KASPERSKY lab

Kaspersky Security für Windows Server

Administratorhandbuch

Produktversion: 10.1.0.622

Sehr geehrter Benutzer!

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

Achtung! Die Rechte an diesem Dokument liegen bei AO Kaspersky Lab (im Folgenden "Kaspersky Lab") und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt. Bei illegalem Kopieren und Weiterverbreiten des Dokumentes und seiner einzelnen Teile haftet der Zuwiderhandelnde nach dem Zivilrecht, Verwaltungsrecht oder Strafrecht der Gesetzgebung.

Jegliche Art der Vervielfältigung oder Verbreitung von Materialien, einschließlich Übersetzungen, ist nur mit schriftlicher Genehmigung von Kaspersky Lab gestattet.

Das Dokument und die damit verbundenen grafischen Darstellungen dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Kaspersky Lab behält sich das Recht vor, dieses Dokument ohne weitere Benachrichtigung zu ändern.

Für den Inhalt, die Qualität, die Richtigkeit und Vertrauenswürdigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für Schäden, die in Verbindung mit der Nutzung dieser Unterlagen entstehen, lehnt Kaspersky Lab die Haftung ab.

Eingetragene Marken und Dienstleistungszeichen, die in diesem Dokument verwendet werden, sind Eigentum der jeweiligen Rechteinhaber.

Redaktionsdatum des Dokuments: 26.03.2018

© 2018 AO Kaspersky Lab. Alle Rechte vorbehalten.

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

Inhalt

Über dieses Handbuch

Das Administratorhandbuch für Kaspersky Security 10.1.0.622 für Windows Server. Das Administratorhandbuch (im Weiteren "Kaspersky Security 10.1 für Windows Server") richtet sich an die Experten, die für die Installation und die Verwaltung von Kaspersky Security 10.1 für Windows Server auf allen geschützten Geräten zuständig sind, sowie an die Experten für den technischen Support der Unternehmen, die Kaspersky Security 10.1 für Windows Server verwenden.

Dieses Handbuch enthält Informationen über die Konfiguration und Verwendung von Kaspersky Security 10.1 für Windows Server.

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

In diesem Kapitel

In diesem Dokument

Das Administratorhandbuch für Kaspersky Security 10.1 für Windows Server enthält folgende Abschnitte.

Informationsquellen über Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt beschreibt Funktionen, Komponenten und Lieferumfang von Kaspersky Security 10.1 für Windows Server sowie die Hard- und Software-Voraussetzungen für Kaspersky Security 10.1 für Windows Server.

Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält schrittweise Anleitungen zur Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server.

Programmoberfläche

Dieser Abschnitt enthält Informationen zu den Elementen der Programmoberfläche von Kaspersky Security 10.1 für Windows Server.

Lizenzverwaltung für das Programm

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

Starten und Beenden von Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält Informationen zum Start und Stoppen des Verwaltungs-Plug-ins für Kaspersky Security 10.1 für Windows Server (im Weiteren Verwaltungs-Plug-in für Kaspersky Security 10.1 für Windows Server) sowie von Kaspersky Security Service.

Über Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält Informationen über die Rechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server und der Windows®-Dienste, die das Programm registriert, sowie eine Anleitung zur Konfiguration dieser Rechte.

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt enthält Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Security 10.1 für Windows Server auf mehreren Servern.

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Security 10.1 für Windows Server, ihre Erstellung, die Konfiguration ihrer Ausführung sowie über den Start/die Beendigung von Aufgaben.

Programmeinstellungen verwalten

Dieser Abschnitt enthält Informationen über die Konfiguration der allgemeinen Einstellungen von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center.

Echtzeitschutz

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

Überwachung der Server-Aktivitäten

Dieser Abschnitt enthält Informationen über die Funktionen von Kaspersky Security 10.1 für Windows Server zur Kontrolle der Starts und Verbindungen von Apps durch externe Geräte über USB.

Netzwerküberwachung

Dieser Abschnitt enthält Informationen über die Aufgaben zur Firewall-Verwaltung und zum Schutz vor Verschlüsselung.

System-Diagnose

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

Leistungskontrolle. Indikatoren in Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt informiert über die Indikatoren von Kaspersky Security 10.1 für Windows Server: Leistungsindikatoren für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps.

Arbeiten mit Kaspersky Security 10.1 für Windows Server aus der Befehlszeile

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Security 10.1 für Windows Server aus der Befehlszeile.

Kontaktaufnahme mit dem Technischen Support

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

Glossar

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

AO Kaspersky Lab

Dieser Abschnitt bietet Informationen über AO Kaspersky Lab.

Informationen über den Code von Drittherstellern

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

Markenrechtliche Hinweise

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

Sachregister

Dieser Abschnitt ermöglicht das schnelle Auffinden bestimmter Angaben im Dokument.

Formatierung mit besonderer Bedeutung

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

Tabelle 1. Formatierung mit besonderer Bedeutung

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

Textbeispiel	Beschreibung der Formatierung
► *Um den Aufgabenzeitplan anzupassen, gehen Sie wie folgt vor:*	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.
Geben Sie in der Befehlszeile den Text `help` ein. Es erscheint folgende Meldung: Geben Sie das Datum im Format `TT:MM:JJ` an.	Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben: • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt. • Daten, die über die Tastatur eingegeben werden müssen.
<Benutzername>	Variable stehen in eckigen Klammern. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

Informationsquellen über Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

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

In diesem Kapitel

Quellen für die selbstständige Informationssuche

Für Kaspersky Security 10.1 für Windows Server stehen Ihnen folgende Informationsquellen zur Verfügung:

- Seite von Kaspersky Security 10.1 für Windows Server auf der Webseite von Kaspersky Lab
- Seite von Kaspersky Security 10.1 für Windows Server auf der Webseite des Technischen Supports (Wissensdatenbank)
- Dokumentation

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

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

Seite von Kaspersky Security 10.1 für Windows Server auf der Website von Kaspersky Lab

Auf der Seite von Kaspersky Security 10.1 für Windows Server https://www.kaspersky.de/small-to-medium-business-security/windows-server-security stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

Auf der Seite für Kaspersky Security 10.1 für Windows Server befindet sich ein Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite von Kaspersky Security 10.1 für Windows Server in der Wissensdatenbank

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

Auf der Seite von Kaspersky Security 10.1 für Windows Server in der Wissensdatenbank http://support.kaspersky.com/de/ksws10 finden Sie Artikel, die nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zum Erwerb, zur Installation und zur Anwendung des Programms enthalten.

Artikel der Wissensdatenbank beantworten Fragen nicht nur in Bezug auf Kaspersky Security 10.1 für Windows Server, sondern auch auf andere Programme von Kaspersky Lab. Außerdem können Artikel der Wissensdatenbank auch Neuigkeiten über den Technischen Support enthalten.

Dokumentation für Kaspersky Security 10.1 für Windows Server

Das Administratorhandbuch von Kaspersky Security 10.1 für Windows Server enthält Informationen über die Installation, Deinstallation, Konfiguration und Nutzung des Programms.

Diskussion über die Programme von Kaspersky Lab im Forum

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

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

Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt beschreibt Funktionen, Komponenten und Lieferumfang von Kaspersky Security 10.1 für Windows Server sowie die Hard- und Software-Voraussetzungen für Kaspersky Security 10.1 für Windows Server.

In diesem Kapitel

Über Kaspersky Security 10.1 für Windows Server

Kaspersky Security 10.1 für Windows Server (früher "Kaspersky Anti-Virus für Windows Server Enterprise Edition") schützt Server mit Microsoft® Windows®-Betriebssystemen und Netzwerkspeicher vor Viren und anderen Bedrohungen für die Computersicherheit, die bei der Übertragung von Dateien eindringen können. Kaspersky Security 10.1 für Windows Server ist zum Einsatz in lokalen Netzwerken mittlerer und großer Unternehmen vorgesehen. Als Benutzer von Kaspersky Security 10.1 für Windows Server gelten Netzwerkadministratoren des Unternehmens und Mitarbeiter, die für den Antiviren-Schutz des Unternehmensnetzwerks zuständig sind.

Sie können Kaspersky Security 10.1 für Windows Server auf den folgenden Servern installieren:

- Terminalserver
- Druckerserver
- App-Server
- Domain Controller
- Server zum Schutz von Netzwerkspeichern
- Dateiserver – Diese Arten von Servern unterliegen dem höchsten Infektionsrisiko, weil sie Dateien mit Benutzer-Workstations austauschen.

Kaspersky Security 10.1 für Windows Server kann auf folgende Arten verwaltet werden:

- Über die Konsole für Kaspersky Security 10.1, die auf einem Server mit Kaspersky Security 10.1 für Windows Server oder auf einem anderen Computer installiert ist.
- Mithilfe eines Befehls in der Befehlszeile.
- Über die Verwaltungskonsole für Kaspersky Security Center.

Sie können das Programm Kaspersky Security Center verwenden, das der zentralisierten Verwaltung des Schutzes mehrerer Server dient, auf denen jeweils eine Exemplar von Kaspersky Security 10.1 für Windows Server installiert ist.

Sie können die Leistungsindikatoren von Kaspersky Security 10.1 für Windows Server für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps analysieren.

Komponenten und Funktionen von Kaspersky Security 10.1 für Windows Server

Im Lieferumfang des Programms sind folgende Komponenten enthalten:

- **Echtzeitschutz**. Kaspersky Security 10.1 für Windows Server untersucht Objekte, wenn darauf zugegriffen wird. Kaspersky Security 10.1 für Windows Server untersucht die folgenden Objekte:
  - Dateien
  - alternative Datenströme der Dateisysteme (NTFS-Streams)
  - MBR und Bootsektoren von lokalen Festplatten und Wechseldatenträgern.
- **Untersuchung auf Befehl**. Kaspersky Security 10.1 für Windows Server überprüft den angegebenen Bereich einmalig auf Viren und andere Bedrohungen der Computersicherheit. Das Programm prüft die Dateien, den Arbeitsspeicher des geschützten Geräts sowie die Objekte des Autostarts.
- **Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern** und **Schutz von per ICAP-Protokoll verbundenen Netzwerkspeichern**. Wenn Kaspersky Security 10.1 für Windows Server auf einem Server mit einem Microsoft Windows-Betriebssystem installiert ist, werden Netzwerkspeicher vor Viren und anderen Bedrohungen für die Computersicherheit geschützt, die bei der Übertragung von Dateien eindringen können.
- **Kontrolle des Programmstarts**. Diese Komponente überwacht die Versuche der Benutzer, das Programm zu starten, und regelt den Programmstart.
- **Gerätekontrolle**. Diese Komponente ermögliche eine Kontrolle der Registrierung und der Verwendung von Massenspeichergeräten und CD-/DVD-Geräten, um den Computer vor Gefahren zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können.
- **Schutz vor Verschlüsselung** und **Anti-Cryptor für NetApp**. Die Komponenten schützen freigegebene Ordner auf Servern und Netzwerkspeichern vor bösartiger Verschlüsselung, indem Computer, die bösartige Aktivitäten zeigen, blockiert werden.
- **Skript-Untersuchung**. Diese Komponente kontrolliert die Ausführung von Skripten, die unter Verwendung von Microsoft Windows Script Technologies erstellt wurden.
- **Schutz des Datenverkehrs**. Diese Komponente fängt Objekte ab, die über den Web-Datenverkehr übertragen werden (einschließlich E-Mails), und untersucht sie, um bekannte Computer- und andere Bedrohungen auf dem geschützten Server zu erkennen.
- **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 Konfiguration der Firewall-Einstellungen auf andere Weise.
- **Überwachung der Datei-Integrität**. Kaspersky Security 10.1 für Windows Server erkennt Änderungen in Dateien im in den Aufgabeneinstellungen festgelegten Überwachungsbereich. Diese Änderungen können auf eine Sicherheitsverletzung auf dem geschützten Computer hinweisen.
- **Protokollanalyse**. Diese Komponente führt eine Integritätsprüfung des geschützten Mittwochs auf Grundlage der Ergebnisse der Protokollanalyse von Windows-Ereignissen aus.

Das Programm verfügt über folgenden Funktionen:

- **Update der Programm-Datenbanken** und **Update der Programm-Module.** Für den Download von Updates der Programm-Datenbanken und Programm-Module verwendet Kaspersky Security 10.1 für Windows Server die FTP- oder HTTP-Kaspersky Lab Update-Server, den Administrationsserver

von Kaspersky Security Center oder andere Update-Quellen.

- **Quarantäne**. Objekte, die von Kaspersky Security 10.1 für Windows Server als möglicherweise infiziert eingestuft wurden, werden unter Quarantäne gestellt, d. h. die Objekte werden von ihrem ursprünglichen Speicherort in die *Quarantäne* verschoben. Aus Sicherheitsgründen werden Objekte in der Quarantäne in verschlüsselter Form gespeichert.
- **Backup**. Bevor ein Objekt mit dem Status *Infiziert* oder *Möglicherweise infiziert* desinfiziert oder gelöscht wird, speichert Kaspersky Security 10.1 für Windows Server eine verschlüsselte Sicherungskopie im *Backup*.
- **Benachrichtigungen an den Administrator und die Benutzer**. Sie können die Benachrichtigung des Administrators und der Benutzer, die auf den geschützten Computer zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Security 10.1 für Windows Server und dem Status des Antiviren-Schutzes des Computers zusammenhängen, anpassen.
- **Import und Export von Einstellungen**. Sie können die Einstellungen von Kaspersky Security 10.1 für Windows Server in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Security 10.1 für Windows Server importieren. In einer Konfigurationsdatei können entweder alle Einstellungen des Programms oder nur die Einstellungen bestimmter Programmkomponenten gespeichert werden.
- **Verwendung von Vorlagen**. Sie können die Sicherheitseinstellungen eines Knotens in der Struktur oder in der Liste der Dateiressourcen des Computers manuell konfigurieren und die Werte der angepassten Einstellungen in einer Vorlage speichern. Sie können diese Vorlage später bei der Konfiguration der Sicherheitseinstellungen anderer Knoten in den Schutz- und Untersuchungsaufgaben von Kaspersky Security 10.1 für Windows Server verwenden.
- **Verwaltung der Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server**. Sie können die Rechte für die Verwaltung von Kaspersky Security 10.1 für Windows Server und der Windows-Dienste, die das Programm registriert, für Benutzer und Benutzergruppen konfigurieren.
- **Protokollieren von Ereignissen im Ereignisbericht des Programms**. Kaspersky Security 10.1 für Windows Server protokolliert Informationen über die Einstellungen von Softwarekomponenten, den aktuellen Aufgabenstatus, Ereignisse, die bei der Aufgabenausführung eintreten, Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Security 10.1 für Windows Server sowie Informationen, die für die Fehlerdiagnose in Kaspersky Security 10.1 für Windows Server erforderlich sind.
- **Hierarchischer Speicher**. Kaspersky Security 10.1 für Windows Server kann zusammen mit Systemen für die Verwaltung hierarchischer Speicher (HSM-Systemen) verwendet werden. Die Verwendung von HSM-Systemen ermöglicht die Übertragung von Daten zwischen schnellen lokalen Laufwerken und langsamen Geräten für die langfristige Datenspeicherung.
- **Vertrauenswürdige Zone**. Sie können eine Liste mit Ausnahmen aus dem Schutzbereich bzw. Untersuchungsbereich anlegen, die Kaspersky Security 10.1 für Windows Server bei der Ausführung der Aufgaben zur Untersuchung auf Befehl und zum Echtzeitschutz für Dateien anwenden wird.
- **Exploit-Prävention**. Sie können den Prozess-Speicher mithilfe des in die Prozesse eingebetteten Schutz-Agenten vor Exploits schützen.
- **Liste der nicht vertrauenswürdigen Computer**. Sie können Remote-Computer, die versuchen, auf die Netzwerkfreigaben des Servers zuzugreifen, blockieren, wenn von ihnen schädliche Aktivitäten ausgehen.

Neuerungen

Kaspersky Security 10.1 für Windows Server ist eine Lösung zum Schutz von Unternehmensservern

und Datenspeichersystemen. Der verfügbare Schutzbereich (Server unter Windows, Datenspeichersysteme) und die Auswahl der Funktionskomponenten sind vom Typ der erworbenen Lizenz abhängig.

Kaspersky Security 10.1 für Windows Server verbessert die Funktionalität der vorherigen Programmversion und behält sie vollständig bei, während neue Schutzkomponenten hinzugefügt werden.

Die neue Version von neue Kaspersky Security 10.1 für Windows Server bringt Ihnen Folgendes:

- Eine neu hinzugefügte Komponente zum Schutz des Datenverkehrs (siehe Abschnitt "Schutz des Datenverkehrs" auf Seite 208): Sie können Ihren Server zusätzlich zu E-Mail-Bedrohungen jetzt auch vor Bedrohungen aus dem Internet schützen, die über HTTP oder HTTPS gesendet werden. Diese neue Komponente unterstützt folgende Szenarien:
  - Anti-Virus- und Anti-Phishing-Schutz des E-Mail-Datenverkehrs mithilfe von Kaspersky Security 10.1.0.622 Microsoft Outlook®-Add-in (im Weiteren "Kaspersky Security 10.1 Microsoft Outlook-Add-in")
  - Anti-Virus- und Anti-Phishing-Schutz des Web-Datenverkehrs
  - Link-Verifizierung mithilfe von Datenbanken für bösartige Webadressen
  - Link-Verifizierung mithilfe von Cloud-basierten Datenbanken für bösartige Webadressen
  - Web-Kontrolle mithilfe von Regeln für Links und Zertifikate
  - Kontrolle von Web-Ressourcen auf der Grundlage von Kategorien
  - Verifizierung von Webserver-Zertifikaten bei der Verbindung

  Der Datenverkehr wird mithilfe des ICAP-Dienstes in einer von drei Konfigurationen geschützt:
  - Externer Proxyserver: Analyse des von einem externen Proxyserver umgeleiteten Datenverkehrs (ohne Netzwerktreiber)
  - Redirector: Analyse des von in einer Terminalsitzung gestarteten Browsern umgeleiteten Datenverkehrs (ohne Netzwerktreiber) Das Programm verwendet einen internen System-Proxy.
  - Treiber-Interceptor: Der Datenverkehr wird mithilfe eines Netzwerktreibers in einer Terminalsitzung abgefangen.
- Neue Komponente "Anti-Cryptor für NetApp": Sie können jetzt einen Server mit installiertem Kaspersky Security 10.1 für Windows Server verwenden, um verbundene NetApp-Netzwerkspeicher vor Verschlüsselung zu schützen.

Siehe *Implementierungshandbuch für Netzwerkspeicher*.

- Eine neue Komponente zur Gerätekontrolle (siehe Abschnitt "Erstellen von Regeln aufgrund der Systemdaten der externen Geräte, die an die Netzwerkcomputer angeschlossen sind" auf Seite 255): Ab jetzt können Sie Listen von Regeln erstellen, die das Programm verwendet, um den Datenaustausch mit externen Geräten zur Datenspeicherung (über USB und MTP verbundene Massenspeichergeräte, CD/DVD-Laufwerke) zu erlauben oder zu blockieren.
- Eine neue Komponente zur Exploit-Prävention (siehe Abschnitt "Exploit-Prävention" auf Seite 199): Jetzt können Sie Einstellungen zum Schutz von Prozessen vor Exploits mithilfe von Verfahren zur Risikominderung festlegen.
- Eine neue Komponente zur Überwachung der Datei-Integrität (sieh Abschnitt "Überwachung der Datei-Integrität" auf Seite 273): Sie können jetzt Objekte festlegen, deren Integrität Sie überwachen möchten.

- Eine neue Komponente zur Protokollanalyse (siehe Abschnitt "Protokollanalyse" auf Seite 281): Sie können jetzt Regeln für die Protokollanalyse für Windows-Ereignisprotokolle festlegen und die Nutzung der heuristischen Analyse für Windows-Ereignisprotokolle anpassen.
- Neue Funktion zur Integration in externe SIEM-Systeme (s. Abschnitt "Anpassen der Einstellungen der SIEM-Integration" auf S. 173): Jetzt können Sie die Einstellungen für den Export von Programmberichten in Drittanbietersysteme für Ereignis-Management über das Protokoll syslog anpassen.
- Neue Möglichkeit zur Überwachung von USB-Verbindungen zu geschützten Geräten (s. Abschnitt "Über die Aufgabe zur Gerätekontrolle" auf S. 252): Sie können jetzt Einstellungen für Benachrichtigungen über USB-Verbindungen verschiedener Gerätetypen zu geschützten Computern anpassen.
- Sicherheits-Ereignisprotokoll (auf S. 173) integriert: Sie können jetzt in einem einzigen Protokoll alle Ereignisse nach Programmkomponente anzeigen, die darauf hindeuten, dass das geschützte System möglicherweise gefährdet ist.
- Eine neue Komponente zur Firewall-Verwaltung (siehe Abschnitt "Firewall-Verwaltung" auf Seite 260): Sie können über die grafische Benutzeroberfläche von Kaspersky Security 10.1 für Windows Server jetzt die Windows-Firewall-Regeln verwalten.
- Neue Möglichkeit zur Untersuchung von USB-Wechseldatenträgern (siehe Abschnitt "Untersuchung von Wechseldatenträgern" auf Seite 163): Sie können jetzt Massenspeichergeräte untersuchen, wenn diese an einen geschützten Computer angeschlossen sind.
- Neue Möglichkeit zur Aktivierung des Kennwortschutzes für die Programmverwaltung (siehe Abschnitt "Passwortgeschützter Zugang zu den Funktionen von Kaspersky Security 10.1 für Windows Server" auf Seite 106): Sie können jetzt auch Kaspersky Security 10.1 für Windows Server schützen und ein Kennwort verwenden, um den Zugang zu kritischen Abläufen zu beschränken.
- Neue Möglichkeit zum automatischen Erlauben des Starts von Programmen (siehe Abschnitt "Konfiguration der Kontrolle für Installationspakete" auf Seite 240) aus vertrauenswürdigen Installationspaketen: Sie können in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts jetzt Ausnahmen für Installationspakete hinzufügen, um den Prozess zum Erlauben des Starts von Dateien beim Installieren oder Aktualisieren von Software zu vereinfachen.
- Neue Funktion zur Virenuntersuchung und zum Virenschutz von Microsoft Windows Server 2016 Containern (s. Abschnitt "Über die Aufgabe zum Echtzeitschutz für Dateien" auf S. 179) wurde hinzugefügt.
- Die Blockierung nicht vertrauenswürdiger Geräte wurde vereinfacht (s. Abschnitt "Blockierung nicht vertrauenswürdiger Geräte.Liste der nicht vertrauenswürdigen Computer" auf S. 168): Die Komponenten "Schutz vor Verschlüsselung" und "Echtzeitschutz für Dateien" fügen jetzt unter Blockierte Geräte die ID-Nummern der angreifenden Computer hinzu. Sie können in den Einstellungen der Schutzaufgabe das automatische Füllen des Speichers für blockierte Geräte deaktivieren. Sie können auch alle nicht vertrauenswürdigen Computer in einer zentralen Liste in der Konsole des Administrationservers anzeigen.
- Optimierte Möglichkeit zur Erstellung einer Liste der Regeln für vertrauenswürdige Prozesse (siehe Abschnitt "Vertrauenswürdige Prozesse hinzufügen" auf Seite 160) für die vertrauenswürdige Zone: Sie können jetzt Prozesse auf Basis ihrer Prüfsumme, ihres Pfades oder einer Kombination aus Pfad und Prüfsumme ausschließen.
- Vereinfachter und erweiterter Mechanismus zum Befüllen von Listen der Regeln für die Kontrolle des Programmstarts (siehe Abschnitt "Über die Erstellung von Regeln für die Kontrolle des Programmstarts für das gesamte Netzwerk über Kaspersky Security Center" auf Seite 245): Neue Möglichkeit zur gleichzeitigen Verwendung von Regellisten, die auf lokalen Computern und in einer Richtlinie erstellt wurden, und neuer Mechanismus zur Erstellung von Regeln auf der Grundlage von Aufgabenereignissen in Kaspersky Security Center.

