommen.

Syntax des Befehls KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <vollständiger Pfad zur erstellten Datei samt Dateiname>
```

Beispiel für den Befehl KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Befehlszeilenparameter KAVSHELL OMSINFO

Parameter	Beschreibung
<Pfad zur erstellten Datei samt Dateiname>	Name der erstellten Datei, die Informationen über den Programmstatus und die erkannten Bedrohungen enthalten wird.

Die Aufgabe zur Überwachung der Baseline-Integrität verwalten: KAVSHELL FIM /BASELINE

Mithilfe des Befehls `KAVSHELL FIM/BASELINE` können Sie den Ausführungsmodus der Aufgabe zur Überwachung der Baseline-Integrität anpassen und den Laden von DLL-Modulen überwachen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL FIM/BASELINE

```
KAVSHELL FIM /BASELINE [/CREATE: [<Überwachungsbereich> | /L:<Pfad der TXT-Datei, welche die Liste der Überwachungsbereiche enthält>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<Baseline-ID> | /ALIAS:<vorhandener Alias>]] | [/EXPORT:<Pfad der TXT-Datei> [/BL:<Baseline-ID> | /ALIAS:<vorhandener Alias>]] | [/SHOW [/BL:<Baseline-ID> | /ALIAS:<vorhandener Alias>]] | [/SCAN [/BL:<Baseline-ID> | /ALIAS:<vorhandener Alias>]] | [/PWD:<Kennwort>]
```

Beispiele für den Befehl KAVSHELL FIM/BASELINE

Führen Sie zum Löschen einer Baseline den folgenden Befehl aus:

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<Baseline-ID>
```

Sie können die Einstellungen der Aufgabe zur Überwachung der Baseline-Integrität mithilfe von Schlüsseln anpassen (s. Tabelle unten).

`KAVSHELL FIM/ BASELINE` Befehlszeilenparameter/-optionen

Parameter/Option	Beschreibung
`/CREATE`	Erstellt eine neue Aufgabe zur Überwachung der Baseline-Integrität. Kaspersky Embedded Systems Security startet die neue Aufgabe zur Überwachung der Baseline-Integrität, um eine Baseline zu erstellen.
`/L`	Geben Sie den Pfad der TXT-Datei an, welche die Liste der Überwachungsbereiche enthält.
`/MD5`	Legt den Algorithmus MD5 für die Berechnung einer Prüfsumme fest (optionaler Parameter). Der Parameter `/MD5` kann nicht zusammen mit `/SHA256` verwendet werden. Der Algorithmus MD5 wird standardmäßig verwendet.
`/SHA256`	Legt den Algorithmus SHA256 für die Berechnung einer Prüfsumme fest (optionaler Parameter). Der Parameter `/SHA256` kann nicht zusammen mit `/MD5` verwendet werden.