Lieferumfang

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

- Installationsassistent für Kaspersky Security 10.1 für Windows Server starten
- Installationsassistent der Konsole für Kaspersky Security 10.1 starten
- Starten Sie den Installationsassistent für das Verwaltungs-Plug-in für Kaspersky Security 10.1 für Windows Server, um das Programm über Kaspersky Security Center zu verwalten.
- Das Administratorhandbuch lesen
- Das Benutzerhandbuch lesen
- Das Implementierungshandbuch zum Schutz für Netzwerkspeicher (NAS) lesen
- Zur Seite von Kaspersky Security 10.1 für Windows Server https://www.kaspersky.de/small-to-medium-business-security/windows-server-security auf der Website von Kaspersky Lab wechseln
- Website des Technischen Supports (https://support.kaspersky.com/de) aufrufen
- Informationen über die aktuelle Version von Kaspersky Security 10.1 für Windows Server lesen

Der Ordner \client beinhaltet die Installationsdateien für die Konsole für Kaspersky Security 10.1 (Komponentenpaket "Administrations-Tools für die Konsole für Administration-Tools von Kaspersky Security 10.1 für Windows Server").

Der Ordner \server enthält Folgendes:

- Dateien für die Installation der Serverkomponenten von Kaspersky Security 10.1 für Windows Server auf einem Computer, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows läuft.
- Installationsdatei für das Verwaltungs-Plug-in für Kaspersky Security 10.1 für Windows Server 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 \setup enthält Dateien, die für den Start des Begrüßungsprogramms erforderlich sind.

Der Ordner \email_plugin enthält das Installationspaket für das Microsoft Outlook-Add-in für Kaspersky Security 10.1.

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

Tabelle 2. Dateien im Lieferumfang von Kaspersky Security 10.1 für Windows Server

Datei	Ziel
autorun.inf	Autostart-Datei des Installationsassistenten von Kaspersky Security 10.1 für Windows Server bei der Programminstallation von Wechseldatenträgern
ks4ws_admin_guide_de.pdf	Administratorhandbuch.
ks4ws_user_guide_de.pdf	Benutzerhandbuch
release_notes.txt	Datei enthält Ausgabedaten.
setup.exe	Startdatei des Begrüßungsprogramms (startet setup.hta).

Datei	Ziel
\client\ks4wstools_x86(x64).msi	Installationspaket des Dienstes Windows Installer; installiert die Konsole für Kaspersky Security 10.1 auf dem geschützten Server.
\client\setup.exe	Startdatei für den Assistenten zur Installation des Komponentensatzes "Administrationswerkzeuge" (dazu gehört die Konsole für Kaspersky Security 10.1); startet die Datei des Installationspakets ks4wstools.msi mit den im Assistenten gewählten Installationsparametern.
\server\bases.cab	Archiv der zum Zeitpunkt der Veröffentlichung des Programms aktuellen Antiviren-Datenbanken.
\server\setup.exe	Startdatei des Assistenten zur Installation von Kaspersky Security 10.1 für Windows Server auf dem geschützten Server; startet die Datei des Installationspakets ks4ws.msi mit den im Assistenten gewählten Installationsparametern.
\server\ks4ws_x86(x64).msi	Installationspaket des Dienstes Windows Installer; installiert Kaspersky Security 10.1 für Windows Server auf dem geschützten Server.
\server\ks4ws.kud	Datei im Format Kaspersky Unicode Definition mit einer Beschreibung des Installationspakets für die Remote-Installation von Kaspersky Security Center 10.1 für Windows Server über Kaspersky Security Center.
\server\klcfginst.exe	Installationsprogramm für das Verwaltungs-Plug-in für Kaspersky Security 10.1 für Windows Server über das Kaspersky Security Center. Installieren Sie das Verwaltungs-Plug-in auf jedem Server, auf dem die Verwaltungskonsole von Kaspersky Security Center installiert ist, wenn Sie Kaspersky Security 10.1 für Windows Server mit dieser Konsole verwalten möchten.
\server\license.txt	Text des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie.
\setup\setup.hta	Datei für den Start des Begrüßungsprogramms.
\email_plugin\ksmail_x86(x64).msi	Installationspaket des Dienstes Windows Installer; installiert das Microsoft Outlook-Add-in für Kaspersky Security 10.1 auf dem geschützten Server.

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

Hard- und Software-Voraussetzungen

Dieser Abschnitt enthält eine Liste der Hardware- und Softwarevoraussetzungen für Kaspersky Security 10.1 für Windows Server.

In diesem Kapitel

Anforderungen an den Server, auf dem Kaspersky Security 10.1 für Windows Server bereitgestellt wird

Vor der Installation von Kaspersky Security 10.1 für Windows Server müssen andere Virenschutzprogramme vom Server deinstalliert werden.

Sie können Kaspersky Security 10.1 für Windows Server installieren, ohne Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition oder Kaspersky Security 10 für Windows Server vorher zu deinstallieren.

Hardwarevoraussetzungen für den Server

Generelle Voraussetzungen:

- x86-64-kompatible Systeme in Single-Core- oder Multi-Core-Konfiguration
- Benötigter Speicherplatz:
  - für die Installation aller Programmkomponenten – 70 MB
  - für den Download und zum Speichern der Antiviren-Datenbanken des Programms – 2 GB (empfohlen)
  - zum Speichern von Objekten in Quarantäne und Backup – 400 MB (empfohlen)
  - zum Speichern von Protokollen – 1 GB (empfohlen).

Minimalkonfiguration:

- Prozessor – Single Core, 1,4 GHz
- Arbeitsspeicher – 1 GB
- Datenträger-Subsystem – 4 GB freier Speicherplatz

Empfohlene Konfiguration:

- Prozessor – Quad-Core, 2,4 GHz
- Arbeitsspeicher – 2 GB
- Datenträger-Subsystem – 4 GB freier Speicherplatz

Softwarevoraussetzungen für den Server

Sie können Kaspersky Security 10.1 für Windows Server auf einem Server installieren, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows läuft.

Für die Installation und Ausführung von Kaspersky Security 10.1 für Windows Server muss auf dem Server Microsoft Windows Installer 3.1 vorhanden sein.

Sie können Kaspersky Security 10.1 für Windows Server auf einem Server installieren, der unter einem der folgenden 32-Bit-Betriebssysteme von Microsoft Windows läuft.

- Windows Server® 2003 Standard / Enterprise / Datacenter SP2 oder höher
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 oder höher
- Windows Server 2008 Core / Standard / Enterprise / Datacenter SP1 oder höher

Sie können Kaspersky Security 10.1 für Windows Server auf einem Server installieren, der unter einem der folgenden 64-Bit-Betriebssysteme von Microsoft Windows läuft.

- Windows Server 2003 Standard / Enterprise / Datacenter SP2
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 oder höher
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 oder höher
- Windows Server 2008 R2 Core / Standard / Enterprise / Datacenter SP1 oder höher
- Windows Hyper-V® Server 2008 R2 SP1 oder höher
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint™ Server 2011
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server
- Windows Server 2012 Core / Standard / Datacenter
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Core / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server

- Windows Server 2016 Core / Standard / Datacenter
- Windows Storage Server 2016
- Windows Hyper-V Server 2016

Die folgenden Betriebssysteme werden nicht mehr von Microsoft Windows unterstützt: Windows Server 2003 Standard / Enterprise / Datacenter SP2, Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 32-Bit, 64-Bit. Auf Seiten von Kaspersky Lab kann es für den technischen Support von Servern mit diesen Betriebssystemen Einschränkungen geben.

Sie können Kaspersky Security 10.1 für Windows Server auf den folgenden Terminal-Servern installieren:

- Microsoft Remote Desktop Services auf der Grundlage des Windows Server 2008
- Microsoft Remote Desktop Services auf der Grundlage des Windows Server 2008 R2
- Microsoft Remote Desktop Services auf der Grundlage des Windows Server 2012
- Microsoft Remote Desktop Services auf der Grundlage des Windows Server 2012 R2
- Microsoft Remote Desktop Services auf der Grundlage des Windows Server 2016
- Citrix XenApp 6.0, 6.5, 7.0, 7.5 - 7.9, 7.15
- Citrix XenDesktop 7.0, 7.1, 7.5 - 7.9, 7.15

Anforderungen an den geschützten Netzwerkspeicher

Kaspersky Security 10.1 für Windows Server kann zum Schutz folgender Netzwerkspeicher eingesetzt werden:

- NetApp unter einem der folgenden Betriebssysteme:
  - Data ONTAP 7.x und Data ONTAP 8.x im Modus 7-mode;
  - Data ONTAP 8.2.1 oder höher im Modus cluster-mode.
- Dell™ EMC™ Celerra™ / VNX™ mit folgender Software:
  - Betriebssystem EMC DART 6.0.36 oder höher
  - Celerra Anti-Virus Agent (CAVA) 4.5.2.3 oder höher
- Dell EMC Isilon™ unter dem Betriebssystem OneFS™ 7.0 oder höher
- Hitachi NAS auf einer der folgenden Plattformen:
  - HNAS 4100
  - HNAS 4080
  - HNAS 4060
  - HNAS 4040
  - HNAS 3090
  - HNAS 3080

- IBM NAS Serie IBM System Storage N Serie
- Oracle® NAS Systems der Oracle ZFS Storage Appliance-Familie
- Dell NAS auf der Dell Compellent™ FS8600-Plattform

Anforderungen an den Computer, auf dem die Konsole für Kaspersky Security 10.1 installiert wird

Hardwarevoraussetzungen für den Computer

Empfohlener Arbeitsspeicher – 128 MB oder mehr.

Freier Platz auf der Festplatte – 30 MB.

Softwarevoraussetzungen für den Computer

Sie können die Konsole für Kaspersky Security 10.1 auf einem Computer installieren, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft Windows läuft.

Für die Installation und Ausführung der Konsole für Kaspersky Security 10.1 muss auf dem Computer Microsoft Windows Installer 3.1 vorhanden sein.

Sie können die Konsole für Kaspersky Security 10.1 auf einem Computer installieren, der unter einem der folgenden 32-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 oder höher
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 oder höher
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 oder höher
- Microsoft Windows XP Professional SP2 oder höher
- Microsoft Windows Vista® Editions
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Sie können die Konsole für Kaspersky Security 10.1 auf einem Computer installieren, der unter einem der folgenden 64-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 oder höher
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 oder höher
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 oder höher
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 oder höher
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint Server 2011
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server

- Windows Storage Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server;
- Windows Storage Server 2016
- Microsoft Windows XP Professional SP2 oder höher
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10

Funktionale Anforderungen und Einschränkungen

In diesem Abschnitt werden die zusätzlichen funktionalen Anforderungen und vorhandenen Einschränkungen der Komponenten von Kaspersky Security 10.1 für Windows Server beschrieben.

In diesem Abschnitt

Installation und Deinstallation

- Während der Programminstallation erscheint eine Warnung, wenn der Pfad zum Installationsordner von Kaspersky Security 10.1 für Windows Server mehr als 150 Zeichen enthält. Die Warnung hat keine Auswirkung auf den Installationsvorgang: Kaspersky Security 10.1 für Windows Server wird ordnungsgemäß installiert und ausgeführt.
- Um die Komponente "Unterstützung des SNMP-Protokolls" zu installieren, muss der SNMP-Dienst neu gestartet werden, falls dieser läuft.
- Für die Installation und Funktionsweise von Kaspersky Security 10.1 für Windows Server auf dem Gerät, das vom eingebetteten Betriebssystem verwaltet wird, muss die Komponente Filter Manager installiert sein.
- Die Installation der Administrations-Tools für Kaspersky Security 10.1 für Windows Server über die Gruppenrichtlinien von Microsoft Active Directory® ist nicht verfügbar.
- Bei der Installation des Programms auf Computern mit älteren Betriebssystemen, die keine regelmäßigen Updates beziehen können, müssen Sie folgende Stammzertifikate überprüfen: DigiCert Assured ID Root

CA, DigiCert_High_Assurance_EV_Root_CA, DigiCertAssuredIDRootCA. Das Fehlen der aufgezählten Zertifikate kann zu Fehlern in der Funktionsweise der Anwendung führen. Es wird empfohlen, diese Zertifikate mit einer beliebigen, Ihnen verfügbaren Methode zu installieren.

- Die Konsole für Kaspersky Security 10.1 kann nicht über das Startmenü deinstalliert werden. Sie können die Konsole für Kaspersky Security 10.1 über den Link im Fenster **Programme hinzufügen/löschen** deinstallieren.

Schutz des Datenverkehrs

- Die Komponente ist nur auf Servern mit dem Betriebssystem Microsoft Windows Server 2008 R2 oder höher ordnungsgemäß verfügbar.
- Der Datenverkehr kann nicht verifiziert werden, wenn die Webverbindungen mithilfe eines kryptografischen Tokens hergestellt werden.
- Es wird nicht empfohlen, VPN-Datenverkehr in den Schutzbereich einzuschließen (Port 1723).
- Die Verwendung von IP-Adressen im IPv6-Format ist nicht verfügbar.
- Die Anwendung stuft selbstsignierte Zertifikate als ungültig ein und blockiert entsprechende Verbindungen, wenn das Kontrollkästchen **Webservern mit falschem Zertifikat nicht vertrauen** in den Aufgabeneinstellungen aktiviert ist.
- Die Anwendung verarbeitet nur TCP-Pakete.
- Die Komponente "Schutz vor E-Mail-Bedrohungen" untersucht den ausgehenden E-Mail-Verkehr nicht.
- Es wird empfohlen, das Verwaltungs-Plug-in zu installieren, bevor die Komponente "Schutz des Datenverkehrs" bereitgestellt wird, da der Administrationsagent des Administrationsservers die Komponente "Schutz des Datenverkehrs" beim Herstellen einer Verbindung mit der Anwendung erkennt. Wenn die Komponente "Schutz des Datenverkehrs" installiert und die Aufgabe vor der Installation des Verwaltungs-Plug-ins gestartet wurde, starten Sie die Aufgabe "Schutz des Datenverkehrs" neu.
- Die Komponente "Schutz des Datenverkehrs" funktioniert nicht mit Yandex.Disk und Dropbox.
- VPN-Einschränkungen: Es können Probleme bei der Verwendung der Microsoft VPN-Verbindungsprotokolle auftreten.
- Wenn die Installation über KSC im Modus "Treiber-Interceptor" vorgenommen wird, blockiert der Schutz des Datenverkehrs die Verbindung von der MMC-Konsole zum Server von Kaspersky Security Center, da dieser Verbindungstyp ein nicht vertrauenswürdiges Zertifikat nutzt.
- Die Komponente blockiert die Verbindung zu Websites, die alte Technologien zur Erstellung von Stammzertifikaten (z. B. sha1-Zertifikat) verwenden.
- Der Wert **Objekte nicht scannen, wenn größer als (MB)** darf 100 MB nicht überschreiten. Wenn ein großer Wert angegeben wird und die Internetverbindung langsam ist, können beim Empfang großer Dateien Probleme auftreten. Der empfohlene Wert ist 20 MB.
- Das Programm erkennt HTTPS-Verbindungen als gefährlich und blockiert sie, wenn die folgenden Voraussetzungen erfüllt sind:
  - Die Aufgabe wird im Modus **Treiber-Interceptor** ausgeführt.
  - Datenverkehr wird von externen Geräten umgeleitet.
  - Die Geräte, von denen der Datenverkehr umgeleitet wird, ist durch Kaspersky Security 10.1

für Windows Server geschützt, und die vorkonfigurierte Aufgabe "Schutz des Datenverkehrs" wurde mindestens einmal ausgeführt.

Wir empfehlen, den von externen Computern umgeleiteten Datenverkehr nicht im Modus **Redirector** zu prüfen: Neben den zuvor erwähnten Fehlalarmen kann eine solche Konfiguration auch zu hoher Serverauslastung führen und die Leistung der Anwendung reduzieren.

Überwachung der Datei-Integrität

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

Die folgenden Ordner/Dateien werden aus dem Überwachungsbereich ausgeschlossen:

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

Die Anwendung schließt Verzeichnisse der obersten Ebene aus.

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

Firewall-Verwaltung

- Die Verwendung von IP-Adressen im IPv6-Format ist nicht verfügbar, wenn der festgelegte angewendete Regelbereich aus einer einzigen Adresse besteht.
- Die vorkonfigurierten Richtlinienregeln der Firewall ermöglichen die Ausführung grundlegender Interaktionsszenarien zwischen lokalen Computern und dem Administrationsserver. Um die Funktionen von Kaspersky Security Center vollständig zu verwenden, müssen manuell Regeln für Ports eingerichtet werden. Informationen über Portnummern, Protokolle und deren Funktionen finden Sie in der Wissensdatenbank von Kaspersky Security Center (Artikel-ID: 9297).
- Die Anwendung kontrolliert während der minutenweisen Abfragen durch die Aufgabe "Firewall-Verwaltung" keine Änderungen in den Windows Firewall-Regeln und Regelgruppen, wenn diese Regeln während der Programminstallation nicht zur Konfiguration der Aufgabe hinzugefügt wurden. Um den Status zu aktualisieren und solche Regeln einzuschließen, muss die Aufgabe "Firewall-Verwaltung" neu gestartet werden.
- Für die Betriebssystemreihe Microsoft Windows Server 2008 und höher gilt: Der Dienst Windows Firewall muss gestartet sein (standardmäßig gestartet), bevor die Komponente Firewall-Verwaltung installiert wird.
- Wenn die Aufgabe zur Firewall-Verwaltung gestartet wird, werden die folgenden Regeltypen automatisch aus den Firewall-Einstellungen des Betriebssystems entfernt:
  - Verbotsregeln;
  - Regeln zur Überwachung ausgehenden Datenverkehrs.

Andere Einschränkungen

Untersuchung auf Befehl, Echtzeitschutz für Dateien:

- Die Untersuchung von MTP-Geräten bei ihrem Anschluss ist nicht verfügbar.
- Die Untersuchung von Archivobjekten ist ohne die Untersuchung von SFX-Archiven nicht verfügbar: Wenn die Untersuchung von Archiven in den Schutzeinstellungen von Kaspersky Security 10.1 für Windows Server aktiviert ist, untersucht die Anwendung automatisch Objekte in Archiven und SFX-Archiven. Die Untersuchung von SFX-Archiven ist auch ohne die Untersuchung von Archiven verfügbar.

Computer-Kontrolle und Diagnose:

- Der Schutzbereich der Aufgabe "Gerätekontrolle" schließt MTP-Geräte ein, wenn der geschützte Computer unter dem Betriebssystem Microsoft Windows Server 2008 R2 oder höher läuft.
- Die Aufgabe "Protokollanalyse" erkennt potenzielle Muster eines Kerberos-Angriffs (MS14-068) nur auf Computern unter Windows Server 2008 oder höher, die als Domain-Controller fungieren und alle Updates installiert haben.

Lizenzverwaltung:

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

Updates:

- Nach der Installation von Updates für kritische Module von Kaspersky Security 10.1 für Windows Server wird das Symbol der Anwendung standardmäßig ausgeblendet.
- KLRAMDISK wird auf Computern unter Windows XP oder Windows 2003 nicht unterstützt.

Oberfläche:

- Wenn Sie die Filterfunktion in der Konsole für Kaspersky Security 10.1 in der Quarantäne, dem Backup, dem Systemaudit-Bericht oder den Berichten über Aufgabenausführung verwenden, berücksichtigen Sie die Groß-/Kleinschreibung.
- Bei der Konfiguration des Schutz- oder Untersuchungsbereichs in der Konsole für Kaspersky Security 10.1 können Sie nur eine einzige Maske verwenden und sie nur am Pfadende platzieren. Beispiele für die korrekte Verwendung der Maske: "C:\Temp\Temp*" oder "C:\Temp\Temp???.doc" oder "C:\Temp\Temp*.doc". Diese Einschränkung betrifft nicht die Konfiguration der vertrauenswürdigen Zone.

Sicherheit:

- Wenn im Betriebssystem die Benutzerkontensteuerung (User Account Control) aktiviert ist, muss das Benutzerkonto zur Gruppe KAVWSEE Administrators gehören, um die Konsole für Kaspersky Security 10.1 mit einem Doppelklick auf das Programmsymbol im Infobereich der Taskleiste öffnen zu können. Andernfalls wird das Fenster "Über das Programm" geöffnet.
- Die Deinstallation über das Microsoft Windows-Fenster "Programme und Features" ist nicht verfügbar, wenn die Benutzerkontensteuerung aktiviert ist.