	Der Algorithmus MD5 wird standardmäßig verwendet.
`/SF`	Bezieht alle Unterordner in dem Aufgabenbereich der Überwachung der Baseline-Integrität ein (optionaler Parameter). Standardmäßig werden alle Unterordner aus dem Aufgabenbereich der Überwachung der Baseline-Integrität ausgeschlossen.
`/CLEAR`	Löscht die Baseline mit der angegebenen `<Baseline-ID>` oder die Baseline für die Aufgabe mit dem angegebenen `<vorhandenen Alias>`. Löscht alle Baselines, wenn weder eine `<Baseline-ID>` noch ein `<vorhandener Alias>` angegeben wurde. Optionaler Parameter.
`/BL`	Geben Sie die eindeutige ID einer Baseline an (optionaler Parameter).
`/EXPORT`	Exportiert die Daten zu allen Baselines in eine TXT-Datei.
`/SHOW`	Zeigt Daten zu allen Baselines an.
`/SCAN`	Startet die neue Aufgabe zur Überwachung der Baseline-Integrität mit der angegebenen `<Baseline-ID>` oder dem angegebenen `<vorhandenen Alias>`.
`/ALIAS`	Geben Sie den Namen einer vorhandenen Aufgabe oder den Namen einer neuen Aufgabe an.
`<Überwachungsbereich>`	Geben Sie die Datei oder den Ordner an, die bzw. der in den Aufgabenbereich der Überwachung der Baseline-Integrität aufgenommen werden soll. Mit diesem Parameter kann nur ein Bereich angegeben werden.
`<Pfad der TXT-Datei, welche die Liste der Überwachungsbereiche enthält>`	Geben Sie den Pfad der TXT-Datei an, welche die Liste der Überwachungsbereiche enthält. Die Datei muss UTF-8-codiert sein. Jeder Pfad zu einem Überwachungsbereich muss in einer separaten Zeile angegeben werden.
`<Pfad der TXT-Datei>`	Geben Sie den Pfad der Datei an, in welche die Daten zu allen Baselines exportiert werden sollen.
`<Baseline-ID>`	Geben Sie die eindeutige ID einer Baseline an. Mithilfe des Parameters `/SHOW` können Sie die ID einer Baseline ermitteln.
`<vorhandener Alias>`	Geben Sie den Namen einer vorhandenen Aufgabe an.
`<neuer Alias>`	Geben Sie den Namen einer neuen Aufgabe an.

Rückgabecodes der Befehle

Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP

Rückgabecode 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 Kaspersky Security Service schon gestartet oder schon beendet)
-7	Service ist nicht registriert
-8	Der automatische Start des Dienstes ist deaktiviert
-9	Versuch zum Starten des geschützten Geräts unter einem anderen Benutzerkonto war erfolglos (in der Standardeinstellung arbeitet der Dienst Kaspersky Security Service unter dem Benutzerkonto Lokales System)
-99	Unbekannter Fehler

Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL

Rückgabecode 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	Fehler beim Erstellen des Protokolls der Aufgabenausführung
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR

Rückgabecode für den Befehl KAVSHELL TASK LOG-INSPECTOR

Feedback-Code	Beschreibung

0	Operation wurde erfolgreich ausgeführt.
-6	Ungültiger Vorgang (zum Beispiel ist Kaspersky Security Service schon gestartet oder schon beendet)
402	Aufgabe ist schon gestartet (für die Option /STATE)

Rückgabecodes für den Befehl KAVSHELL TASK

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 die Option /STATE)
402	Aufgabe ist schon gestartet (für die Option /STATE)
403	Aufgabe ist schon angehalten (für die Option /STATE)
-404	Ungültiger Vorgang (eine Änderung im Status der Aufgabe führt zu einem Absturz)

Rückgabecodes für den Befehl KAVSHELL RTP

Rückgabecodes für den Befehl KAVSHELL RTP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (eine oder alle Aufgaben zum Echtzeit-Computerschutz wurden 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

Rückgabecodes für den Befehl KAVSHELL UPDATE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
200	Alle Objekte sind aktuell (Datenbanken oder Programm-Komponenten sind in einem aktuellen Zustand)
-2	Service nicht gestartet
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-99	Unbekannter Fehler
-206	Updatedateien sind nicht vorhanden oder falsches Format
-209	Fehler bei Verbindung mit Update-Quelle
-232	Authentifizierungsfehler bei Verbindung mit dem Proxyserver
-234	Fehler bei Verbindung zum Programm Kaspersky Security Center
-235	Kaspersky Embedded Systems Security hat die Authentifizierungsprüfung beim Verbinden mit der Update-Quelle nicht bestanden
-236	Die Datenbanken von Kaspersky Embedded Systems Security sind beschädigt
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-99	Unbekannter Fehler
-221	Backup-Kopie der Datenbanken nicht gefunden
-222	Backup-Kopie der Datenbanken ist beschädigt

Rückgabecodes für den Befehl KAVSHELL LICENSE

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

Rückgabecodes für den Befehl KAVSHELL TRACE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (angegebener Pfad für Ordner mit den Log-Dateien für das Ablaufverfolgungsprotokoll nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch den Befehl "KAVSHELL TRACE /OFF" auszuführen, während die Ablaufverfolgungen bereits deaktiviert sind)
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL FBRESET