Integration in Kaspersky Security Center:

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

Exploit-Prävention:

- Die Exploit-Prävention ist nicht verfügbar, wenn die Bibliotheken apphelp.dll in der aktuellen Umgebungskonfiguration nicht geladen sind.
- Die Komponente "Exploit-Prävention" ist auf Computern mit dem Betriebssystem Microsoft Windows 10 nicht mit dem Microsoft-Dienstprogramm EMET kompatibel: Kaspersky Security 10.1 für Windows Server blockiert EMET, wenn die Komponente "Exploit-Prävention" auf einem Computer installiert wird, auf dem EMET bereits installiert ist.

Anti-Cryptor für NetApp:

- Der Schutz vor Verschlüsselung ist für Netzwerkspeicher mit neuen Betriebssystemen (ONTAP 9 und höher) nicht verfügbar, wenn für diese Server FlexGroup-Container verwendet werden.
- Die Funktion zum Erkennen von Dateibedrohungen auf NetApp-Netzwerkspeichern in 7-Mode ist eingeschränkt.
- Anti-Cryptor für NetApp ist nur im Cluster-Modus verfügbar.
- Ein Server kann nur eine einzige Netzwerkschnittstelle und nur eine IPv4-Adresse verwenden.

Blockierte Geräte: wird kontinuierlich ausgeführt, wenn die Komponenten "Schutz vor Verschlüsselung" oder

"Echtzeitschutz für Dateien" aktiviert sind.

Schutz von per ICAP-Protokoll verbundenen Netzwerkspeichern: Die Verwaltung der Inhalte des geschützten Speichers ist von den Einstellungen des Speichers abhängig. Zum Beispiel können gefundene infizierte Objekte nicht gelöscht werden, wenn der Speicher diese Aktion nicht erlaubt. Speicher von HP 3Par funktioniert nur im Modus "Zugriff verweigern". Die vertrauenswürdige Zone kann nicht verwendet werden.

Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern: Für den Cluster-Modus ist Active Directory erforderlich.

Verwendung von KSN: Für Windows Vista und älter unterstützt diese Komponente keine Statistik für Web-Anti-Virus und Mail-Anti-Virus.

Programm installieren und deinstallieren

Dieser Abschnitt enthält schrittweise Anleitungen zur Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server.

In diesem Kapitel

Programmkomponenten von Kaspersky Security 10.1 für Windows Server und ihre Codes für den Dienst Windows Installer

Standardmäßig werden mithilfe der Dateien \server\ks4ws_x86(x64).msi alle Programmkomponenten von Kaspersky Security 10.1 für Windows Server installiert. Sie können die Installation dieser Komponente bei einer benutzerdefinierten Installation des Programms aktivieren.

Durch die Dateien \client\ks4wstools_x86(x64).msi werden alle Programmkomponenten des Pakets "Administrations-Tools" installiert.

Die folgenden Abschnitte enthalten die Codes der Programmkomponenten von Kaspersky Security 10.1 für Windows Server für den Dienst Windows Installer. Sie können diese Codes verwenden, um die Liste der zu installierenden Komponenten festzulegen, wenn Kaspersky Security 10.1 für Windows Server aus der Befehlszeile installiert wird.

In diesem Abschnitt

Programmkomponenten von Kaspersky Security 10.1 für Windows Server

Die folgende Tabelle enthält die Codes und eine Beschreibung der Programmkomponenten von Kaspersky Security 10.1 für Windows Server.

Tabelle 3. Beschreibung der Programmkomponenten von Kaspersky Security 10.1 für Windows Server

Komponente	Code	Ausgeführte Funktion
Hauptfunktionen	core	Diese Komponente beinhaltet ein Paket von Basisfunktionen des Programms und gewährleistet deren Ausführung.
Kontrolle des Programmstarts	AppCtrl	Diese Komponente überwacht die Versuche von Benutzern, Programme zu starten, und erlaubt oder verbietet den Programmstart in Übereinstimmung mit den festgelegten Regeln für die Kontrolle des Programmstarts. Die Komponente wird in der Aufgabe "Kontrolle des Programmstarts" realisiert.
Gerätekontrolle	DevCtrl	Diese Komponente überwacht die Verbindungsversuche von USB-Massenspeichergeräten auf einem geschützten Server und verbietet oder erlaubt deren Verwendung entsprechend den festgelegten Regeln zur Gerätekontrolle. Die Komponente wird in der Aufgabe Gerätekontrolle realisiert.
Schutz des Datenverkehrs	WebGW	Diese Komponente verarbeitet den Web-Datenverkehr (einschließlich des Datenverkehrs, der über die Mail-Dienste eingeht) und fängt Objekte ab, die über den Web-Datenverkehr übertragen werden, und untersucht sie, um bekannte Computer- und andere Bedrohungen auf dem geschützten Server zu erkennen.
Antiviren-Schutz	AVProtection	Diese Komponente gewährleistet den Antiviren-Schutz und beinhaltet die folgenden Komponenten: • Untersuchung auf Befehl • Echtzeitschutz für Dateien

Komponente	Code	Ausgeführte Funktion
Untersuchung auf Befehl	Ods	Diese Komponente installiert die Systemdateien von Kaspersky Security 10.1 für Windows Server und Dateien, die die Aufgaben zur Untersuchung auf Befehl (Untersuchung von Objekten des geschützten Servers) umsetzen. Wenn Sie beim Installieren von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile andere Komponenten von Kaspersky Security 10.1 für Windows Server angeben, ohne die Core-Komponente zu nennen, wird die Core-Komponente automatisch installiert.
Echtzeitschutz für Dateien	Oas	Diese Komponente führt auf dem geschützten Server eine Untersuchung von Dateien auf Viren durch, sobald auf diese Dateien zugegriffen wird. Sie setzt die Aufgabe Echtzeitschutz für Dateien um.
Verwendung von Kaspersky Security Network	KSN	Diese Komponente gewährleistet den Schutz auf Basis der Cloud-Technologien von Kaspersky Lab. Sie setzt die Aufgabe Verwendung von KSN um (Versand von Anfragen und Erhalt von Einstufungen von den Diensten von Kaspersky Security Network).
Überwachung der Datei-Integrität	Fim	Diese Komponente ermöglicht es, Dateioperationen im festgelegten Überwachungsbereich zu protokollieren. Die Komponente wird in der Aufgabe Überwachung der Datei-Integrität umgesetzt.
Exploit-Prävention	AntiExploit	Diese Komponente ermöglicht die Verwaltung der Einstellungen zum Schutz des Prozess-Speichers im Speicher des geschützten Servers.
Firewall-Verwaltung	Firewall	Diese Komponente ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Security 10.1 für Windows Server zu verwalten. Die Komponente wird in der Aufgabe Firewall-Verwaltung umgesetzt.
Modul für die Integration in den Administrationsagenten von Kaspersky Security Center	AKIntegration	Koordination der Verbindung zwischen dem Server von Kaspersky Security 10.1 für Windows Server und dem Administrationsagenten von Kaspersky Security Center. Sie können diese Komponente auf dem geschützten Server installieren, wenn Sie vorhaben, das Programm über Kaspersky Security Center zu verwalten.

Komponente	Code	Ausgeführte Funktion
Protokollanalyse	LogInspector	Diese Komponente führt eine Integritätsprüfung des geschützten Mittwochs auf Grundlage der Ergebnisse der Protokollanalyse von Windows-Ereignissen aus.
Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern	RPCProt	Diese Komponente schützt Netzwerkspeicher, die per RPC-Protokoll verbunden werden (wie z. B. NetApp-Netzwerkspeicher), vor Viren und anderen Bedrohungen für die Computersicherheit, die bei der Übertragung von Dateien eindringen können.
Schutz von per ICAP-Protokoll verbundenen Netzwerkspeichern	ICAPProt	Diese Komponente schützt Netzwerkspeicher, die per ICAP-Protokoll verbunden werden (wie z. B. EMC Isilon), vor Viren und anderen Bedrohungen für die Sicherheit, die bei der Übertragung von Dateien eindringen können.
Anti-Cryptor für NetApp	AntiCryptorNAS	Diese Komponente bietet Schutz vor Verschlüsselung für die Ordner der Netzwerkspeicher. Bei Erkennen einer schädlichen Verschlüsselung blockiert Kaspersky Security 10.1 für Windows Server den Zugriff auf die Ordner der geschützten Netzwerkspeicher.
Satz von Leistungsindikatoren der Anwendung "Systemmonitor"	PerfMonCounters	Diese Komponente installiert Leistungsindikatoren des Programms Systemmonitor. Die Leistungsindikatoren messen die Leistungsfähigkeit von Kaspersky Security 10.1 für Windows Server und finden mögliche Engpässe bei gleichzeitiger Ausführung von Kaspersky Security 10.1 für Windows Server und anderen Programme.
SNMP-Indikator und Traps	SnmpSupport	Die Komponente veröffentlicht die Indikatoren und Traps für Kaspersky Security 10.1 für Windows Server über den Dienst Simple Network Management Protocol (SNMP) von Microsoft Windows. Sie können diese Komponente nur auf dem geschützten Server installieren, wenn der Service Microsoft SNMP auf diesem Computer installiert ist.
Symbol für Kaspersky Security 10.1 für Windows Server im Infobereich	TrayApp	Die Komponente zeigt das Symbol für Kaspersky Security 10.1 für Windows Server im Infobereich der Taskleiste des geschützten Servers an. Das Symbol für Kaspersky Security 10.1 für Windows Server zeigt den Status des Schutzes auf dem Computer an und erlaubt, die Konsole für Kaspersky Security 10.1 in MMC (falls installiert) und das Fenster "Über das Programm" zu öffnen.

Komponente	Code	Ausgeführte Funktion
Befehlszeilen-Utility	Shell	Verwaltung von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile des geschützten Servers.

Programmkomponenten des Pakets „Administrations-Tools"

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

Tabelle 4. Beschreibung der Programmkomponenten des Satzes Administrationswerkzeuge

Komponente	Code	Funktionen der Komponente
Snap-ins von Kaspersky Security 10.1 für Windows Server	MmcSnapin	Die Komponente installiert das Microsoft Management Console Snap-in für die Verwaltung über die Konsole für Kaspersky Security 10.1. Wenn Sie beim Installieren eines Satzes der Administrationswerkzeuge aus der Befehlszeile andere Satz-Komponenten angeben, ohne die MmcSnapin-Komponente zu nennen, wird die MmcSnapin-Komponente automatisch installiert.
Help	Help	chm-Hilfedatei; wird im Ordner mit den Dateien der Administrations-Tools für Kaspersky Security 10.1 für Windows Server gespeichert. Sie können die Hilfedatei aus dem Menü **Start** oder in einem geöffneten Fenster der Konsole für Kaspersky Security 10.1 mithilfe der Taste **F1** öffnen.
Dokumentation	Docs	Kaspersky Security 10.1 für Windows Server speichert das Implementierungshandbuch für den Schutz für Netzwerkspeicher, das Administratorhandbuch und das Benutzerhandbuch im PDF-Format auf dem geschützten Server. Sie können alle Handbücher aus dem Menü **Start** öffnen.

Systemänderungen nach der Installation von Kaspersky Security 10.1 für Windows Server

Bei der Installation von Kaspersky Security 10.1 für Windows Server und der Konsole für Kaspersky Security 10.1 (aus dem Paket "Administrations-Tools") nimmt der Dienst von Windows Installer auf dem Server folgende Veränderung vor:

- Auf dem geschützten Server sowie auf dem Server, auf dem die Konsole für Kaspersky Security 10.1 installiert ist, werden Ordner für Kaspersky Security 10.1 für Windows Server erstellt.

- Die Dienste von Kaspersky Security 10.1 für Windows Server werden registriert.
- Eine Benutzergruppe für Kaspersky Security 10.1 für Windows Server wird erstellt.
- In der Systemregistrierung werden die Schlüssel für Kaspersky Security 10.1 für Windows Server registriert.

Diese Veränderungen sind in der Tabelle unten beschrieben.

Ordner für Kaspersky Security 10.1 für Windows Server

Tabelle 5. Ordner für Kaspersky Security 10.1 für Windows Server auf einem geschützten Server

Ordner	Dateien für Kaspersky Security 10.1 für Windows Server
Ordner %Kaspersky Security 10.1 für Windows Server%; standardmäßig: In der 32-Bit-Version von Microsoft Windows – %Programme%\Kaspersky Lab\Kaspersky Security 10.1 für Windows Server\ In der 64-Bit-Version von Microsoft Windows – %Programme (x86)%\Kaspersky Security 10.1 für Windows Server\	Ausführbare Dateien für Kaspersky Security 10.1 für Windows Server (Zielordner wird während der Installation angegeben).
Ordner %Kaspersky Security 10.1 für Windows Server%\mibs	Dateien für die Management Information Base (MIB). Diese Dateien enthalten eine Beschreibung der Indikatoren und Traps, die von Kaspersky Security 10.1 für Windows Server mit dem SNMP-Protokoll veröffentlicht werden.
Ordner %Kaspersky Security 10.1 für Windows Server%\x64	64-Bit-Version der ausführbaren Dateien von Kaspersky Security 10.1 für Windows Server (der Ordner wird nur erstellt, wenn Kaspersky Security 10.1 für Windows Server unter einer 64-Bit-Version von Microsoft Windows installiert wird.)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Security for Windows Server\10.1\Dskm\	Dienstdateien für Kaspersky Security 10.1 für Windows Server
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\	Dateien mit Einstellungen für die Update-Quellen.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Update\Distribution\	Datenbanken-Updates und Updates der Programm-Module, die mithilfe der Aufgabe Update-Verteilung empfangen wurden (Der Ordner wird erstellt, wenn zum ersten Mal Updates mithilfe der Aufgabe Update-Verteilung empfangen werden).

Ordner	Dateien für Kaspersky Security 10.1 für Windows Server
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Reports\	Berichte über Aufgabenausführung und Systemaudit-Bericht.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Current\	Satz der Datenbanken, die im Moment verwendet werden.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Backup\	Backup-Kopie der Datenbanken; wird bei jedem Datenbanken-Update überschrieben
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Bases\Temp\	Temporäre Dateien, die beim Ausführen der Update-Aufgabe angelegt werden.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Quarantine\	Objekte in der Quarantäne (standardmäßiger Ordner).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security for Windows Server\10.1\Backup\	Objekte im Backup (standardmäßiger Ordner).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security für Windows Server\10.1\Restored\	Objekte, die aus Backup oder Quarantäne wiederhergestellt wurden (standardmäßiger Ordner für die Wiederherstellung von Objekten).

Tabelle 6. Ordner, die bei der Installation der Konsole für Kaspersky Security 10.1 erstellt werden

Ordner	Dateien für Kaspersky Security 10.1 für Windows Server
Ordner %Kaspersky Security 10.1 für Windows Server%; standardmäßig: • In der 32-Bit-Version von Microsoft Windows – %Programme%\Kaspersky Lab\Kaspersky Security 10.1 für Windows Server\ In der 64-Bit-Version von Microsoft Windows – %Programme(x86)%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server\	Dateien für "Administrations-Tools" (Zielordner, der bei der Installation der Konsole für Kaspersky Security 10.1 angegeben wird)

Dienste von Kaspersky Security 10.1 für Windows Server

Die Dienste von Kaspersky Security 10.1 für Windows Server werden unter dem Systemkonto (SYSTEM) gestartet.

Tabelle 7. Dienste von Kaspersky Security 10.1 für Windows Server

Dienst	Ziel

Dienst von Kaspersky Security Service (KAVFS)	Wichtiger Dienst von Kaspersky Security 10.1 für Windows Server, der Aufgaben und Workflows in Kaspersky Security 10.1 für Windows Server verwaltet
Dienst von Kaspersky Security Management Service (KAVFSGT)	Der Dienst ist für die Programmverwaltung von Kaspersky Security 10.1 für Windows Server mithilfe der Konsole für Kaspersky Security 10.1 vorgesehen.
Kaspersky Security Broker Service (KAVFSWH)	Dienst, der die Vermittlerrolle bei der Übermittlung von Schutzeinstellungen an externe Schutzagenten sowie beim Abruf von Daten über sicherheitsrelevante Ereignisse von externen Schutzagenten übernimmt.
Kaspersky Security Script Checker (KAVFSSCS)	Der Dienst wird zusammen mit der Aufgabe zur Skript-Untersuchung gestartet und ermöglicht die Kontrolle der Ausführung von Skripten, die mithilfe der Microsoft Windows Script Technologies erstellt wurden.

Gruppen von Kaspersky Security 10.1 für Windows Server

Tabelle 8. Gruppen von Kaspersky Security 10.1 für Windows Server

Gruppe	Ziel
KAVWSEE Administrators	Die Benutzer aus dieser Gruppe besitzen auf dem geschützten Server Vollzugriff auf Kaspersky Security Management Service sowie Zugriff auf alle Funktionen von Kaspersky Security 10.1 für Windows Server

Schlüssel der Systemregistrierung

Tabelle 9. Schlüssel der Systemregistrierung

Schlüssel	Ziel
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Eigenschaften des Dienstes für Kaspersky Security 10.1 für Windows Server
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Einstellungen des Ereignisprotokolls für Kaspersky Security 10.1 für Windows Server (Kaspersky Event Log).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Eigenschaften des Dienstes zur Verwaltung von Kaspersky Security 10.1 für Windows Server

In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]	Parameter für die Leistungsindikatoren
In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\SnmpAgent] In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\SnmpAgent]	Parameter für die Komponente Unterstützung des SNMP-Protokolls.
In der 32-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\WSEE\10.1\CrashDump\ In der 64-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.1\CrashDump\	Einstellungen für Einträge in die Dump-Datei.
In der 32-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\Software\KasperskyLab\WSEE\10.1\Trace\ In der 64-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\WSEE\10.1\Trace\	Parameter des Protokolls zur Ablaufverfolgung.
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\WSEE\10.1\Environment]	Konfiguration der Aufgaben und Funktionen der Anwendung.

Prozesse von Kaspersky Security 10.1 für Windows Server

Kaspersky Security 10.1 für Windows Server startet die in der folgenden Tabelle beschriebenen Prozesse.

Tabelle 10. Prozesse von Kaspersky Security 10.1 für Windows Server

Dateiname	Ziel
kavfswp.exe	Workflow von Kaspersky Security 10.1 für Windows Server
kavtray.exe	Prozess für das Infobereich-Symbol von Kaspersky Security 10.1 für Windows Server
kavshell.exe	Prozess von Befehlszeilen-Utility
kavfsrcn.exe	Prozess zur Fernverwaltung von Kaspersky Security 10.1 für Windows Server
kavfs.exe	Dienstprozess von Kaspersky Security Service
kavfsgt.exe	Prozess des Verwaltungsdienstes Kaspersky Security Management Service

Dateiname	Ziel
kavfswh.exe	Prozess des Dienstes zur Kontrolle externer Prozesse von Kaspersky Security Service Broker Host
kavfsscs.exe	Kaspersky Security Script Checker Dienst

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

In den folgenden Tabellen werden die Einstellungen für die Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server und deren Standardwerte beschrieben. Außerdem werden die Schlüssel für die Änderung der Einstellungswerte und die mögliche Werte dieser Schlüssel erläutert. Sie können diese Schlüssel gemeinsam mit den Standardschlüsseln des Befehls msiexec des Dienstes Windows Installer verwenden, wenn Kaspersky Security 10.1 für Windows Server aus der Befehlszeile installiert wird.

Tabelle 11. Installationseinstellungen und deren Schlüssel in Windows Installer

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren	Bedingungen des Endbenutzer-Lizenzvertrags ablehnen	EULA=<Wert> 0 – Sie lehnen die Bedingungen des Endbenutzer-Lizenzvertrags ab. 1 – Sie akzeptieren die Bedingungen des Endbenutzer-Lizenzvertrags.	Um Kaspersky Security 10.1 für Windows Server zu installieren, müssen Sie die Bedingungen des Endbenutzer-Lizenzvertrags akzeptieren.
Annahme der Datenschutzrichtlinie	Ablehnung der Datenschutzrichtlinie	PRIVACYPOLICY=<value> 0 – Sie lehnen die Bedingungen der Datenschutzrichtlinie ab. 1 – Sie akzeptieren die Bedingungen der Datenschutzrichtlinie.	Um Kaspersky Security 10.1 für Windows Server zu installieren, müssen Sie die Bedingungen der Datenschutzrichtlinie akzeptieren.

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Zielordner	Kaspersky Security 10.1 für Windows Server: %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server Administrations-Tools: %ProgramFiles%\Kaspersky Lab\Kaspersky Security 10.1 for Windows Server Admins Tools In der 64-Bit-Version von Microsoft Windows: %ProgramFiles(x86)%	INSTALLDIR=<Vollständiger Pfad zum Ordner>	Ordner, in dem die Dateien für Kaspersky Security 10.1 für Windows Server bei der Installation gespeichert werden. Sie können einen anderen Ordner angeben.
Echtzeitschutz für Dateien beim Start von Kaspersky Security 10.1 für Windows Server starten (**Echtzeitschutz nach der Installation des Programms aktivieren**)	Starten	RUNRTP=<Wert> 1 – starten 0 – nicht starten	Aktivieren Sie diese Einstellung, damit der Echtzeitschutz für Dateien und die Skript-Untersuchung beim Start von Kaspersky Security 10.1 für Windows Server gestartet werden (empfohlen).
Untersuchungsausnahmen, die von der Firma Microsoft empfohlen werden (**Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**)	Ausschließen	ADDMSEXCLUSION=<Wert> 1 – ausschließen 0 – nicht ausschließen	In der Aufgabe Echtzeitschutz für Dateien werden jene Objekte auf dem Server vom Schutzbereich ausgenommen, deren Ausnahme die Firma Microsoft empfiehlt. Einige Anwendungen auf dem Server laufen möglicherweise nicht stabil, wenn Antiviren-Anwendungen Dateien abfangen oder ändern, auf die diese Programme zugreifen. Zu solchen Programmen zählt Microsoft beispielsweise einige Anwendungen wie Domain-Controller.