Rückgabecodes für den Befehl KAVSHELL FBRESET

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL DUMP

Rückgabecodes für den Befehl KAVSHELL DUMP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet

-3	Zugriffsfehler
-4	Objekt nicht gefunden (angegebener Pfad für Ordner mit Dump-Datei nicht gefunden; 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

Rückgabecodes für den Befehl KAVSHELL IMPORT

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (es wurde keine Konfigurationsdatei gefunden, die importiert werden kann)
-5	Ungültige Syntax
-99	Unbekannter Fehler
501	Der Vorgang wurde erfolgreich mit einem Fehler bzw. Kommentar ausgeführt (z. B. Kaspersky Embedded Systems Security hat die Einstellungen für bestimmte funktionelle Komponente nicht importiert).
-502	Importdatei 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 exportiert)

Rückgabecodes für den Befehl KAVSHELL EXPORT

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 mit einem Fehler bzw. Kommentar ausgeführt (z. B. Kaspersky

	Embedded Systems Security hat die Einstellungen für bestimmte funktionelle Komponente nicht exportiert).

Rückgabecodes für den Befehl KAVSHELL FIM /BASELINE

Rückgabecodes für den Befehl KAVSHELL FIM /BASELINE

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 (beispielsweise wurde die Baseline bereits gelöscht)
-10	Konfigurationsdatei konnte nicht erstellt werden (beispielsweise kein Zugang zum Ordner, welcher im Pfad vorgegeben wurde)
-12	Ungültiges Kennwort
-80	Inkonsistent mit den erkannten Baseline-Objekten
-85	Fehler beim Erstellen des Protokolls der Aufgabenausführung
-99	Interner Fehler
-303	Ungültiger Lizenzschlüssel
-502	Aufgabe wird nicht ausgeführt
200	Alle Objekte sind mit der Baseline konsistent
501	Die Aufgabe wurde erfolgreich mit einem Fehler oder Kommentar abgeschlossen

Kontaktaufnahme mit dem Technischen Support

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

Wie Sie technischen Support erhalten

Wenn Sie in der Dokumentation oder in 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.

Die Programmunterstützung wird entsprechend des Programmlebenszyklus bereitgestellt (siehe auch Seite mit Produktlebenszyklen).

Bevor Sie sich an unseren Technischen Support wenden, machen Sie sich bitte mit unseren Support-Regeln vertraut.

Sie können eine Anfrage an den Technischen Support von Kaspersky über das Portal Kaspersky CompanyAccount senden.

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Programme von Kaspersky verwenden. Über das Portal Kaspersky CompanyAccount können Benutzer mit Kaspersky-Experten mithilfe von Online-Anfragen kommunizieren. Über das Portal Kaspersky CompanyAccount kann der Status der Verarbeitung elektronischer Anfragen durch Kaspersky-Spezialisten nachverfolgt sowie eine Chronik der elektronischen Anfragen gespeichert werden.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Ein Benutzerkonto ermöglicht Ihnen die zentralisierte Verwaltung von elektronischen Anfragen aller registrierten Mitarbeiter an Kaspersky sowie die Verwaltung der Rechte dieser Mitarbeiter in Kaspersky CompanyAccount.

Das Portal Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch

- Portugiesisch
- Russisch
- Französisch
- Japanisch

Mehr über Kaspersky CompanyAccount erfahren Sie auf der Website des Technischen Supports.

Protokolldatei und AVZ-Skript verwenden

Wenn Sie sich mit einem Problem an die Experten des Technischen Supports von Kaspersky wenden, werden Sie möglicherweise darum gebeten, einen Bericht über Kaspersky Embedded Systems Security zu erstellen und den Bericht an den Technischen Support von Kaspersky zu schicken. Zusätzlich können die Experten des Technischen Supports von Kaspersky 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 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 geschützten Geräts erstellt werden.