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Untersuchungsausnahmen, die von Kaspersky Lab empfohlen werden (**Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen**)	Ausschließen	ADDKLEXCLUSION=<Wert> 1 – ausschließen 0 – nicht ausschließen	In der Aufgabe zum Echtzeitschutz für Dateien werden Objekte auf dem Server in Übereinstimmung mit der Empfehlung von Kaspersky Lab aus dem Schutzbereich ausgeschlossen.
Remote-Verbindung zur Konsole für Kaspersky Security 10.1 erlauben	Verbieten	ALLOWREMOTECON = <Wert> 1 – erlauben 0 – verbieten	Standardmäßig wird die Remote-Verbindung zu einer auf dem geschützten Server installierten Konsole für Kaspersky Security 10.1 nicht erlaubt. Während der Installation können Sie die Verbindung erlauben. Kaspersky Security 10.1 für Windows Server erstellt Erlaubnisregeln für den Prozess kavfsgt.exe gemäß TCP-Protokoll für alle Ports.

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Pfad der Schlüsseldatei (**Schlüssel**)	Ordner im Lieferumfang \server	LICENSEKEYPATH=<Pfad der Schlüsseldatei>	Das Installationsprogramm sucht standardmäßig in dem im Lieferumfang enthaltenen Ordner \server nach einer Datei mit der Erweiterung .key. Wenn der Ordner \server mehrere Schlüsseldateien enthält, wählt das Installationsprogramm die Schlüsseldatei aus, deren Gültigkeitsdauer zuletzt abläuft. Sie können die Schlüsseldatei zuvor im Ordner \server\ speichern oder mit dem Installationsparameter **Schlüssel hinzufügen** einen anderen Pfad für die Schlüsseldatei angeben. Sie können den Schlüssel während der Installation von Kaspersky Security 10.1 für Windows Server hinzufügen, mithilfe der von Ihnen gewählten Administrationswerkzeuge, zum Beispiel mit der Konsole für Kaspersky Security 10.1. Wenn Sie während der Programminstallation keinen Programmschlüssel hinzufügen, funktioniert Kaspersky Security 10.1 für Windows Server nach Abschluss der Installation nicht.

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Pfad der Konfigurationsdatei	Nicht festgelegt	CONFIGPATH=<Pfad der Schlüsseldatei>	Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server nicht aus der Konfigurationsdatei importiert. Nach dem Import der Parameter müssen alle Kennwörter manuell eingegeben werden. Wenn Sie die Konfigurationsdatei nicht angeben, beginnt das Programm nach der Installation mit den Standardparametern zu arbeiten.

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Netzwerkverbindungen für die Konsole erlauben	Deaktiviert	ADDWFEXCLUSION=<Wert> **1** – erlauben **0** – verbieten	Verwenden Sie diese Option, um Kaspersky Security 10.1 für Windows Server auf einem anderen Server zu installieren. Mit Hilfe der Konsole für Kaspersky Security 10.1, die auf einem anderen Server installiert ist, können Sie den Computerschutz ferngesteuert verwalten. Auf dem Computer wird in der Firewall von Microsoft Windows der TCP-Port 135 geöffnet, Netzwerkverbindungen für die ausführbare Datei kavfsrcn.exe werden erlaubt (Prozess zur Fernverwaltung von Kaspersky Security 10.1 für Windows Server) und der Zugriff auf DCOM-Programme wird zugelassen. Wenn der Server unter dem Betriebssystem Windows Server 2008 läuft, fügen Sie nach Abschluss der Installation die Benutzer, die das Programm ferngesteuert verwalten werden, zur Gruppe KAVWSEE Administrators auf dem Server hinzu und erlauben Sie darauf Netzwerkverbindungen für den Dienst Kaspersky Security Management Service (Datei kavfsgt.exe). Mehr zur weiteren Konfiguration bei Installation der Konsole für Kaspersky Security 10.1 auf einem anderen Server finden Sie im Abschnitt "Erweiterte Einstellungen nach der Installation der Konsole für Kaspersky Security 10.1 auf einem anderen Computer" auf Seite 58.

Einstellung	Standardwert	Befehlszeilenoptionen von Windows Installer und deren mögliche Werte	Beschreibung
Untersuchung auf nicht kompatible Software deaktivieren	Die Untersuchung wird ausgeführt	SKIPINCOMPATIBLESW = <Wert> 0 – Untersuchung auf nicht kompatible Software wird ausgeführt 1 – Untersuchung auf nicht kompatible Software wird nicht ausgeführt	Verwenden Sie diese Einstellung, um die Untersuchung auf nicht kompatible Software bei der Installation des Programms auf dem Gerät im Hintergrundmodus zu aktivieren bzw. deaktivieren. Unabhängig vom Wert dieser Einstellung warnt das Programm bei der Installation von Kaspersky Security 10.1 für Windows Server immer vor anderen auf diesem Gerät installierten Programmversionen.

Tabelle 12. Deinstallationsparameter und deren Schlüssel in Windows Installer

Einstellung	Standardwert	Beschreibung, Schlüssel von Windows Installer und deren Werte
Wiederherstellung von Objekten aus der Quarantäne	Löschen	RESTOREQTN =<Wert> **0** – Quarantäne-Inhalt löschen **1** – Inhalt der Quarantäne in dem Ordner wiederherstellen, der mit der Einstellung RESTOREPATH vorgegeben ist.
Wiederherstellen des Backup-Inhalts	Löschen	RESTOREBCK =<Wert> **0** – Backup-Inhalt löschen **1** – Inhalt des Backups in dem Ordner wiederherstellen, der mit der Einstellung RESTOREPATH vorgegeben ist.
Eingabe des aktuellen Kennworts für die Bestätigung des Löschvorgangs (wenn die Verwendung eines Kennworts aktiv ist)	Nicht festgelegt	UNLOCK_PASSWORD=<festgelegtes Kennwort>

Einstellung	Standardwert	Beschreibung, Schlüssel von Windows Installer und deren Werte
Ordner für wiederhergestellte Objekte	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Security für Windows Server\10.1\Restored	RESTOREPATH=<vollständiger Pfad des Ordners> Wiederhergestellte Objekte werden in dem Ordner gespeichert, der durch folgende Parameter angegeben wird: Objekte aus der Quarantäne werden im Unterordner \Quarantine gespeichert. Objekte aus dem Backup werden im Unterordner \Backup gespeichert.

Installations- und Deinstallationsprotokoll für Kaspersky Security 10.1 für Windows Server

Wenn Sie die Installation oder Deinstallation von Kaspersky Security 10.1 für Windows Server mit Hilfe des Assistenten zur Installation (Deinstallation) starten, erstellt der Dienst Windows Installer ein Protokoll über die Installation (Deinstallation). Die Log-Datei mit dem Namen ks4ws_install_<uid>.log (wobei <uid> für die individuelle achtstellige ID des Protokolls steht) wird im Ordner %temp% des Benutzers gespeichert, mit dessen Rechten der Installationsassistent gestartet wurde.

Wenn Sie die Installation oder Deinstallation von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile ausführen, wird in der Grundeinstellung kein Installationsprotokoll erstellt.

► *Geben Sie einen der folgenden Befehle ein, damit bei der Installation von Kaspersky Security 10.1 für Windows Server installieren die Log-Datei ks4ws.log auf dem Laufwerk C:\ angelegt wird:*

- `msiexec /i ks4ws_x86.msi /l*v C:\log.txt /qn EULA=1`
- `msiexec /i ks4ws_x64.msi /l*v C:\log.txt /qn EULA=1`

Installation planen

Dieser Abschnitt enthält eine Beschreibung der Administrations-Tools für Kaspersky Security 10.1 für Windows Server und der besonderen Aspekte bei der Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server mithilfe eines Assistenten (siehe Abschnitt "Installation und Deinstallation des Programms mit dem Assistenten" auf Seite 53), der Befehlszeile (siehe Abschnitt "Installation und Deinstallation des Programms aus der Befehlszeile" auf Seite 68), über Kaspersky Security Center (siehe Abschnitt "Installation und Deinstallation von Kaspersky Anti-Virus überKaspersky Security Center" auf Seite 73) und mittels Active Directory®-Gruppenrichtlinie (siehe Abschnitt "Installation und Deinstallation mittels Active Directory-Gruppenrichtlinien" auf Seite 78).

Bevor Sie mit der Installation von Kaspersky Security 10.1 für Windows Server installieren beginnen, sollten Sie die wichtigsten Installationsetappen planen.

1. Wählen Sie die Administrations-Tools aus, die Sie zur Verwaltung und Konfiguration von Kaspersky

Security 10.1 für Windows Server einsetzen möchten.

2. Legen Sie fest, welche Programmkomponenten für die Installation erforderlich sind (siehe Abschnitt "Programmkomponenten von Kaspersky Security 10.1 für Windows Server und ihre Codes für den Dienst Windows Installer" auf S. 34).
3. Wählen Sie eine Installationsmethode aus.

In diesem Abschnitt

Administrations-Tools auswählen

Entscheiden Sie, welche Administrations-Tools Sie für die Konfiguration der Einstellungen von Kaspersky Security 10.1 für Windows Server und dessen Verwaltung einsetzen möchten. Als Administrations-Tools für Kaspersky Security 10.1 für Windows Server können die Konsole für Kaspersky Security 10.1, das Befehlszeilen-Tool sowie die Verwaltungskonsole von Kaspersky Security Center dienen.

Konsole für Kaspersky Security 10.1

Die Konsole für Kaspersky Security 10.1 ist ein isoliertes Snap-in, das in die Microsoft Management Console eingefügt wird. Sie können Kaspersky Security 10.1 für Windows Server über die Konsole für Kaspersky Security 10.1 verwalten, die auf dem geschützten Server oder auf einem anderen Computer im Unternehmensnetzwerk installiert ist.

Einer Microsoft Management Console, die im Authoring-Modus geöffnet ist, können Sie mehrere Snap-ins von Kaspersky Security 10.1 für Windows Server hinzufügen, um mit ihr den Schutz mehrerer Server zu verwalten, auf denen Kaspersky Security 10.1 für Windows Server installiert ist.

Die Konsole für Kaspersky Security 10.1 gehört zu den Programmkomponenten "Administrations-Tools".

Befehlszeilen-Utility

Sie können Kaspersky Security 10.1 für Windows Server aus der Befehlszeile eines geschützten Servers verwalten.

Das Befehlszeilen-Tool gehört zum Paket der Programmkomponenten von Kaspersky Security 10.1 für Windows Server.

Kaspersky Security Center

Wenn Sie zur zentralisierten Verwaltung des Antiviren-Schutzes für die Computer in Ihrem Unternehmen das Programm Kaspersky Security Center verwenden, können Sie Kaspersky Security 10.1 für Windows Server über die Verwaltungskonsole von Kaspersky Security Center verwalten.

Die folgenden Programmkomponenten müssen installiert werden:

- **Modul für die Integration in den Administrationsagenten von Kaspersky Security Center**. Diese Komponente gehört zum Paket der Programmkomponenten von Kaspersky Security 10.1 für Windows Server. Sie gewährleistet die Kommunikation zwischen Kaspersky Security 10.1 für Windows Server und dem Administrationsagenten. Installieren Sie das Modul zur Integration mit dem Administrationsagenten von Kaspersky Security Center auf dem geschützten Server.
- **Administrationsagent von Kaspersky Security Center**. Installieren Sie ihn auf jedem geschützten Server. Diese Komponente koordiniert die Interaktion zwischen dem auf dem Computer installierten Programm Kaspersky Security 10.1 für Windows Server und der Verwaltungskonsole von Kaspersky Security Center. Die Installationsdatei des Administrationsagenten gehört zum Lieferumfang von Kaspersky Security Center.
- **Plug-in für Kaspersky Security 10.1 für Windows Server**. Installieren Sie auf den Computer, auf dem die Verwaltungskonsole für Kaspersky Security 10.1 für Windows Server installiert ist, zusätzlich das Verwaltungs-Plug-in für den Kaspersky Security Center-Administrationsserver. Das Plug-in bietet die Oberfläche zur Verwaltung des Programms über Kaspersky Security Center. Die Installationsdatei für das Plug-in \server\klcfginst.exe gehört zum Lieferumfang von Kaspersky Security 10.1 für Windows Server.

Installationstyp auswählen

Nach Festlegung der Programmkomponenten für die Installation von Kaspersky Security 10.1 für Windows Server (siehe Abschnitt "Programmkomponenten von Kaspersky Security 10.1 für Windows Server und ihre Codes für den Dienst Windows Installer" auf S. 34) müssen Sie die Installationsmethode auswählen.

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

- Ob spezielle Installationseinstellungen für Kaspersky Security 10.1 für Windows Server festgelegt oder die empfohlenen Installationseinstellungen (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 43) verwendet werden sollen
- Ob die Installationseinstellungen für alle Server einheitlich oder für jeden Server individuell sind

Sie können Kaspersky Security 10.1 für Windows Server mit dem Installationsassistenten sowie ohne Benutzereingriff installieren, indem Sie die Installationseinstellungen in die Befehlszeile eingeben. Sie können Kaspersky Security 10.1 für Windows Server zentral als Remote-Installation installieren: über Gruppenrichtlinien von Active Directory oder mithilfe der Aufgabe zur Remote-Installation von Kaspersky Security Center.

Sie können Kaspersky Security 10.1 für Windows Server auf einem Server installieren, ihn konfigurieren und die Einstellungen in einer Konfigurationsdatei speichern, um später die angelegte Datei für die Installation von Kaspersky Security 10.1 für Windows Server auf anderen Servern zu benutzen (Option gilt nicht bei der Installation über Gruppenrichtlinien des Active Directory).

Installationsassistent starten

Mit dem Installationsassistenten können Sie installieren:

- Komponenten von Kaspersky Security 10.1 für Windows Server (siehe Abschnitt "Programmkomponenten von Kaspersky Security 10.1 für Windows Server" auf Seite 35) auf einem geschützten Server aus einer \server\setup.exe-Datei aus dem Lieferumfang.
- Konsole für Kaspersky Security 10.1 (siehe Abschnitt "Konsole für Kaspersky Security 10.1 installieren" auf Seite 57) aus der Datei \client\setup.exe aus dem Lieferumfang auf dem geschützten Server oder einem anderen LAN-Computer.

Datei des Installationspaketes mit den erforderlichen Installationseinstellungen aus der Befehlszeile starten

Wenn Sie die Datei des Installationspaketes ohne Befehlszeilenoption aufrufen, installieren Sie Kaspersky Security 10.1 für Windows Server mit den Standardinstallationseinstellungen. Mit den Optionen von Kaspersky Security 10.1 für Windows Server können Sie die Installationseinstellungen ändern.

Sie können die Konsole für Kaspersky Security 10.1 auf dem geschützten Server und/oder auf dem Administrator-Arbeitsplatz installieren.

Beispiele für Befehle zur Installation von Kaspersky Security 10.1 für Windows Server und der Konsole für Kaspersky Security 10.1 finden Sie im Abschnitt "Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile" (siehe Abschnitt "Installation und Deinstallation des Programms aus der Befehlszeile" auf Seite 68).

Zentrale Installation über Kaspersky Security Center

Wenn Sie Kaspersky Security Center zur Verwaltung des Antiviren-Schutzes der Netzwerk-Computer einsetzen, können Sie Kaspersky Security 10.1 für Windows Server mit der Aufgabe zur Remote-Installation von Kaspersky Security Center auf mehreren Servern installieren.

Die Server, auf denen Sie Kaspersky Security 10.1 für Windows Server installieren mittels Kaspersky Security Center installieren möchten (siehe Abschnitt "Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center" auf Seite 73) kann sich entweder in derselben Domäne wie das Kaspersky Security Center oder in einer anderen Domäne befinden oder überhaupt zu keiner Domäne gehören.

Zentrale Installation über Gruppenrichtlinien des Active Directory

Mit den Gruppenrichtlinien von Active Directory können Sie Kaspersky Security 10.1 für Windows Server auf dem geschützten Server installieren. Sie können auch die Konsole für Kaspersky Security 10.1 auf dem geschützten Server oder auf dem Administrator-Arbeitsplatz installieren.

Es ist möglich, Kaspersky Security 10.1 für Windows Server nur mit den empfohlenen Installationseinstellungen zu installieren.

Die Server, auf denen Kaspersky Security 10.1 für Windows Server mithilfe von Active Directory-Gruppenrichtlinien installiert wird (siehe Abschnitt "Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory" auf Seite 78) muss sich in derselben Domäne und derselben Organisationseinheit befinden.
Die Installation erfolgt beim Start des Computers vor der Anmeldung bei Microsoft Windows.

Installation und Deinstallation des Programms mit dem Assistenten

Dieser Abschnitt enthält eine Beschreibung des Installations- bzw. Deinstallationsprozesses für Kaspersky Security 10.1 für Windows Server und die Konsole für Kaspersky Security 10.1 mithilfe eines Installationsassistenten, sowie Informationen über die erweiterten Einstellungen von Kaspersky Security 10.1 für Windows Server und die Aktionen nach der Installation des Programms.

In diesem Abschnitt

Installation mit dem Installationsassistenten

Die folgenden Abschnitte enthalten Informationen über die Installation von Kaspersky Security 10.1 für Windows Server und der Konsole für Kaspersky Security 10.1.

► *Gehen Sie folgendermaßen vor, um Kaspersky Security 10.1 für Windows Server zu installieren und das Programm zu verwenden:*

1. Installieren Sie Kaspersky Security 10.1 für Windows Server auf einem geschützten Server.
2. Installieren Sie die Konsole für Kaspersky Security 10.1 auf den Computern, von denen Sie Kaspersky Security 10.1 für Windows Server verwalten möchten.
3. Wenn Sie die Konsole für Kaspersky Security 10.1 im Netzwerk auf keinem anderen Computer als dem geschützten Server installiert haben, sind zusätzliche Einstellungen erforderlich, damit Kaspersky Security 10.1 für Windows Server von den Konsolenbenutzern ferngesteuert verwaltet werden kann.
4. Führen Sie nach der Installation von Kaspersky Security 10.1 für Windows Server Aktionen durch.

In diesem Abschnitt

Installation von Kaspersky Security 10.1 für Windows Server

Bevor Sie Kaspersky Security 10.1 für Windows Server installieren, gehen Sie wie folgt vor:

- Vergewissern Sie sich, dass auf dem Server keine anderen Antiviren-Anwendungen installiert sind. Sie können Kaspersky Security 10.1 für Windows Server installieren, ohne Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition oder Kaspersky Security 10 für Windows Server vorher zu entfernen.
- Vergewissern Sie sich, dass das Benutzerkonto, mit dessen Berechtigungen Sie den Installationsassistenten starten, in der Administratorengruppe auf dem geschützten Server angemeldet ist.

Wechseln Sie nach der Durchführung der oben beschriebenen Aktionen zum Installationsvorgang. Folgen Sie den Anweisungen des Installationsassistenten und geben Sie die Installationseinstellungen für Kaspersky Security

10.1 für Windows Server an. Sie können die Installation von Kaspersky Security 10.1 für Windows Server bei jedem Schritt des Installationsassistenten abbrechen. Klicken Sie dazu im Fenster des Installationsassistenten auf die Schaltfläche **Abbrechen**.

Mehr über die Installations- bzw. Deinstallationseinstellungen finden Sie im Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 43.

► *So installieren Sie Kaspersky Security 10.1 für Windows Server mithilfe eines Installationsassistenten:*

1. Starten Sie auf dem Server die Datei des Begrüßungsprogramms setup.exe.
2. Klicken Sie im folgenden Fenster im Block "Installation" auf den Link **Kaspersky Security 10.1 für Windows Server installieren**.
3. Klicken Sie im folgenden Begrüßungsfenster des Installationsassistenten von Kaspersky Security 10.1 für Windows Server auf die Schaltfläche **Weiter**.

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

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

   Wenn auf dem Server eine kompatible Version der Anwendung installiert ist, wird das Fenster **Vorgängerversion des Programms wurde gefunden** geöffnet.

   Wenn keine Vorgängerversion gefunden wurde, gehen Sie zu Schritt 8 dieser Anleitung.
7. Um ein Upgrade des Programms von der Vorgängerversion durchzuführen, klicken Sie auf die Schaltfläche **Installieren**. Der Installationsassistent führt ein Upgrade des Programms auf Kaspersky Security 10.1 für Windows Server durch und speichert kompatible Einstellungen in der neuen Version. Nach Abschluss des Programm-Upgrades wird das Fenster **Vollständige Installation** geöffnet (fahren Sie mit Schritt 15 dieser Anleitung fort).

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

   Sie können Informationen über untersuchte Objekte des Servers anzeigen: Anzahl der untersuchten Objekte, Anzahl der gefundenen Bedrohungstypen, Anzahl der gefundenen infizierten und möglicherweise infizierten Objekte, Anzahl der infizierten oder verdächtigen Prozesse, die Kaspersky Security 10.1 für Windows Server aus dem Arbeitsspeicher entfernt hat, und Anzahl der infizierten oder verdächtigen Prozesse, die das Programm nicht löschen konnte.

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

Das Fenster **Benutzerdefinierte Installation** wird geöffnet.

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

    Standardmäßig umfasst die empfohlene Installation alle Komponenten von Kaspersky Security 10.1 für Windows Server, mit Ausnahme der Komponenten "Firewall-Verwaltung" und "Skript-Untersuchung".

    > Die Komponente Unterstützung des SNMP-Protokolls von Kaspersky Security 10.1 für Windows Server wird nur auf dem geschützten Server installiert, wenn auf dem Server der Dienst SNMP Microsoft Windows installiert ist.

11. Um alle Änderungen im Fenster **Benutzerdefinierte Installation** zu verwerfen, klicken Sie auf die Schaltfläche **Zurücksetzen**. Klicken Sie auf **Weiter**.
12. Gehen Sie im folgenden Fenster **Zielordner auswählen** wie folgt vor:
    - Geben Sie bei Bedarf einen Ordner an, in dem die Dateien von Kaspersky Security 10.1 für Windows Server 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**.
13. Passen Sie im folgenden Fenster **Erweiterte Einstellungen für die Installation** folgende Installationseinstellungen an:
    - **Echtzeitschutz nach der Installation des Programms aktivieren**.
    - **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**.
    - **Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen**.

      Klicken Sie auf **Weiter**.
14. Gehen Sie im folgenden Fenster **Einstellungen aus einer Konfigurationsdatei importieren** wie folgt vor:
    a. Um die Einstellungen für Kaspersky Security 10.1 für Windows Server 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**.
15. Führen Sie im folgenden Fenster **Programm aktivieren** eine der folgenden Aktionen aus:
    - Wenn Sie das Programm aktivieren möchten, geben Sie die Schlüsseldatei für Kaspersky Security 10.1 für Windows Server zur Aktivierung des Programms an.
    - Wenn Sie das Programm später aktivieren möchten, klicken Sie auf die Schaltfläche **Weiter**.
    - Wenn Sie zuvor eine Schlüsseldatei im Ordner \server (der zum Lieferumfang gehört) gespeichert haben, wird der Name dieser Datei im Feld **Schlüssel** angezeigt.
    - Wenn Sie einen Schlüssel aus der Datei, die in einem anderen Ordner gespeichert ist, hinzufügen möchten, geben Sie die Schlüsseldatei an.

      > Sie können das Programm aus dem Installationsassistenten nicht mithilfe eines Aktivierungscodes aktivieren. Wenn Sie das Programm mithilfe eines Aktivierungscodes aktivieren möchten, können Sie diesen nach der Installation des Programms hinzufügen.

      Nach dem Hinzufügen der Schlüsseldatei werden im Fenster die Lizenzinformationen angezeigt.

Kaspersky Security 10.1 für Windows Server zeigt das berechnete Datum an, an dem die Lizenz abläuft. Die Gültigkeitsdauer der Lizenz wird ab dem Hinzufügen des Schlüssels gezählt, läuft jedoch spätestens nach dem Ablauf der Gültigkeitsfrist der Schlüsseldatei ab.

Klicken Sie auf die Schaltfläche **Weiter**, um den Schlüssel im Programm anzuwenden.

16. Klicken Sie im Fenster **Bereit zur Installation** auf die Schaltfläche Installieren. Der Assistent installiert nun die Komponenten von Kaspersky Security 10.1 für Windows Server.
17. Sobald die Installation abgeschlossen wurde, öffnet sich das Fenster **Die Installation wurde erfolgreich abgeschlossen.**
18. Aktivieren Sie das Kontrollkästchen **Versionshinweise lesen**, um die Ausgabedaten nach Fertigstellung des Installationsassistenten anzusehen.
19. Klicken Sie auf **OK**.

Das Fenster des Installationsassistenten wird geschlossen. Sobald die Installation abgeschlossen wurde, ist Kaspersky Security 10.1 für Windows Server einsatzbereit, vorausgesetzt, dass Sie einen Schlüssel für die Aktivierung des Programms hinzugefügt haben.

Installation der Konsole für Kaspersky Security 10.1

Folgen Sie den Anweisungen des Installationsassistenten und geben Sie die Installationseinstellungen für die Konsole für Kaspersky Security 10.1 an. Sie können die Installation bei jedem Schritt des Assistenten abbrechen. Klicken Sie dazu im Fenster des Assistenten auf die Schaltfläche **Abbrechen**.

► *Gehen Sie folgendermaßen vor, um die Konsole für Kaspersky Security 10.1 zu installieren:*

1. Vergewissern Sie sich, dass das Benutzerkonto, mit dessen Berechtigungen Sie den Installationsassistenten starten, zur Administratorengruppe auf dem Computer gehört.
2. Starten Sie auf dem Computer die Begrüßungsdatei setup.exe.

   Das Fenster des Willkommen-Programms wird geöffnet.
3. Klicken Sie auf den Link **Konsole für Kaspersky Security 10.1 installieren**.

   Es öffnet sich das Begrüßungsfenster des Installationsassistenten. Klicken Sie auf **Weiter**.
4. Machen Sie sich im geöffneten Fenster mit den Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie vertraut und wählen Sie **Bedingungen dieser EULA** und **Datenschutzrichtlinie, die den Umgang mit Daten beschreibt**, um mit der Installation fortzufahren. Klicken Sie auf **Weiter**.
5. Gehen Sie im folgenden Fenster **Erweiterte Einstellungen für die Installation** wie folgt vor:
   - Wenn Sie planen, Kaspersky Security 10.1 für Windows Server auf einem Remote-Computer mithilfe der Konsole für Kaspersky Security 10.1 zu verwalten, aktivieren Sie das Kontrollkästchen **Remote-Zugriff erlauben**.
   - Um das Fenster **Benutzerdefinierte Installation** zu öffnen und Komponenten auszuwählen, gehen Sie wie folgt vor:
     a. Klicken Sie auf die Schaltfläche **Erweitert**.

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

        Standardmäßig werden alle Komponenten installiert.

c. Klicken Sie auf **Weiter**.

> Detailliertere Informationen über die Komponenten von Kaspersky Security 10.1 für Windows Server finden Sie im Abschnitt "Programmkomponenten von Kaspersky Security 10.1 für Windows Server und ihre Codes für den Dienst Windows Installer" auf Seite 34.

6. Gehen Sie im folgenden Fenster **Zielordner auswählen** wie folgt vor:
   a. Geben Sie bei Bedarf einen anderen Ordner an, in dem die Dateien des Anti-Virus gespeichert werden sollen.
   b. Klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster **Bereit zur Installation** auf die Schaltfläche **Installieren**.

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

Das Fenster des Installationsassistenten wird geschlossen. Die Konsole für Kaspersky Security 10.1 wird auf einem geschützten Server installiert.

Wenn Sie das Paket "Administrations-Tools" nicht auf dem geschützten Server, sondern auf einem anderen Netzwerkcomputer installiert haben, nehmen Sie Erweiterte Einstellungen vor (siehe Abschnitt "Erweiterte Einstellungen nach der Installation der Konsole für Kaspersky Security 10.1 auf einem anderen Computer" auf S. 58).

Erweiterte Einstellungen nach der Installation der Konsole für Kaspersky Security 10.1 auf einem anderen Computer

Wenn Sie die Konsole für Kaspersky Security 10.1 nicht auf dem geschützten Computer, sondern auf einem anderen Netzwerkcomputer installiert haben, gehen Sie wie unten beschrieben vor, damit Kaspersky Security 10.1 für Windows Server von den Benutzern ferngesteuert verwaltet werden kann:

- Fügen Sie auf dem geschützten Server die Benutzer von Kaspersky Security 10.1 für Windows Server zur Gruppe KAVWSEE Administrators hinzu.
- Erlauben Sie die Netzwerkverbindungen für den Dienst Kaspersky Security Management Service (kavfsgt.exe), wenn auf dem geschützten Server die Windows-Firewall oder die Firewall eines Drittherstellers verwendet wird.
- Wenn Sie während der Installation der Konsole für Kaspersky Security 10.1 auf einem Computer unter Microsoft Windows das Kontrollkästchen **Remote-Zugriff erlauben** nicht aktiviert haben, erlauben Sie Netzwerkverbindungen für die Konsole für Kaspersky Security 10.1 manuell über die Firewall auf diesem Computer.

In diesem Abschnitt

Über Zugriffsrechte für Kaspersky Security Management Service

Sie können die Liste der Dienste von Kaspersky Security 10.1 für Windows Server überprüfen.

Während der Installation registriert Kaspersky Security 10.1 für Windows Server den Verwaltungsdienst für Kaspersky Security 10.1 für Windows Server (KAVFSGT). Zur Verwaltung des Programms über die auf einem anderen Computer installierte Konsole für Kaspersky Security 10.1 muss das Benutzerkonto, mit dessen Rechten die Verbindung zu Kaspersky Security 10.1 für Windows Server hergestellt wird, unbeschränkten Zugriff auf den Verwaltungsdienst für Kaspersky Security 10.1 für Windows Server auf dem geschützten Server haben.

Folgende Benutzer besitzen standardmäßig Zugriff zur Verwaltung von Kaspersky Security Management Service: Benutzer, die auf dem geschützten Server zur Gruppe "Administratoren" gehören, und Benutzer der Gruppe KAVWSEE Administrators, die bei der Installation von Kaspersky Security 10.1 für Windows Server auf dem geschützten Server erstellt wird.

Sie können Kaspersky Security Management Service nur über das Snap-In **Dienste** von Microsoft Windows verwalten.

Sie können den Benutzerzugriff auf den Verwaltungsdienst von Kaspersky Security 10.1 für Windows Server nicht durch Anpassen von Kaspersky Security 10.1 für Windows Server erlauben oder verweigern.

Sie können unter dem lokalen Benutzerkonto eine Verbindung mit Kaspersky Security 10.1 für Windows Server herstellen, wenn auf dem geschützten Server das Benutzerkonto mit dem gleichen Namen und dem gleichen Kennwort registriert ist.

Netzwerkverbindungen für die Konsole für Kaspersky Security 10.1 erlauben

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

Die Konsole für Kaspersky Security 10.1 auf dem Remote-Computer verwendet das Protokoll DCOM, um Informationen über die Ereignisse für Kaspersky Security 10.1 für Windows Server, zum Beispiel untersuchte Objekte oder abgeschlossene Aufgaben, vom Verwaltungsdienst für Kaspersky Security 10.1 für Windows Server auf dem geschützten Server zu erhalten. Sie müssen die Netzwerkverbindungen in der Windows-Firewall für die Konsole für Kaspersky Security 10.1 freigeben, um die Verbindung zwischen der Konsole von Kaspersky Security 10.1 und dem Verwaltungsdienst für Kaspersky Security 10.1 für Windows Server herzustellen.

Führen Sie folgende Aktionen aus:

- Vergewissern Sie sich, dass der anonyme Remote-Zugriff auf COM-Anwendungen erlaubt ist (nicht aber der Remote-Start und die Remote-Aktivierung von COM-Anwendungen).
- Schalten Sie in der Windows-Firewall den TCP-Port 135 frei und erlauben Sie Netzwerkverbindungen für die ausführbare Datei des Fernverwaltungsprozesses für Kaspersky Security 10.1 für Windows Server kavfsrcn.exe.

  Über TCP-Port 135 greift der Client-Computer, auf dem die Konsole für Kaspersky Security 10.1 installiert ist, auf den geschützten Server zu und der Server beantwortet seine Anfragen.

Wenn die Konsole für Kaspersky Security 10.1 geöffnet war, während Sie die Verbindung zwischen dem geschützten Server und dem Server, auf dem die Konsole installiert ist, angepasst haben, müssen Sie die Konsole für Kaspersky Security 10.1 schließen, auf die Beendigung des Prozesses zur Remote-Verwaltung von Kaspersky Security 10.1 für Windows Server kavfsrcn.exe warten und die Konsole anschließend neu starten. Die neuen Verbindungseinstellungen werden angewendet.

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

1. Öffnen Sie auf dem Server, auf dem die Konsole für Kaspersky Security 10.1 installiert ist, die Konsole Komponentendienste:
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 Servers den Knoten **Computer**.
6. Öffnen Sie das Kontextmenü im Knoten **Arbeitsplatz**.
7. Wählen Sie den Menüpunkt **Eigenschaften**.
8. Klicken Sie auf der Registerkarte **COM-Sicherheit** im Fenster **Eigenschaften** auf die Schaltfläche **Beschränkungen ändern** in der Einstellungsgruppe **Zugriffsrechte**.
9. Vergewissern Sie sich im Fenster **Remote-Zugriff erlauben**, dass für den Benutzer ANONYMOUS LOGON das Kontrollkästchen **Remote-Zugriff erlauben** aktiviert ist.
10. Klicken Sie auf **OK**.

► *Um den TCP-Port 135 in der Windows-Firewall freizugeben und Netzwerkverbindungen für die ausführbare Datei des Prozesses zur Remote-Verwaltung von Kaspersky Security 10.1 für Windows Server zu erlauben, gehen Sie wie folgt vor:*

1. Schließen Sie die Konsole für Kaspersky Security 10.1 auf dem Remote-Computer.
2. Führen Sie eine der Aktionen durch:
   - In Microsoft Windows XP oder Microsoft Windows Vista:
     a. Klicken Sie in Microsoft Windows XP SP2 oder höher auf **Start** → **Windows-Firewall**.

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

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

     c. Geben Sie im Feld **Name** den Portnamen RPC(TCP/135) an, oder geben Sie einen anderen Namen an, z. B. DCOM für Kaspersky Security 10.1 für Windows Server. 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**. Wählen Sie im Fenster **Windows-Firewall** den Punkt **Ein Programm oder Feature durch die Windows-Firewall zulassen**.

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

3. Geben Sie im Fenster **Programm hinzufügen** die Datei kavfsrcn.exe an. Sie befindet sich im Ordner, den Sie bei der Installation der Konsole für Kaspersky Security 10.1 mithilfe von MMC als Zielordner angegeben haben.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf die Schaltfläche **OK** im Fenster **Windows-Firewall** (**Einstellungen für Windows-Firewall**).

Netzwerkverbindungen für den Dienst Kaspersky Security Management Service erlauben

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

Um eine Verbindung zwischen der Konsole für Kaspersky Security 10.1 und dem Kaspersky Security Management Service herzustellen, müssen Sie für den Dienst Netzwerkverbindungen über die Firewall auf dem geschützten Server erlauben.

Wenn Kaspersky Security unter Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2 läuft, müssen Sie die Netzwerkverbindungen anpassen.

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

1. Wählen Sie auf einem geschützten Server unter Windows den Punkt **Start > Systemsteuerung > Sicherheit > Windows-Firewall**.
2. Wählen Sie im Fenster **Einstellungen für Windows-Firewall** den Befehl **Einstellungen ändern** aus.
3. Aktivieren Sie auf der Registerkarte **Ausnahmen** in der Liste mit vordefinierten Ausnahmen die Kontrollkästchen **COM + Netzwerkzugriff, Windows Management Instrumentation (WMI)** und **Remote Administration**.
4. Klicken Sie auf die Schaltfläche **Programm hinzufügen**.
5. Geben Sie im Dialogfenster **Programm hinzufügen** die Datei kavfsgt.exe an. Sie befindet sich im Ordner, den Sie bei der Installation der Konsole von Kaspersky Security 10.1 für Windows Server mithilfe von MMC als Zielordner angegeben haben.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Dialogfenster **Eigenschaften der Windows-Firewall** auf **OK**.

Netzwerkverbindungen werden für den Dienst Kaspersky Security Management Service erlaubt.

Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server ausgeführt werden müssen

Wenn Sie das Programm aktiviert haben, startet Kaspersky Security 10.1 für Windows Server die Aufgaben zum Schutz und zur Untersuchung sofort nach der Installation. Wenn während der Installation von Kaspersky Security 10.1 für Windows Server die Option **Echtzeitschutz nach der Installation des Programms aktivieren** (Standardoption) ausgewählt wurde, untersucht Kaspersky Security 10.1 für Windows Server die Objekte des Dateisystems des Servers, wenn darauf zugegriffen wird. Wenn während der benutzerdefinierten Installation die Komponente Skript-Untersuchung installiert wurde, untersucht Kaspersky Security den Programmcode aller Skripts, wenn diese ausgeführt werden. Jeden Freitag um 20:00 Uhr führt Kaspersky Security 10.1 für Windows Server die Aufgabe Untersuchung wichtiger Bereiche aus.

Es wird empfohlen, nach der Installation von Kaspersky Security 10.1 für Windows Server folgende Aktionen auszuführen:

- Aufgabe Update der Programm-Datenbanken von Kaspersky Security 10.1 für Windows Server starten. Nach der Installation untersucht Kaspersky Security 10.1 für Windows Server Objekte anhand von Datenbanken, die im Lieferumfang des Programms enthalten sind.

  Es wird empfohlen, sofort ein Update der Datenbanken von Kaspersky Security 10.1 für Windows Server 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 Server durch, wenn vor der Installation von Kaspersky Security 10.1 für Windows Server auf dem geschützten Server kein Virenschutzprogramm mit aktivierter Funktion zum Echtzeitschutz für Dateien installiert war.
- Benachrichtigungen des Administrators über Ereignisse in Kaspersky Security 10.1 für Windows Server anpassen.

In diesem Abschnitt

Aufgabe Update der Programm-Datenbanken von Kaspersky Security 10.1 für Windows Server starten und anpassen

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

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

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

1. Starten Sie auf eine der folgenden Arten die Konsole für Kaspersky Security 10.1:
   - Öffnen Sie die Konsole für Kaspersky Security 10.1 auf dem geschützten Server. Wählen Sie dazu **Start > Programme > Kaspersky Security 10.1 für Windows Server** >**Administrations-Tools > Konsole für Kaspersky Security 10.1**.
   - Wenn Sie die Konsole für Kaspersky Security 10.1 nicht auf einem geschützten Server gestartet haben, stellen Sie eine Verbindung mit dem geschützten Server her:
     a. Öffnen Sie das Kontextmenü des Knotens **Kaspersky Security** in der Struktur der Konsole für Kaspersky Security 10.1.
     b. Wählen Sie den Punkt **Verbindung mit anderem Computer herstellen** aus.
     c. Wählen Sie im Fenster **Computer auswählen** die Option **Anderer Computer** und geben Sie im Eingabefeld den Netzwerknamen des geschützten Servers an.

   Wenn das Benutzerkonto, mit dem Sie sich in Microsoft Windows angemeldet haben, über keine Zugriffsrechte für den Verwaltungsdienst Kaspersky Security Management Service verfügt (siehe Abschnitt "Über Zugriffsrechte für Kaspersky Security Management Service" auf S. 59), geben Sie ein Benutzerkonto mit den erforderlichen Rechten an.

   Das Fenster Konsole für Kaspersky Security 10.1 wird geöffnet.
2. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Update**.
3. Wählen Sie den untergeordneten Knoten **Update der Programm-Datenbanken** aus.
4. Klicken Sie im Ergebnisbereich auf den Link **Eigenschaften**.
5. Öffnen Sie im folgenden Fenster **Aufgabeneinstellungen** die Registerkarte **Verbindungseinstellungen**.
6. Führen Sie folgende Aktionen aus:
   a. Wenn in Ihrem Netzwerk das Web Proxy Auto-Discovery Protocol (WPAD-Protokoll) zur automatischen Erkennung von Proxyservern in einem lokalen Netzwerk eingerichtet ist, tragen Sie die Einstellungen des Proxyservers ein: Aktivieren Sie im Einstellungsblock **Proxyserver-Einstellungen** das Kontrollkästchen **Einstellungen des angegebenen Proxyservers verwenden**, tragen Sie im Feld **Adresse** die Adresse und im Feld **Port** die Portnummer des Proxyservers ein.
   b. Wenn in Ihrem Netzwerk eine Authentifizierung für den Zugriff auf den Proxyserver erforderlich ist, wählen Sie die gewünschte Methode zur Authentifizierung in der Dropdown-Liste des Blocks **Einstellungen für die Authentifizierung auf dem Proxyserver** aus:
      - **NTLM-Authentifizierung verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung (NTLM-authentication) unterstützt. Kaspersky Security 10.1 für Windows Server 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 Name und Kennwort verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung unterstützt. Kaspersky Security 10.1 für Windows Server verwendet das von Ihnen vorgegebene Benutzerkonto für die Authentifizierung am Proxyserver. Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.
      - **Benutzernamen und Kennwort verwenden**, um die übliche Authentifizierung auszuwählen (Basic authentication). Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.

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

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

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

1. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 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 Security** anzeigen.

Untersuchung wichtiger Bereiche

Nachdem Sie die Datenbanken von Kaspersky Security 10.1 für Windows Server aktualisiert haben, untersuchen Sie den Server mit der Aufgabe Untersuchung wichtiger Bereiche auf Schadsoftware.

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

1. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie im Kontextmenü des untergeordneten Knotens **Untersuchung wichtiger Bereiche** den Befehl **Starten**.

Die Aufgabe wird gestartet. Im Arbeitsbereich wird der Aufgabenstatus als **Läuft** angegeben.

► *Um den Bericht über Aufgabenausführung anzuzeigen, machen Sie Folgendes,*

klicken Sie im Ergebnisbereich des Knotens **Untersuchung wichtiger Bereiche** auf den Link **Bericht über Aufgabenausführung öffnen**.

Ändern der Programmkomponenten und Wiederherstellen von Kaspersky Security 10.1 für Windows Server

Komponenten von Kaspersky Security 10.1 für Windows Server können hinzugefügt oder entfernt werden. Wenn Sie die Komponente Echtzeitschutz für Dateien deinstallieren wollen, müssen Sie vorsichtshalber zuerst die Aufgabe Echtzeitschutz für Dateien entfernen. In den übrigen Fällen ist es nicht erforderlich, die Aufgabe zum Echtzeitschutz für Dateien oder Kaspersky Security Service anzuhalten.

Wenn der Zugriff auf die Programmverwaltung kennwortgeschützt ist, verlangt Kaspersky Security 10.1 für Windows Server beim Versuch, im erweiterten Schritt des Assistenten Programmkomponenten zu löschen oder ihre Zusammensetzung zu verändern, die Eingabe des Kennworts.

► *Um die Programmkomponenten von Kaspersky Security 10.1 für Windows Server zu ändern, gehen Sie wie folgt vor:*

1. Wählen Sie im **Startmenü** den Punkt **Alle Programme > Kaspersky Security 10.1 für Windows Server >**

Ändern oder Löschen aus.

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

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

   Das Fenster **Benutzerdefinierte Installation** wird geöffnet.

3. Wählen Sie im Fenster **Benutzerdefinierte Installation** aus der Liste der für die Installation verfügbaren Komponenten die Komponenten, die Sie zu Kaspersky Security 10.1 für Windows Server hinzufügen bzw. entfernen möchten. Gehen Sie hierzu wie folgt vor:

   - Um die Zusammenstellung von Komponenten zu verändern, klicken Sie auf die Schaltfläche neben dem Namen der ausgewählten Komponente und wählen Sie im Kontextmenü:
     - den Punkt **Die Komponente wird auf der lokalen Festplatte installiert**, wenn Sie eine einzelne Komponente installieren möchten,
     - den Punkt **Die Komponente und ihre Teilkomponenten werden auf der lokalen Festplatte installiert**, wenn Sie eine Gruppe von Komponenten installieren möchten.
   - Um früher installierte Komponenten zu entfernen, klicken Sie auf die Schaltfläche neben dem Namen der ausgewählten Komponente und wählen Sie im Kontextmenü den Punkt **Die Komponente wird nicht verfügbar sein**.

   Klicken Sie auf **Installieren**.