Glossar

Administrationsserver

Programmkomponente von Kaspersky Security Center, mit der die zentralisierte Speicherung von Informationen über die im Unternehmensnetzwerk installierten Programme von Kaspersky realisiert wird. Die Verwaltung dieser Programme erfolgt ebenfalls über diese Komponente.

Aktiver Schlüssel

Ein Lizenzschlüssel, der momentan vom Programm verwendet wird.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die Kaspersky 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 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-Programm führt seine Funktionen in Form von Aufgaben aus, zum Beispiel: "Echtzeitschutz für Dateien", "Vollständige Untersuchung des Computers" und "Update der Programm-Datenbanken".

Aufgabeneinstellungen

Programmeinstellungen, die für den jeweiligen Aufgabentyp gelten.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die ordnungsgemäße Ausführung des auf dem Computer installierten Betriebssystems und der Software benötigt wird. Diese Objekte werden bei jedem Start des Betriebssystems ausgeführt. Es gibt Viren, die genau diese Objekte infizieren können, was beispielsweise dazu führen kann, dass das Betriebssystem nicht gestartet wird.

Backup

Ein spezieller Speicher für Backup-Kopien von Dateien, die vor dem Desinfektionsversuch oder dem Löschen der Dateien erstellt werden.

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.

Ereignispriorität

Eigenschaft eines Ereignisses, das während der Ausführung eines Kaspersky-Programms aufgetreten ist. Es gibt folgende Signifikanzen:

- Kritisches Ereignis
- Funktionsfehler
- Warnung
- Info

Ereignisse vom gleichen Typ können je nach der Situation, in der sie auftreten, unterschiedliche Signifikanzen haben.

Fehlalarm

Eine Situation, in der ein Programm von Kaspersky ein nicht infiziertes Objekt als infiziert betrachtet, weil dessen Code dem eines Virus ähnelt.

Heuristische Analyse

Technologie zur Erkennung von Bedrohungen, über die noch keine Informationen in den Datenbanken von Kaspersky 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).

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 empfiehlt nicht, auf solche Objekte zuzugreifen.

Kaspersky Security Network (KSN)

Infrastruktur aus Cloud-Diensten, die Zugriff auf die Kaspersky-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 auf neue Bedrohungen, erhöht die Effektivität der Arbeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

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.

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.

Quarantäne

Ordner, in den die Programme von Kaspersky erkannte möglicherweise infizierte Objekte verschieben. Objekte werden in der Quarantäne in verschlüsselter Form gespeichert, um eine Einwirkung auf den Computer zu vermeiden.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen eines Programms und verwaltet die Möglichkeiten zum Konfigurieren dieses Programms auf Computern innerhalb einer Administrationsgruppe. Für jedes Programm muss eine separate Richtlinie erstellt werden. Sie können für Programme, die auf Computern in jeder Administrationsgruppe installiert sind, mehrere Richtlinien erstellen; allerdings kann jeweils nur eine Richtlinie gleichzeitig für ein Programm innerhalb einer Administrationsgruppe übernommen werden.

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.

Update

Vorgang zum Ersetzen bestehender oder zum Hinzufügen neuer Dateien (Datenbanken oder Programm-Module), die von den Kaspersky-Update-Servern heruntergeladen wurden.

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 Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

CVE ist ein eingetragenes Markenzeichen von The MITRE Corporation.

Core, Intel und Pentium sind in den USA und/oder anderen Ländern eingetragene Markenzeichen der Intel Corporation.

Linux ist ein registriertes Warenzeichen von Linus Torvalds in den USA und anderen Ländern.

Microsoft, Active Directory, Excel, Internet Explorer, Outlook, Windows, Windows Server und Windows Vista sind in den USA und anderen Ländern eingetragene Markenzeichen der Microsoft Corporation.

UNIX ist ein registriertes Warenzeichen in den Vereinigten Staaten und anderen Ländern, das ausschließlich über X/Open Company Limited lizenziert ist.