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

Die Zusammensetzung der Komponenten von Kaspersky Security 10.1 für Windows Server wird gemäß den angegebenen Einstellungen geändert.

Wenn bei der Ausführung von Kaspersky Security 10.1 für Windows Server Probleme aufgetreten sind (Kaspersky Security 10.1 für Windows Server stürzt ab, Aufgaben stürzen ab oder werden nicht gestartet), können Sie versuchen, Kaspersky Security 10.1 für Windows Server zu reparieren. Wenn die Reparatur ausgeführt wird, können entweder die aktuellen Werte der Einstellungen von Kaspersky Security 10.1 für Windows Server beibehalten werden, oder alle Einstellungen von Kaspersky Security 10.1 für Windows Server können auf die Standardwerte zurückgesetzt werden.

► *Um Kaspersky Security 10.1 für Windows Server nach der fehlerhaften Beendigung des Programms oder der Aufgaben wieder herzustellen, gehen Sie wie folgt vor:*

1. Wählen Sie im **Startmenü** den Punkt **Alle Programme > Kaspersky Security 10.1 für Windows Server > Ändern oder Löschen** aus.

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

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

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

3. Aktivieren Sie im Fenster **Installierte Komponenten reparieren** das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**, wenn Sie die konfigurierten Einstellungen des Programms zurücksetzen und Kaspersky Security 10.1 für Windows Server mit den vorinstallierten Standardeinstellungen wiederherstellen möchten. Klicken Sie auf **Installieren**.
4. Bestätigen Sie im Fenster **Bereit zur Wiederherstellung** den Vorgang zur Wiederherstellung

der Zusammensetzung des Programms, indem Sie auf die Schaltfläche **Installieren** klicken.

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

Kaspersky Security 10.1 für Windows Server wird gemäß den angegebenen Einstellungen wiederhergestellt.

Deinstallation mit dem Installationsassistenten

Dieser Abschnitt enthält Anleitungen zur Deinstallation von Kaspersky Security 10.1 für Windows Server und der Konsole für Kaspersky Security 10.1 vom geschützten Server mithilfe des Installationsassistenten.

In diesem Abschnitt

Deinstallation von Kaspersky Security 10.1 für Windows Server

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

Sie können Kaspersky Security 10.1 für Windows Server mit dem Installations-/Deinstallationsassistenten vom geschützten Server deinstallieren.

Nach der Deinstallation von Kaspersky Security 10.1 für Windows Server von einem geschützten Server ist möglicherweise ein Neustart erforderlich. Sie können den Neustart verschieben.

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

Wenn der Zugriff auf die Programmverwaltung kennwortgeschützt ist, verlangt Kaspersky Security 10.1 für Windows Server beim Versuch, im erweiterten Schritt des Assistenten Programmkomponenten zu löschen oder ihre Zusammensetzung zu verändern, die Eingabe des Kennworts.

► *So deinstallieren Sie Kaspersky Security 10.1 für Windows Server:*

1. Wählen Sie im **Startmenü** den Punkt **Alle Programme > Kaspersky Security 10.1 für Windows Server > Ändern oder Löschen** aus.

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

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

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

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

   a. Aktivieren Sie das Kontrollkästchen **Quarantäne-Objekte exportieren**, damit Kaspersky Security 10.1 für Windows Server die Quarantäne-Objekte exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   b. Aktivieren Sie das Kontrollkästchen **Backup-Objekte exportieren**, damit Kaspersky Security 10.1 für Windows Server die Objekte aus der Quarantäne exportiert. Das Kontrollkästchen ist standardmäßig deaktiviert.

   c. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie den Ordner an, in den Sie die wiederhergestellten Objekte exportieren möchten. Standardmäßig erfolgt der Export von Objekten in den Ordner: %ProgramData%\Kaspersky Lab\Kaspersky Security 10.1 für Windows Server\Uninstall.

   Klicken Sie auf **Weiter**.

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

Kaspersky Security 10.1 für Windows Server wird von einem geschützten Server deinstalliert.

Deinstallation der Konsole für Kaspersky Security 10.1

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

Sie können die Konsole für Kaspersky Security 10.1 mit Hilfe des Installations-/Deinstallationsassistenten vom Server deinstallieren.

Nach der Deinstallation der Konsole für Kaspersky Security 10.1 ist kein Neustart des Servers erforderlich.

► *Gehen Sie folgendermaßen vor, um die Konsole für Kaspersky Security 10.1 zu deinstallieren:*

1. Wählen Sie im **Startmenü** den Punkt **Alle Programme > Kaspersky Security 10.1 für Windows Server > Administrations-Tools > Ändern oder Löschen** aus.
2. Das Fenster **Installation ändern, reparieren oder entfernen** des Assistenten wird geöffnet.

   Wählen Sie die Variante **Entfernen von Programmkomponenten** und klicken Sie auf **Weiter**.
3. Es öffnet sich das Fenster **Bereit zur Deinstallation**. Klicken Sie auf die Schaltfläche **Löschen**.

   Es öffnet sich das Fenster **Die Deinstallation wurde abgeschlossen**.
4. Klicken Sie auf **OK**.

Der Deinstallationsvorgang wird abgeschlossen, und das Fenster des Assistenten wird geschlossen.

Installation und Deinstallation des Programms aus der Befehlszeile

Dieser Abschnitt enthält eine Beschreibung der Besonderheiten, die für die Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile gelten. Außerdem finden Sie hier Beispiele für Befehle, mit denen Kaspersky Security 10.1 für Windows Server aus der Befehlszeile installiert und deinstalliert werden kann, sowie Beispiele für Befehle, mit denen Komponenten von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile hinzugefügt oder entfernt werden können.

In diesem Abschnitt

Über die Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile

Sie können Kaspersky Security 10.1 für Windows Server installieren oder deinstallieren, sowie seine Komponenten hinzufügen oder entfernen, indem Sie die Dateien des Installationspakets \server\ks4ws_x86(x64).msi aus der Befehlszeile starten und die Installationseinstellungen mithilfe von Schlüsseln angeben.

Sie können den Satz "Administrations-Tools" auf dem geschützten Server oder auf einem anderen Computer im Netzwerk installieren, damit Sie mit der Konsole für Kaspersky Security 10.1 lokal oder im Remote-Betrieb arbeiten können. Sie können dazu das Installationspaket \client\ks4wstools.msi verwenden.

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

Wenn Sie auf dem geschützten Server eine der Dateien aus \server\ks4ws_x86(x64).msi ohne Reserveschlüssel starten, wird Kaspersky Security 10.1 für Windows Server mit der empfohlenen Installation installiert.

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

Beispiele von Befehlen für die Installation von Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt bietet Beispiele für Befehle zur Installation von Kaspersky Security 10.1 für Windows Server.

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

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

Beispiele für die Installation von Kaspersky Security 10.1 für Windows Server aus der Datei setup.exe

► *Führen Sie folgenden Befehl aus, um Kaspersky Security 10.1 für Windows Server installieren mit den empfohlenen Installationseinstellungen zu installieren, ohne dass eine Interaktion mit dem Benutzer erfolgt:*

\server\setup.exe /s/p EULA=1 PRIVACYPOLICY=1

► *Um Kaspersky Security 10.1 für Windows Server mit den folgenden Einstellungen zu installieren, gehen Sie wie folgt vor:*

- nur Komponente Echtzeitschutz für Dateien und Untersuchung auf Befehl installieren;
- den Echtzeitschutz beim Start von Kaspersky Security 10.1 für Windows Server nicht starten
- und Dateien nicht von der Untersuchung auszuschließen, deren Ausnahme von Microsoft empfohlen wird,

führen Sie folgenden Befehl aus:

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

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

► *Führen Sie folgenden Befehl aus, um Kaspersky Security 10.1 für Windows Server installieren mit den empfohlenen Installationseinstellungen zu installieren, ohne dass eine Interaktion mit dem Benutzer erfolgt:*

```
msiexec /i ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Führen Sie folgenden Befehl aus, um Kaspersky Security 10.1 für Windows Server mit den empfohlenen Installationseinstellungen zu installieren und die Installationsoberfläche anzuzeigen:*

```
msiexec /i ks4ws.msi /qf EULA=1 PRIVACYPOLICY=1
```

► *Um Kaspersky Security 10.1 für Windows Server mit der Aktivierung aus der Schlüsseldatei C:\0000000A.key zu installieren:*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
```

```
PRIVACYPOLICY=1
```

- *Um Kaspersky Security 10.1 für Windows Server zu installieren und vorher die aktiven Prozesse und die Bootsektoren der lokalen Computerlaufwerke zu untersuchen, geben Sie folgenden Befehl ein:*

```
msiexec /i ks4ws.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- *Um Kaspersky Security 10.1 für Windows Server zu installieren und seine Dateien im Zielordner C:\WSEE zu speichern, geben Sie den folgenden Befehl ein:*

```
msiexec /i ks4ws.msi INSTALLDIR=C:\WSEE /qn EULA=1 PRIVACYPOLICY=1
```

- *Um Kaspersky Security 10.1 für Windows Server zu installieren, speichern Sie die Log-Datei des Installationsprotokolls mit dem Namen ks4ws.log im Ordner, in dem die msi-Datei des Installationspakets für Kaspersky Security 10.1 für Windows Server gespeichert ist, und geben Sie den folgenden Befehl ein:*

```
msiexec /i ks4ws.msi /l*v ks4ws.log /qn EULA=1 PRIVACYPOLICY=1
```

- *Um die Konsole für Kaspersky Security 10.1 zu installieren, führen Sie folgenden Befehl aus:*

```
msiexec /i ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

- *Um Kaspersky Security 10.1 für Windows Server mit der Aktivierung aus der Schlüsseldatei C:\0000000A.key zu installieren und Kaspersky Security 10.1 für Windows Server gemäß den in der Konfigurationsdatei C:\settings.xml beschriebenen Einstellungen anzupassen, geben Sie den folgenden Befehl ein:*

```
msiexec /i ks4ws.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server ausgeführt werden müssen

Wenn Sie das Programm aktiviert haben, startet Kaspersky Security 10.1 für Windows Server die Aufgaben zum Schutz und zur Untersuchung sofort nach der Installation. Wenn Sie während der Installation von Kaspersky Security 10.1 für Windows Server die Option **Echtzeitschutz nach der Installation des Programms aktivieren** ausgewählt haben, untersucht Kaspersky Security 10.1 für Windows Server die Objekte des Dateisystems des Servers, wenn darauf zugegriffen wird. Wenn während der benutzerdefinierten Installation die Komponente Skript-Untersuchung installiert wurde, untersucht Kaspersky Security 10.1 für Windows Server den Programmcode aller Skripts, wenn diese ausgeführt werden. Jeden Freitag um 20:00 Uhr führt Kaspersky Security 10.1 für Windows Server die Aufgabe Untersuchung wichtiger Bereiche aus.

Es wird empfohlen, nach der Installation von Kaspersky Security 10.1 für Windows Server folgende Aktionen auszuführen:

- Aufgabe Update der Programm-Datenbanken von Kaspersky Security 10.1 für Windows Server starten. Nach der Installation untersucht Kaspersky Security 10.1 für Windows Server Objekte anhand von Datenbanken, die im Lieferumfang enthalten sind. Es wird empfohlen, die sofort ein Datenbanken-Update für Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server von den Kaspersky-Lab-Update-Servern heruntergeladen. Die Verbindung mit der Update-Quelle erfolgt über einen Proxyserver (Adresse des Proxyservers: proxy.company.com, Port: 8080), wobei für den Serverzugriff die integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung) unter einem Benutzerkonto (Benutzername: inetuser; Kennwort:123456) verwendet wird.

- Führen Sie eine Untersuchung wichtiger Bereiche des Computers durch, wenn vor der Installation von Kaspersky Security 10.1 für Windows Server auf dem geschützten Server kein Virenschutzprogramm mit aktivierter Funktion zum Echtzeitschutz für Dateien installiert war.

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

KAVSHELL SCANCRITICAL /W:scancritical.log

Dieser Befehl speichert den Bericht über Aufgabenausführung in der Datei scancritical.log im aktuellen Ordner.

- Benachrichtigungen des Administrators über Ereignisse in Kaspersky Security 10.1 für Windows Server anpassen.

Komponenten hinzufügen und entfernen. Beispiele für Befehle

Die Komponente "Untersuchung auf Befehl" wird automatisch installiert. Sie müssen sie nicht in der Liste mit den Werten des Schlüssels ADDLOCAL angeben, um die Komponenten von Kaspersky Security 10.1 für Windows Server hinzuzufügen oder zu entfernen.

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

```
msiexec /i ks4ws.msi ADDLOCAL=Oas,AppCtrl /qn EULA=1 PRIVACYPOLICY=1
```

oder

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

Wenn Sie nicht nur Komponenten, die Sie installieren möchten, sondern auch bereits installierte Komponenten angeben, installiert Kaspersky Security 10.1 für Windows Server die angegebenen Komponenten neu.

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

```
msiexec /i ks4ws.msi REMOVE=AppCtrl,WiFiControl /qn EULA=1 PRIVACYPOLICY=1
```

Deinstallation von Kaspersky Security 10.1 für Windows Server. Beispiele für Befehle

► *Um Kaspersky Security 10.1 für Windows Server vom geschützten Server zu deinstallieren, führen Sie folgenden Befehl aus:*

```
msiexec /x ks4ws.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Um die Konsole für Kaspersky Security 10.1 zu deinstallieren, führen Sie folgenden Befehl aus:*

```
msiexec /x ks4wstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

oder

- Für 32-Bit-Betriebssysteme:

```
msiexec /x {232497F6-6572-4934-A6AF-24986952598B} /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec /x {F96C7F1F-9B03-480D-A8F3-19D43CA89090} /qn
```

► *Um Kaspersky Security 10.1 für Windows Server von einem geschützten Server zu deinstallieren, auf dem der Kennwortschutz aktiviert ist, führen Sie folgenden Befehl aus:*

- Für 32-Bit-Betriebssysteme:

```
msiexec.exe /x {DD1532DD-387B-43C5-8968-7E8130CC8A5E} UNLOCK_PASSWORD=*** /qn
```

- Für 64-Bit-Betriebssysteme:

```
msiexec.exe /x {D025308B-AA7E-42D6-8058-B2B79A3D71F5} UNLOCK_PASSWORD=***
/qn
```

► *Um das Plug-in für Kaspersky Security 10.1 für Windows Server von einem geschützten Server zu deinstallieren, auf dem ein Kennwortschutz aktiviert ist, führen Sie folgenden Befehl aus:*

```
msiexec.exe /x {DA15CF4A-75FF-4C92-AFC2-0A16DC645D2E} UNLOCK_PASSWORD=***
/qn
```

Rückgabecodes

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

Tabelle 13. Rückgabecodes

Code	Beschreibung
1324	Der Name des Zielordners enthält unzulässige Zeichen.
25001	Unzureichende Rechte für die Installation von Kaspersky Security 10.1 für Windows Server. Um das Programm zu installieren, starten Sie den Installationsassistenten mit den Rechten des lokalen Administrators.
25003	Kaspersky Security 10.1 für Windows Server kann nicht auf Computern unter der Verwaltung dieser Version von Microsoft Windows installiert werden. Bitte starten Sie den Installationsassistenten, der für die 64-Bit-Version von Microsoft Windows vorgesehen ist.

Code	Beschreibung
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 Security 10.1 für Windows Server über Kaspersky Security Center. Er beschreibt ferner, wie man Kaspersky Security 10.1 für Windows Server über Kaspersky Security Center installiert und deinstalliert, sowie die Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server ausgeführt werden müssen.

In diesem Abschnitt

Allgemeine Informationen zur Installation über Kaspersky Security Center

Sie können Kaspersky Security 10.1 für Windows Server mithilfe einer Remote-Installationsaufgabe über Kaspersky Security Center installieren.

Nach Abschluss der Remote-Installationsaufgabe ist Kaspersky Security 10.1 für Windows Server auf mehreren Servern mit einheitlichen Einstellungen installiert.

Alle Server können in eine Administrationsgruppe zusammengeführt werden und Sie können eine Gruppenaufgabe zur Installation von Kaspersky Security 10.1 für Windows Server auf den Servern dieser Gruppe erstellen.

Sie können eine Remote-Installationsaufgabe für Kaspersky Security 10.1 für Windows Server erstellen, die sich auf eine Auswahl von Servern bezieht, die nicht zur gleichen Administrationsgruppe gehören. Legen Sie dazu eine Liste mit Servern an, auf denen Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server

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

- Auf den Computern, auf denen Sie Kaspersky Security 10.1 für Windows Server installieren möchten, ist bereits der Administrationsagent von Kaspersky Security Center installiert (unabhängig davon, in welcher Domäne sich die Computer befinden und ob sie zu einer Domäne gehören).

  Wenn der Administrationsagent noch nicht auf den Servern installiert ist, können Sie ihn im Rahmen der Remote-Installationsaufgabe zusammen mit Kaspersky Security 10.1 für Windows Server installieren. Bevor Sie den Administrationsagent installieren, vergewissern Sie sich, das Benutzerkonto, das Sie in der Aufgabe angeben, auf allen Servern zur Gruppe der lokalen Administratoren gehört.

- Alle Computer, auf denen Sie Kaspersky Security 10.1 für Windows Server installieren möchten, gehören zur gleichen Domäne wie der Administrationsserver und der Administrationsserver ist unter dem Benutzerkonto Domain-Administrator (**Domain Admin**) registriert (wenn dieses Benutzerkonto über die Rechte eines Administrators auf den Computern der Domäne verfügt).

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

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

- Recht zur Remote-Ausführung von Apps
- Rechte für die **Admin$**-Ressource
- Recht **Als Dienst starten**

Ablauf der Installation von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server künftig über Kaspersky Security Center zu verwalten, vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Auf dem Server, auf dem der Kaspersky Security Center-Administrationsserver installiert ist, ist auch das Verwaltungs-Plug-in für Kaspersky Security 10.1 für Windows Server installiert (Datei \server\klcfginst.exe aus dem Lieferumfang von Kaspersky Security 10.1 für Windows Server).
- Auf den geschützten Servern ist der Administrationsagent von Kaspersky Security Center installiert. Wenn der Administrationsagent von Kaspersky Security Center nicht auf den geschützten Servern installiert ist, können Sie ihn im Rahmen der Remote-Installationsaufgabe zusammen mit Kaspersky Security 10.1 für Windows Server installieren.

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

► *Um Kaspersky Security 10.1 für Windows Server mithilfe einer Aufgabe zur Remote-Installation zu installieren, gehen Sie wie folgt vor:*

1. Starten Sie die Verwaltungskonsole für Kaspersky Security Center.
2. Erweitern Sie im Kaspersky Security Center den Knoten **Remote-Installation**, und wählen Sie im untergeordneten Knoten **Installationspakete** die Option **Neues Installationspaket für ein Kaspersky Lab-Programm** erstellen.
3. Geben Sie den Namen des Installationspakets ein.
4. Geben Sie die Datei "ks4ws.kud" aus dem Lieferumfang von Kaspersky Security 10.1 für Windows Server als Installationspaketdatei an.

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

   Sie müssen den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie akzeptieren, um fortzufahren.
6. So ändern Sie die zu installierenden Komponenten von Kaspersky Security 10.1 für Windows Server (siehe Abschnitt "Ändern der Programmkomponenten und Wiederherstellen von Kaspersky Security 10.1 für Windows Server" auf Seite 64) und die standardmäßigen Installationseinstellungen (siehe Abschnitt "Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf der S. 43 im Installationspaket:

   Erweitern Sie in Kaspersky Security Center den Knoten **Remote-Installation** und öffnen Sie im untergeordneten Knoten **Installationspakete** im Arbeitsbereich das Kontextmenü für das neu erstellte Installationspaket von Kaspersky Security 10.1 für Windows Server. Wählen Sie dort den Befehl

Eigenschaften. Gehen Sie im Fenster **Eigenschaften: <Name des Installationspakets>** im Abschnitt **Einstellungen** wie folgt vor:

a. Aktivieren Sie in der Einstellungsgruppe **Zu installierende Komponenten** die Kontrollkästchen der Komponenten von Kaspersky Security 10.1 für Windows Server, die Sie installieren möchten.

b. Um einen Zielordner anzugeben, der nicht dem standardmäßigen Ordner entspricht, geben Sie im Feld **Zielordner** den Namen und Pfad des Ordners an.

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

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

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

d. Wenn Sie Einstellungen aus der Konfigurationsdatei importieren möchten, die Sie in der vorherigen Version von Kaspersky Security 10.1 für Windows Server erstellt haben, geben Sie die gewünschte Konfigurationsdatei an.

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

7. Erstellen Sie im Knoten **Installationspakete** eine Aufgabe zur Remote-Installation von Kaspersky Security 10.1 für Windows Server installieren auf den ausgewählten Servern (Administrationsgruppe). Passen Sie die Aufgabeneinstellungen an.

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

8. Starten Sie die Remote-Installationsaufgabe für Kaspersky Security 10.1 für Windows Server.

Kaspersky Security 10.1 für Windows Server wird auf den in der Aufgabe angegebenen Servern installiert.

Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server ausgeführt werden müssen

Nach der Installation von Kaspersky Security 10.1 für Windows Server wird empfohlen, die Datenbanken von Kaspersky Security 10.1 für Windows Server auf den Servern zu aktualisieren. Sollte vor der Installation von Kaspersky Security 10.1 für Windows Server auf den Servern kein Virenschutzprogramm mit aktiviertem Echtzeitschutz installiert gewesen sein, wird außerdem empfohlen, eine Untersuchung wichtiger Bereiche der Server durchzuführen.

Wenn Server, auf denen Sie Kaspersky Security 10.1 für Windows Server installiert haben, von Kaspersky Security Center zu einer Administrationsgruppe zusammengefasst sind, können Sie diese Aufgaben auf folgende Arten ausführen:

1. Für die Gruppe der Server, auf denen Sie Kaspersky Security 10.1 für Windows Server installiert haben, eine Aufgabe zum Update der Programm-Datenbanken erstellen. Den Administrationsserver für Kaspersky Security Center als Update-Quelle festlegen.
2. Eine Gruppenaufgabe zur Untersuchung auf Befehl mit dem Aufgabenstatus Untersuchung wichtiger Bereiche erstellen. Das Programm Kaspersky Security Center bewertet den Sicherheitszustand jedes Computers der Gruppe dann aufgrund der Ausführungsergebnisse dieser Gruppe, nicht nach

den Ergebnissen der Systemaufgabe Untersuchung wichtiger Bereiche.

3. Erstellen Sie eine neue Richtlinie für die Servergruppe. In den Eigenschaften der erstellten Richtlinie auf der Registerkarte **Systemaufgaben** den nach Zeitplan gesteuerten Start von Systemaufgaben zur Untersuchung auf Befehl und Update der Programm-Datenbanken auf den Servern der Administrationsgruppe deaktivieren.

Sie können auch die Benachrichtigungen des Administrators über Ereignisse in Kaspersky Security 10.1 für Windows Server anpassen.

Installation der Konsole für Kaspersky Security 10.1 über 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 Konsole für Kaspersky Security 10.1 mithilfe einer Aufgabe zur Remote-Installation zu installieren:*

1. Erweitern Sie in der Verwaltungskonsole für Kaspersky Security Center den Knoten **Remote-Installation** und erstellen Sie im untergeordneten Knoten **Installationspakete** auf Basis der Datei client\setup.exe ein neues Installationspaket. Um das neue Installationspaket zu erstellen:
   - Geben Sie im Fenster **Auswahl des Installationspakets** die Datei client\setup.exe aus dem Ordner des Lieferumfangs von Kaspersky Security 10.1 für Windows Server an und aktivieren Sie das Kontrollkästchen **Ganzen Ordner in das Installationspaket kopieren**.
   - Falls erforderlich, ändern Sie im Feld **Starteinstellungen für ausführbare Datei** (optional) mithilfe der Einstellung ADDLOCAL die Auswahl der zu installierenden Komponenten und ändern Sie den Zielordner.

     Um beispielsweise im Ordner C:\KasperskyConsole nur die Konsole für Kaspersky Security 10.1 zu installieren, nicht aber die Hilfedatei und Dokumentation, geben Sie folgenden Befehl ein:

     ```
     /s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1
     PRIVACYPOLICY=1"
     ```
2. Erstellen Sie im Knoten Installationspakete eine Aufgabe zur Remote-Installation der Konsole für Kaspersky Security 10.1 auf den ausgewählten Computern (Administrationsgruppe). Passen Sie die Aufgabeneinstellungen an.

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

Die Konsole für Kaspersky Security 10.1 wird auf den in der Aufgabe angegebenen Computern installiert.

Deinstallation von Kaspersky Security 10.1 für Windows Server über Kaspersky Security Center

Wenn der Zugriff auf die Verwaltung von Kaspersky Security 10.1 für Windows Server auf den Computern im Netzwerk kennwortgeschützt ist, geben Sie beim Erstellen der Aufgabe zum Löschen von Programmgruppen das Kennwort ein. Wenn der Kennwortschutz nicht zentralisiert mit einer Richtlinie von Kaspersky Security Center verwaltet wird, wird Kaspersky Security 10.1 für Windows Server erfolgreich von den Servern deinstalliert, auf denen der Zugriff auf die Programmverwaltung mit einem Kennwort geschützt ist, das mit dem eingegebenen Kennwort übereinstimmt. Kaspersky Security 10.1 für Windows Server wird nicht von den restlichen Computern deinstalliert.

► *Um Kaspersky Security 10.1 für Windows Server zu deinstallieren, führen Sie in der Verwaltungskonsole von Kaspersky Security Center folgende Aktionen aus:*

1. Erstellen Sie in der Verwaltungskonsole für Kaspersky Security Center eine Aufgabe zur Deinstallation von Programmen.
2. Wählen Sie in der Aufgabe die Deinstallationsmethode (auf die gleiche Weise, wie die Installationsmethode gewählt wurde; s. vorhergehender Abschnitt) und geben Sie das Benutzerkonto an, unter dem der Administrationsserver auf die Server zugreifen soll. Sie können Kaspersky Security 10.1 für Windows Server nur mit den Standarddeinstallationseinstellungen deinstallieren (siehe Abschnitt "Einstellungen für Installation und Deinstallation sowie Optionen für die Befehlszeile für den Dienst Windows Installer" auf Seite 43).

Installation und Deinstallation des Programms über Gruppenrichtlinien von Active Directory

In diesem Abschnitt wird die Installation und Deinstallation von Kaspersky Security 10.1 für Windows Server über Gruppenrichtlinien von Active Directory beschrieben. Er enthält ferner Informationen über die Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server über Gruppenrichtlinien ausgeführt werden müssen.

In diesem Abschnitt

Installation von Kaspersky Security 10.1 für Windows Server über Gruppenrichtlinien von Active Directory

Sie können Kaspersky Security 10.1 für Windows Server auf mehreren Servern über die Gruppenrichtlinie von Active Directory installieren. Auf die gleiche Weise kann auch die Konsole für Kaspersky Security 10.1 installiert werden.

Die Server, auf denen Sie Kaspersky Security 10.1 für Windows Server oder die Konsole für Kaspersky Security 10.1 installieren möchten, müssen zu einer Domäne und einer Organisationseinheit gehören.

Die Betriebssysteme auf den Servern, auf denen Sie Kaspersky Security 10.1 für Windows Server mithilfe der Richtlinie installieren wollen, müssen die gleiche Bit-Version (32-Bit oder 64-Bit) besitzen.

Sie müssen über Administratorrechte auf dem Domain verfügen.

Um Kaspersky Security 10.1 für Windows Server zu installieren, verwenden Sie die Installationspakete ks4ws_x86(x64).msi. Um die Konsole für Kaspersky Security 10.1 zu installieren, verwenden Sie das Installationspaket ks4wstools.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 Security 10.1 für Windows Server (die Konsole für Kaspersky Security 10.1) zu installieren, gehen Sie wie folgt vor:*

1. Speichern Sie die msi-Datei des Installationspakets, die der Bit-Version (32-Bit oder 64-Bit) des installierten Microsoft Windows-Betriebssystems entspricht, in einem freigegebenen Ordner auf dem Domain-Controller.
2. Erstellen Sie auf dem Domain-Controller eine neue Richtlinie für die Gruppe, zu der die Server gehören.
3. Legen Sie mit dem **Group Policy Object Editor** ein neues Installationspaket im Element **Computer-Konfiguration** an. Geben Sie den Pfad zur msi-Datei des Installationspakets für Kaspersky Security 10.1 für Windows Server (die Konsole für Kaspersky Security 10.1) im UNC-Format (Universal Naming Convention) ein.
4. Aktivieren Sie das Kontrollkästchen **Immer mit erhöhten Rechten installieren** für den Dienst Windows Installer, und zwar sowohl im Element **Computer-Konfiguration**, als auch im Element **Benutzer-Konfiguration** für eine ausgewählte Gruppe.
5. Übernehmen Sie die Änderungen mit dem Befehl `gpupdate /force`.

Kaspersky Security 10.1 für Windows Server wird auf den Computern der Gruppe nach deren Neustart und vor der Anmeldung bei Microsoft Windows installiert.

Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server ausgeführt werden müssen

Nach der Installation von Kaspersky Security 10.1 für Windows Server auf den geschützten Servern wird empfohlen, sofort die Programm-Datenbanken zu aktualisieren und eine Untersuchung wichtiger Bereiche des Servers durchzuführen. Sie können diese Aktionen (siehe Abschnitt "Aktionen, die nach der Installation von Kaspersky Security 10.1 für Windows Server ausgeführt werden müssen" auf Seite 62) aus der Konsole für Kaspersky Security 10.1 ausführen.

Sie können auch die Benachrichtigungen des Administrators über Ereignisse in Kaspersky Security 10.1 für Windows Server anpassen.

Deinstallation von Kaspersky Security 10.1 für Windows Server über Gruppenrichtlinien von Active Directory

Wenn Sie Kaspersky Security 10.1 für Windows Server (oder die Konsole für Kaspersky Security 10.1) auf den Gruppenservern mithilfe der Gruppenrichtlinie von Active Directory installiert haben, können Sie diese Richtlinie zur Deinstallation von Kaspersky Security 10.1 für Windows Server (oder der Konsole für Kaspersky Security 10.1) verwenden.

Sie können das Programm nur mit den Standarddeinstallationseinstellungen entfernen.

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

Wenn der Zugriff auf die Programmverwaltung kennwortgeschützt ist, ist die Deinstallation von Kaspersky Security 10.1 für Windows Server über die Gruppenrichtlinien von Active Directory nicht möglich.

► *Um Kaspersky Security 10.1 für Windows Server (die Konsole für Kaspersky Security 10.1) zu deinstallieren, gehen Sie wie folgt vor:*

1. Wählen Sie auf dem Domain-Controller eine Organisationseinheit aus, von deren Servern Sie Kaspersky Security 10.1 für Windows Server oder die Konsole für Kaspersky Security 10.1 deinstallieren möchten.
2. Wählen Sie eine Richtlinie aus, die für die Installation von Kaspersky Security 10.1 für Windows Server erstellt wurde, öffnen Sie im **Editor für Gruppenrichtlinien** im Knoten **Software-Installation** (**Computerkonfiguration > Programm-Konfiguration > Software-Installation**) das Kontextmenü des Installationspakets für Kaspersky Security 10.1 für Windows Server (für die Konsole für Kaspersky Security 10.1) und wählen Sie den Befehl **Alle Aufgaben > Löschen**.
3. Wählen Sie die Deinstallationsmethode **Programm sofort von allen Servern löschen** aus.
4. Übernehmen Sie die Änderungen mit dem Befehl `gpupdate /force`.

Kaspersky Security 10.1 für Windows Server wird von den Servern nach deren Neustart und vor der Anmeldung bei Microsoft Windows deinstalliert.

Funktionsüberprüfung für Kaspersky Security 10.1 für Windows Server. Verwendung des EICAR-Testvirus

Dieser Abschnitt beschreibt den EICAR-Testvirus und das Vorgehen, mit dem die Funktionen "Echtzeitschutz" und "Untersuchung auf Befehl" von Kaspersky Security 10.1 für Windows Server mithilfe des EICAR-Testvirus überprüft werden.

In diesem Abschnitt

EICAR-Testvirus

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

Der Testvirus ist kein Schädling und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte, er wird jedoch von den meisten Antiviren-Anwendungen der Antiviren-Hersteller als Bedrohung erkannt.

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

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

Die Datei eicar.com enthält eine Textzeile. Beim Untersuchen der Datei erkennt Kaspersky Security 10.1 für Windows Server in dieser Textzeile eine Testbedrohung, weist der Datei den Status **Infiziert** zu und löscht sie. Die Daten über die erkannte Bedrohung in der Datei werden in der Konsole für Kaspersky Security 10.1 und im Bericht über Aufgabenausführung angezeigt.

Sie können die Datei eicar.com verwenden, um zu prüfen, wie Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server die Datei eicar.com mit einem Präfix verarbeiten kann, aktivieren Sie im Block der Sicherheitseinstellungen **Schutz von Objekten** die Option **Alle Objekte** für die Aufgaben zum Echtzeitschutz für Dateien und die Aufgaben zur Untersuchung auf Befehl in Kaspersky Security 10.1 für Windows Server.

Tabelle 14. Präfixe in EICAR-Dateien

Präfix	Dateistatus nach Untersuchung und Aktion von Kaspersky Security 10.1 für Windows Server
Ohne Präfix	Kaspersky Security 10.1 für Windows Server weist dem Objekt den Status **Infiziert** zu und löscht es.
SUSP–	Kaspersky Security 10.1 für Windows Server weist dem Objekt den Status **Möglicherweise infiziert** (mit heuristischer Analysemethode erkannt) zu und löscht es (möglicherweise infizierte Objekte werden nicht desinfiziert).

Präfix	Dateistatus nach Untersuchung und Aktion von Kaspersky Security 10.1 für Windows Server
Ohne Präfix	Kaspersky Security 10.1 für Windows Server weist dem Objekt den Status **Infiziert** zu und löscht es.
WARN–	Kaspersky Security 10.1 für Windows Server weist dem Objekt den Status **Möglicherweise infiziert** (Code des Objektes stimmt partiell mit einem bekannten schädlichen Code überein) zu und löscht es (möglicherweise infizierte Objekte werden nicht desinfiziert).
CURE–	Kaspersky Security 10.1 für Windows Server weist dem Objekt den Status **Infiziert** zu und desinfiziert es. Wenn die Desinfektion gelingt, wird der gesamte Text in der Datei durch das Wort "CURE" ersetzt.

Test von Echtzeitschutz und Untersuchung auf Befehl

Nach der Installation von Kaspersky Security 10.1 für Windows Server können Sie bestätigen, dass Kaspersky Security 10.1 für Windows Server Objekte erkennt, die bösartigen Code enthalten. Zur Überprüfung können Sie den EICAR-Testvirus verwenden (siehe Abschnitt "EICAR-Testvirus" auf Seite 81).

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

1. Laden Sie die Datei eicar.com von der EICAR-Website http://www.eicar.org/anti_virus_test_file.htm herunter. Speichern Sie sie in einem freigegebenen Ordner auf einem lokalen Datenträger eines Computers im Netzwerk.

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

2. Wenn Sie außerdem noch die Benachrichtigungen für die Benutzer des Netzwerks prüfen möchten, vergewissern Sie sich, dass auf dem geschützten Server und auf dem Computer, auf dem Sie die Datei eicar.com gespeichert haben, der Windows Messenger Dienst aktiviert ist.
3. Konsole für Kaspersky Security 10.1 öffnen
4. Kopieren Sie auf folgende Weise die gespeicherte Datei eicar.com auf den lokalen Datenträger des geschützten Servers:
   - Um die Funktion Benachrichtigung über Terminaldienste zu überprüfen, kopieren Sie die Datei eicar.com auf einen Server, der 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 Computer, auf dem Sie sie gespeichert haben, über die Netzwerkumgebung dieses Computers.

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

- Die Datei eicar.com wurde vom geschützten Server gelöscht.
- In der Konsole für Kaspersky Security 10.1 wurde dem Bericht über Aufgabenausführung der Status **Kritisch** zugewiesen. Im Bericht ist eine Zeile mit Informationen über eine Bedrohung in der Datei eicar.com erschienen. (Um einen Bericht über Aufgabenausführung anzuzeigen, erweitern Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Echtzeitschutz**, wählen Sie

die Aufgabe Echtzeitschutz für Dateien aus, und klicken Sie im Ergebnisbereich auf den Link **Bericht über Aufgabenausführung öffnen**).

- Auf dem Computer, von dem aus Sie die Datei kopiert haben, wird eine Meldung des Windows Messenger Dienstes mit folgendem Inhalt angezeigt: "`Kaspersky Security 10.1 für Windows Server hat den Zugriff auf <Pfad der Datei eicar.com auf dem Computer>\eicar.com für den Computer <Netzwerkname des Servers> um <Uhrzeit für Ereigniseintritt> gesperrt. Grund: Bedrohung erkannt. Virus: EICAR-Test-File. Name des Objektbenutzers: <Benutzername>. Computername des Objektbenutzers: <Netzwerkname des Computers, von dem die Datei kopiert wurde>`".

> Sehen Sie nach, ob der Windows Messenger Dienst auf dem Computer funktioniert, von dem Sie die Datei eicar.com kopiert haben.

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

1. Laden Sie die Datei eicar.com von der EICAR-Website http://www.eicar.org/anti_virus_test_file.htm herunter. Speichern Sie sie in einem freigegebenen Ordner auf einem lokalen Datenträger eines Computers im Netzwerk.

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

2. Konsole für Kaspersky Security 10.1 öffnen
3. Führen Sie folgende Aktionen aus:
   a. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Untersuchung auf Befehl**.
   b. Wählen Sie den untergeordneten Knoten **Untersuchung wichtiger Bereiche** aus.
   c. Öffnen Sie auf der Registerkarte **Untersuchungsbereich anpassen** das Kontextmenü für den Knoten **Netzwerkumgebung** und wählen Sie **Netzwerkdatei hinzufügen**.
   d. Tragen Sie den Netzwerkpfad zur Datei eicar.com auf dem Remote-Computer im UNC-Format (Universal Naming Convention) ein.
   e. Aktivieren Sie das Kontrollkästchen, um den hinzugefügten Netzwerkpfad in den Untersuchungsbereich aufzunehmen.
   f. Starten Sie die Aufgabe Untersuchung wichtiger Bereiche.

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

- Die Datei eicar.com wurde von der Festplatte des Computers gelöscht.
- In der Konsole für Kaspersky Security 10.1 weist der Bericht über Aufgabenausführung den Status **Kritisch** auf. Im Ausführungsprotokoll für die Aufgabe zur Untersuchung wichtiger Bereiche ist eine Zeile mit Informationen über eine Bedrohung in der Datei eicar.com enthalten. Um einen Bericht über Aufgabenausführung aufzurufen, erweitern Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Untersuchung auf Befehl**, wählen Sie die Aufgabe Untersuchung wichtiger Bereiche aus, und klicken Sie im Ergebnisbereich auf den Link **Bericht über Aufgabenausführung öffnen**.

Programmoberfläche

Sie können Kaspersky Security 10.1 für Windows Server über eine lokale Konsole und das Verwaltungs-Plug-in von Kaspersky Security Center verwalten. Aktionen, die über die lokale Konsole ausgeführt werden können, finden Sie im *Benutzerhandbuch für Kaspersky Security 10.1 für Windows Server*. Die Benutzung des Verwaltungs-Plug-ins erfolgt in der Benutzeroberfläche der Verwaltungskonsole von Kaspersky Security Center. Ausführliche Informationen zur Benutzeroberfläche von Kaspersky Security Center finden Sie in der Dokumentation zu Kaspersky Security Center.

Lizenzverwaltung für das Programm

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

In diesem Kapitel

Über den Endbenutzer-Lizenzvertrag

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

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

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

- Während der Installation von Kaspersky Security 10.1 für Windows Server
- Im Dokument license.txt. Dieses Dokument gehört zum Lieferumfang des Programms.

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

Über die Lizenz

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

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

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

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer des Programms sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen

- Eine *Probelizenz* ist eine kostenlose Lizenz, die zum Kennenlernen des Programms vorgesehen ist.

  Eine Testlizenz besitzt eine kurze Gültigkeitsdauer. Nach Ablauf der Probelizenz stehen nicht mehr alle Funktionen von Kaspersky Security 10.1 für Windows Server zur Verfügung. Sie müssen eine kommerzielle Lizenz erwerben, um das Programm weiter zu nutzen.

  Das Programm kann nur ein einziges Mal mit einer Testlizenz aktiviert werden.

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

  Nach Ablauf der kommerziellen Lizenz funktioniert das Programm auch weiterhin, jedoch lediglich mit eingeschränktem Funktionsumfang (so ist beispielsweise kein Datenbanken-Update für Kaspersky Security verfügbar). Zur weiteren Nutzung von Kaspersky Security 10.1 für Windows Server mit allen Funktionen ist eine Verlängerung der kommerziellen Lizenz erforderlich.

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

In Kaspersky Security 10.1 für Windows Server wird das Ablaufdatum der Lizenz nicht verfolgt. Wenn Sie das Programm noch einmal mit der abgelaufenen Lizenz aktivieren (während der erste Aktivierungscode noch aktiv ist), müssen Sie eine gültige Lizenz verwenden, um den Aktivierungscode erneut hinzuzufügen.

Über Lizenzzertifikate

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

Ein Lizenzzertifikat enthält folgende Lizenzinformationen:

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

- Datum für den Beginn der Lizenzgültigkeit
- Gültigkeitsdauer der Lizenz bzw. Laufzeit der Lizenz
- Lizenztyp

Über Lizenztypen

Kaspersky Security 10.1 für Windows Server ist eine von mehreren Lösungen für den Schutz von Unternehmen. Der Funktionsumfang von Kaspersky Security 10.1 für Windows Server hängt von der ausgewählten Lösung ab. In der Tabelle unten finden Sie die verfügbaren Lösungen und deren jeweiligen Funktionsumfang.

Kaspersky Endpoint Security for Business Basic	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung

Kaspersky Endpoint Security for Business Select	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung

Kaspersky Endpoint Security for Business Advanced	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Kontrolle des Programmstarts Gerätekontrolle Schutz des Datenverkehrs

Kaspersky Endpoint Security for Business Total	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Kontrolle des Programmstarts Gerätekontrolle Schutz des Datenverkehrs

Kaspersky Security for File Server	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Kontrolle des Programmstarts Gerätekontrolle Überwachung der Datei-Integrität Protokollanalyse Schutz des Datenverkehrs (Modus für externen Proxyserver nicht verfügbar)

Kaspersky Security für Datenspeichersysteme	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Kontrolle des Programmstarts Gerätekontrolle Überwachung der Datei-Integrität Protokollanalyse Schutz des Datenverkehrs NAS-Schutz (Speicher) + Schutz vor Verschlüsselung für NAS

Kaspersky Security for Virtualiziation	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Gerätekontrolle Schutz des Datenverkehrs

Kaspersky Security für xSP	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Firewall-Verwaltung Schutz des Datenverkehrs
Kaspersky Hybrid Cloud Security	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Gerätekontrolle Schutz des Datenverkehrs

Kaspersky Hybrid Cloud Security Enterprise	
AWS Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Überwachung der Datei-Integrität Protokollanalyse Kontrolle des Programmstarts Gerätekontrolle Schutz des Datenverkehrs

AWS™ Prepaid-Abonnement	
Komponenten	Datei-Anti-Virus Exploit-Prävention Schutz vor Verschlüsselung (für freigegebene Ordner) Firewall-Verwaltung Überwachung der Datei-Integrität Protokollanalyse Kontrolle des Programmstarts Schutz des Datenverkehrs Gerätekontrolle

Kaspersky Security Internet Gateway	
Komponenten	Datei-Anti-Virus Exploit-Prävention Firewall-Verwaltung Schutz des Datenverkehrs

Über den Schlüssel

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

Mithilfe einer Schlüsseldatei können Sie einen Schlüssel zum Programm hinzufügen. Nachdem Sie den Schlüssel im Programm hinzugefügt haben, wird er auf der Programmoberfläche als unikale Folge aus Buchstaben und Ziffern angezeigt.

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

Es gibt einen aktiven Schlüssel und einen Reserveschlüssel.

Aktiver Schlüssel – Schlüssel, der im Augenblick für die Programmausführung verwendet wird. Als aktiver Schlüssel kann ein Schlüssel für eine Testlizenz oder für eine kommerzielle Lizenz 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.

Der Schlüssel für eine Testlizenz kann nur als aktiver Schlüssel hinzugefügt werden. Der Schlüssel für eine Testlizenz kann nicht als Reserveschlüssel hinzugefügt werden.

Über den Aktivierungscode

Der *Aktivierungscode* ist ein Code, den Sie nach dem Kauf einer kommerziellen Lizenz für Kaspersky Security 10.1 für Windows Server erhalten. Dieser Code ist für die Anforderung der Schlüsseldatei und die Aktivierung des Installationsprogramms mithilfe der Schlüsseldatei erforderlich.

Bei dem Aktivierungscode handelt es sich um eine Folge aus zwanzig Ziffern und lateinischen Buchstaben im Format xxxxx-xxxxx-xxxxx-xxxxx.

Die Gültigkeitsdauer einer Lizenz beginnt mit dem Zeitpunkt der Programmaktivierung. Wenn Sie eine Lizenz für die Nutzung von Kaspersky Security 10.1 für Windows Server auf mehreren Computern gekauft haben, beginnt die Gültigkeitsdauer der Lizenz ab dem Zeitpunkt der Aktivierung des Programms auf dem ersten Computer.

Wenn der Aktivierungscode nach der Aktivierung verloren geht oder versehentlich gelöscht wird, ist für seine Wiederherstellung eine Anfrage an den Technischen Support von Kaspersky Lab erforderlich.

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky Lab erhalten. Mit der Schlüsseldatei wird ein Schlüssel hinzugefügt. Mit diesem Schlüssel wird das Programm aktiviert.

Die Schlüsseldatei wird an die E-Mail-Adresse geschickt, die Sie beim Kauf von Kaspersky Security 10.1 für Windows Server oder der Anforderung einer Testversion von Kaspersky Security 10.1 für Windows Server angegeben haben.

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

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

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

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

Über die Bereitstellung von Daten

Im Endbenutzer-Lizenzvertrag für Kaspersky Security 10.1 für Windows Server, insbesondere im Abschnitt "Bedingungen für die Datenverarbeitung", sind die Bedingungen, die Haftung und das Verfahren für die Übermittlung und Verarbeitung der in diesem Handbuch angegebenen Daten festgelegt. Bevor Sie den Endbenutzer-Lizenzvertrag akzeptieren, lesen Sie die Bedingungen sowie alle Dokumente, die mit dem Endbenutzer-Lizenzvertrag verknüpft sind, sorgfältig.

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

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

- Um den Mechanismus für den Erhalt von Updates zu unterstützen - Informationen über das installierte Programm und das Lizenzzertifikat: Identifikator des zu installierenden Programms und dessen Vollversion, einschließlich Versionsnummer, Typ und Lizenz-ID, Installations-Identifikator, eindeutige ID der Update-Aufgabe.
- Um die Möglichkeit zu nutzen, zu Wissensdatenbankartikeln zu navigieren, wenn Programmfehler auftreten (Redirector-Service) - Informationen über das Programm und den Verknüpfungstyp, insbesondere: Name, Gebietsschema und vollständige Versionsnummer des Programms, Typ des Umleitungslinks und Fehler-ID.
- Zur Verwaltung von Bestätigungen für die Datenverarbeitung - Informationen über den Status der Annahme des Endbenutzer-Lizenzvertrags und anderer Dokumente, die die Bedingungen für die Datenübermittlung festlegen: ID und Version des Lizenzvertrags oder eines anderen Dokuments, als Teil dessen die Bedingungen für die Datenverarbeitung akzeptiert oder abgelehnt werden; ein Attribut, das die Handlung des Benutzers (Bestätigung oder Rückruf der Akzeptanz der Bedingungen) kennzeichnet; Datum und Uhrzeit der Statusänderungen der Annahme der Bedingungen für die Datenverarbeitung.

Lokale Datenverarbeitung

Während der Ausführung der in diesem Handbuch beschriebenen Hauptfunktionen des Programms verarbeitet und speichert Kaspersky Security 10.1 für Windows Server lokal eine Folge von Daten auf dem geschützten Server:

- Informationen über untersuchte Dateien und erkannte Objekte, z. B. Namen und Attribute von verarbeiteten Dateien und vollständige Pfade zu ihnen auf den untersuchten Medien, angewendete Aktionen auf untersuchte Dateien, Konten von Benutzern, die Aktionen im geschützten Netzwerk oder auf dem geschützten Server ausführen, Namen und Daten über untersuchte Geräte, Informationen über Prozesse, die auf dem System ausgeführt werden;
- Informationen über die Aktivität und Einstellungen des Betriebssystems, z. B. Windows-Firewall-Einstellungen, Windows-Ereignisprotokolleinträge, Namen von Benutzerkonten, Instanzen von ausführbaren Dateien, die gestartet werden, und die Typen, Namen, Prüfsummen und Attribute dieser Dateien;
- Informationen über Webaktivitäten, z. B. verarbeitete URLs, zugewiesene Kategorien, Daten über heruntergeladene Objekte, Attribute verarbeiteter digitaler Zertifikate, Daten über verarbeitete E-Mails, einschließlich Absender, Empfänger, Betreff, Nachrichtentext und Anhänge
- Informationen über Netzwerkaktivitäten, einschließlich der IP-Adressen von blockierten Client-Computern.

Kaspersky Security 10.1 für Windows Server 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 verarbeitet und geschützt.

Mit Kaspersky Security 10.1 für Windows Server können Sie die Sicherheitsstufe für lokal verarbeitete Daten konfigurieren: Sie können die Benutzerrechte für den Zugriff auf Prozessdaten ändern, die Aufbewahrungsfristen für diese Daten ändern, die Funktionen zur Datenprotokollierung ganz oder teilweise deaktivieren und den Pfad und die Attribute des Ordners auf dem Laufwerk, auf dem die Daten protokolliert werden, ändern.

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

Aktivierung des Programms mithilfe eines Schlüssels

Sie können Kaspersky Security 10.1 für Windows Server aktivieren, indem Sie einen Schlüssel anwenden.

Wenn Sie einen Schlüssel als aktiven Schlüssel hinzufügen und in Kaspersky Security 10.1 für Windows Server bereits ein anderer aktiver Schlüssel hinzugefügt worden ist, wird der zuvor hinzugefügte Schlüssel durch den neuen ersetzt. Der früher hinzugefügte aktive Schlüssel wird gelöscht.

Wenn Sie einen Schlüssel als Reserveschlüssel hinzufügen und in Kaspersky Security 10.1 für Windows Server bereits ein anderer Reserveschlüssel hinzugefügt worden ist, wird der zuvor hinzugefügte Schlüssel durch den neuen ersetzt. Der früher hinzugefügte Reserveschlüssel wird gelöscht.

Wenn Sie einen neuen Schlüssel als aktiven Schlüssel hinzufügen und in Kaspersky Security 10.1 für Windows Server bereits ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt worden sind, wird der zuvor hinzugefügte aktive Schlüssel durch den neuen ersetzt und der Reserveschlüssel wird nicht gelöscht.

► *Um Kaspersky Security 10.1 für Windows Server mithilfe eines Schlüssels zu aktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Lizenzverwaltung**.
2. Betätigen Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** den Link **Schlüssel hinzufügen**.
3. Klicken Sie im folgenden Fenster auf die Schaltfläche **Durchsuchen** und wählen Sie eine Schlüsseldatei mit der Erweiterung key aus.

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

4. Klicken Sie auf **OK**.

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

Aufrufen von Informationen über die aktive Lizenz

Lizenzinformationen anzeigen

Die Informationen zur aktuellen Lizenz werden im Ergebnisbereich des Knotens **Kaspersky Security** der Konsole für Kaspersky Security 10.1 angezeigt. Der Schlüsselstatus kann folgende Werte annehmen:

- **Schlüsselstatus wird überprüft** – Kaspersky Security 10.1 für Windows Server überprüft eine hinzugefügte Schlüsseldatei oder einen verwendeten Aktivierungscode und wartet auf die Antwort zum aktuellen Lizenzstatus.
- **Gültigkeitsdauer der Lizenz** – Kaspersky Security 10.1 für Windows Server bleibt bis zum angegebenen Zeitpunkt aktiviert. Der Schlüsselstatus ist in folgenden Fällen gelb hervorgehoben:
  - Die Restlaufzeit der Lizenz beträgt noch 14 Tage, und es wurde kein Reserveschlüssel oder Aktivierungscode hinzugefügt.
  - Der hinzugefügte Schlüssel befindet sich in der schwarzen Liste und seine Blockierung steht unmittelbar bevor.
- **Das Programm wurde nicht aktiviert** – Kaspersky Security 10.1 für Windows Server ist nicht aktiviert, da

kein Schlüssel oder Aktivierungscode hinzugefügt wurde. Der Status ist rot hervorgehoben.

- **Die Lizenz ist abgelaufen** – Kaspersky Security 10.1 für Windows Server ist nicht aktiviert, da die Lizenz abgelaufen ist. Der Status ist rot hervorgehoben.
- **Verstoß gegen den Endbenutzer-Lizenzvertrag** – Kaspersky Security 10.1 für Windows Server ist nicht aktiviert, da die Bedingungen des Endbenutzer-Lizenzvertrags verletzt wurden (siehe Abschnitt "Über den Endbenutzer-Lizenzvertrag" auf S. 85). Der Status ist rot hervorgehoben.
- **Der Schlüssel wurde auf die schwarze Liste gesetzt** – die hinzugefügte Schlüsseldatei ist blockiert und wurde durch Kaspersky Lab auf die schwarze Liste gesetzt, beispielsweise wenn der Schlüssel durch Unbefugte zur illegalen Programmaktivierung verwendet wurde. Der Status ist rot hervorgehoben.
- **Abonnement unterbrochen** – das Abonnement wurde vorübergehend unterbrochen. Der Status ist rot hervorgehoben. Sie können das Abonnement jederzeit fortsetzen.

Anzeigen von Informationen über die aktive Lizenz

► *Um die Informationen über die aktuelle Lizenz einzusehen,*

Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Lizenzverwaltung**.

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

Tabelle 15. Allgemeine Lizenzinformationen im Knoten Lizenzverwaltung

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

► *Um Details über die Lizenz einzusehen.*

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

Im Fenster **Eigenschaften:<Status des Aktivierungscodes oder Schlüssels>** auf der Registerkarte **Allgemein** werden ausführliche Informationen über die aktive Lizenz angezeigt, auf der Registerkarte **Erweitert** werden Informationen über den Käufer und Kontaktinformationen von Kaspersky Lab oder dem Partner angezeigt, bei dem Sie Kaspersky Security 10.1 für Windows Server gekauft haben (siehe Tabelle unten).

Tabelle 16. Ausführliche Lizenzinformationen im Fenster Eigenschaften <Schlüsselnummer>

Feld	Beschreibung
Registerkarte Allgemein	
Schlüssel	Nummer des Schlüssels, mit dessen Hilfe Sie das Programm aktiviert haben.
Schlüssel hinzugefügt am	Datum, an dem der Schlüssel zum Programm hinzugefügt wurde.
Lizenztyp	Lizenztyp: kommerziell oder Probe
Läuft ab in (Tage)	Anzahl der Tage bis zum Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz.
Gültig bis	Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz. Wenn Sie das Programm auf Basis eines unbefristeten Abonnements aktivieren, wird der Feldwert *Unbefristet* angezeigt. Wenn Kaspersky Security 10.1 für Windows Server das Ablaufdatum der Lizenz nicht ermitteln kann, wird der Wert *Unbekannt* angezeigt.
Programm	Programmname, für den der Schlüssel oder der Aktivierungscode hinzugefügt wurde.
Nutzungsbeschränkung für Schlüssel	Vorgesehene Beschränkungen für die Verwendung des Schlüssels (sofern vorhanden).
Verfügbarkeit des Technischen Supports	Informationen darüber, ob Kaspersky Lab oder ein Partner dem Kunden nach den Lizenzbedingungen technischen Support leisten.
Registerkarte Erweitert	
Lizenzinformationen	Nummer und Typ der aktiven Lizenz.
Support-Informationen	Kontaktinformationen von Kaspersky Lab oder von dem Partner, der für den technischen Support verantwortlich ist. Dieses Feld kann leer sein, wenn kein technischer Support geleistet wird.
Informationen zum Benutzer	Informationen zum Käufer der Lizenz: Name des Auftraggebers und Name des Unternehmens, für das die Lizenz erworben wurde.

Funktionsbeschränkungen nach Ablauf der Lizenz

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

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

Andere Funktionen (Speicher, Berichte, Diagnoseinformationen) stehen weiterhin zur Verfügung.

Verlängerung der Lizenz

Standardmäßig werden Sie 14 Tage vor dem Ablaufdatum der Lizenzgültigkeit von Kaspersky Security 10.1 für Windows Server über den baldigen Ablauf der Lizenz benachrichtigt. Dabei wird der Status **Gültigkeitsdauer der Lizenz** im Ergebnisbereich des Knotens **Kaspersky Security** gelb hervorgehoben.

Sie können die Gültigkeitsdauer der Lizenz schon vor deren Ablauf verlängern, indem Sie einen zusätzlichen Aktivierungscode oder einen Reserveschlüssel hinzufügen. So vermeiden Sie, dass der Computer nach Ablauf der Laufzeit der aktuellen Lizenz bis zur Aktivierung des Programms mit der neuen Lizenz ungeschützt ist.

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

1. Kaufen Sie einen neuen Aktivierungscode oder eine Schlüsseldatei für das Programm.
2. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 den Knoten **Lizenzverwaltung**.
3. Führen Sie im Ergebnisfenster des Knotens **Lizenzverwaltung** eine der folgenden Aktionen aus:
   - Wenn Sie die Lizenz mithilfe eines Reserveschlüssels verlängern möchten:
     a. Klicken Sie auf den Link Schlüssel **hinzufügen**.
     b. Klicken Sie im erscheinenden Fenster auf die Schaltfläche **Durchsuchen** und wählen Sie die neue Schlüsseldatei mit der Erweiterung key aus.
     c. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.
   - Wenn Sie die Lizenz mithilfe eines Aktivierungscodes verlängern möchten:
     a. Klicken Sie auf den Link **Aktivierungscode hinzufügen**.
     b. Geben Sie den erworbenen Aktivierungscode im erscheinenden Fenster ein.
     c. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.

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

Der Reserveschlüssel bzw. der Aktivierungscode wird hinzugefügt, und nach Ablauf des aktiven Schlüssels bzw. Aktivierungscodes für Kaspersky Security 10.1 für Windows Server automatisch aktiviert.

Schlüssel löschen

Sie können den hinzugefügten Schlüssel entfernen.

Wenn in Kaspersky Security 10.1 für Windows Server 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 Konsole für Kaspersky Security 10.1 den Knoten **Lizenzverwaltung**.
2. Wählen Sie im Ergebnisbereich des Knotens **Lizenzverwaltung** in der Tabelle mit Informationen über die hinzugefügten Schlüssel den Schlüssel aus, den Sie entfernen möchten.
3. Wählen Sie im Kontextmenü der Zeile mit den Informationen über den ausgewählten Schlüssel den Punkt **Löschen** aus.
4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um das Löschen des Schlüssels zu bestätigen.

Der ausgewählte Schlüssel wird gelöscht.

Starten und Beenden von Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält Informationen zum Start und Stoppen des Verwaltungs-Plug-ins für Kaspersky Security 10.1 für Windows Server sowie von Kaspersky Security Service.

In diesem Kapitel

Verwaltungs-Plug-in von Kaspersky Security Center starten

Für den Start des Plug-ins für Kaspersky Security Center sind keine weiteren Aktionen erforderlich, wenn mit Kaspersky Security 10.1 für Windows Server gearbeitet wird. Nach der Installation des Plug-ins auf dem Computer des Administrators wird dieses zusammen mit Kaspersky Security Center gestartet. Ausführliche Informationen über den Start von Kaspersky Security Center finden Sie im *Hilfesystem von Kaspersky Security Center*.

Kaspersky Security Service starten und anhalten

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

Beim Start von Kaspersky Security 10.1 für Windows Server werden standardmäßig folgende Aufgaben gestartet: Echtzeitschutz für Dateien, Skript-Untersuchung (falls installiert), Untersuchung beim Hochfahren des Betriebssystems, Integritätsprüfung für Programme sowie andere Aufgaben, für deren Zeitplan die Startfrequenz **Bei Programmstart** gilt.

Wenn Sie den Dienst von Kaspersky Security Service beenden, werden alle laufenden Aufgaben beendet. Nachdem Sie Kaspersky Security Service neu gestartet haben, startet das Programm nur jene Aufgaben automatisch, bei denen im Zeitplan das Startintervall **Bei Programmstart** festgelegt ist; die anderen Aufgaben müssen manuell gestartet werden.

Sie können den Dienst Kaspersky Security Service über das Kontextmenü des Knotens **Kaspersky Security** oder mithilfe des Snap-Ins **Dienste von Microsoft Windows** starten und beenden.

Sie können Kaspersky Security 10.1 für Windows Server starten und beenden, wenn Sie zur Gruppe "Administratoren" auf dem geschützten Server gehören.

► *Um das Programm mithilfe der Management-Konsole zu beenden oder zu starten, gehen Sie wie*

folgt vor:

1. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 das Kontextmenü des Knotens **Kaspersky Security**.
2. Wählen Sie einen der folgenden Befehle:
   - **Programm beenden**
   - **Programm starten**

Der Dienst von Kaspersky Security Service wird gestartet oder beendet.

Über Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält Informationen über die Rechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server und der Windows-Dienste, die das Programm registriert, sowie eine Anleitung zur Konfiguration dieser Rechte.

In diesem Kapitel

Über Rechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server

Standardmäßig haben die Benutzer der Gruppe "Administratoren" auf dem geschützten Server und die Benutzer der Gruppe "KAVWSEE Administrators", die auf einem geschützten Server bei der Installation von Kaspersky Security 10.1 für Windows Server erstellt wird, sowie die Gruppe "SYSTEM" Zugriff auf alle Funktionen von Kaspersky Security 10.1 für Windows Server .

Benutzer, die Zugriff auf die Funktionen Rechte **ändern** von Kaspersky Security 10.1 für Windows Server haben, können auch anderen Benutzern, die am geschützten Server registriert sind oder zur Domäne gehören, den Zugriff auf Funktionen von Kaspersky Security 10.1 für Windows Server gewähren.

Wenn ein Benutzer nicht in die Liste der Benutzer von Kaspersky Security 10.1 für Windows Server registriert ist, kann er die Konsole für Kaspersky Security 10.1 nicht öffnen.

Sie können für einen Benutzer oder eine Benutzergruppe eine der folgenden vordefinierten Stufen für den Zugriff auf die Funktionen von Kaspersky Security 10.1 für Windows Server auswählen:

- **Vollständige Kontrolle** – Zugriff auf alle Programmfunktionen: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Security 10.1 für Windows Server, der Komponenteneinstellungen, der Rechte von Benutzern von Kaspersky Security 10.1 für Windows Server, sowie Anzeigen der Statistik für Kaspersky Security 10.1 für Windows Server.
- **Ändern** – Zugang zu allen Programmfunktionen mit Ausnahme der Veränderung der Benutzerrechte: Anzeigen und Bearbeiten der allgemeinen Einstellungen von Kaspersky Security 10.1 für Windows Server und der Einstellungen der Komponenten von Kaspersky Security 10.1 für Windows Server.

- **Lesen** – Anzeigen der allgemeinen Einstellungen von Kaspersky Security 10.1 für Windows Server, der Einstellungen der Komponenten von Kaspersky Security 10.1 für Windows Server, der Statistik für Kaspersky Security 10.1 für Windows Server und der Benutzerrechte für Kaspersky Security 10.1 für Windows Server.

Sie können auch die erweiterten Zugriffsrechte konfigurieren (siehe Abschnitt "Konfiguration der Zugriffsrechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server und Kaspersky Security Service" auf Seite 104): Zugriff auf bestimmte Funktionen von Kaspersky Security 10.1 für Windows Server erlauben oder verweigern.

Wenn Sie die Zugriffsrechte für einen Benutzer oder eine Gruppe manuell konfiguriert haben, so wird für diesen Benutzer bzw. diese Gruppe die Zugriffsstufe **Sonderrechte** festgelegt.

Tabelle 17. Über Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server

Zugriffsrechte	Beschreibung
Aufgabenverwaltung	Berechtigung zum Starten, Beenden, Anhalten bzw. Fortsetzen der Aufgaben von Kaspersky Security 10.1 für Windows Server.
Erstellen und Löschen von Aufgaben zur Untersuchung auf Befehl	Berechtigung zum Erstellen und Löschen von Aufgabe zur Untersuchung auf Befehl.
Ändern von Parametern	Berechtigungen: • Einstellungen von Kaspersky Security 10.1 für Windows Server aus einer Konfigurationsdatei importieren • Programmeinstellungen bearbeiten
Lesen von Parametern	Berechtigungen: • Allgemeine Einstellungen und Aufgabeneinstellungen für Kaspersky Security 10.1 für Windows Server anzeigen. • Exportieren der Einstellungen von Kaspersky Security 10.1 für Windows Server in eine Konfigurationsdatei. • Einstellungen für Berichte über Aufgabenausführung, für den Systemaudit-Bericht und für Benachrichtigungen anzeigen.
Verwalten von Speichern	Berechtigungen: • Objekte in Quarantäne verschieben • Objekte aus der Quarantäne und dem Backup löschen • Objekte aus der Quarantäne und dem Backup wiederherstellen
Verwaltung von Berichten	Berechtigung zum Löschen von Berichten über Aufgabenausführung und zum Leeren des Systemaudit-Berichts
Lesen von Berichten	Berechtigung zur Anzeige der Ereignisse von Anti-Virus in Berichten über Aufgabenausführung und im Systemaudit-Bericht.
Lesen der Statistik	Berechtigung zum Anzeigen der Statistik für die einzelnen Aufgaben von Kaspersky Security 10.1 für Windows Server.
Lizenzverwaltung für das Programm	Kaspersky Security 10.1 für Windows Server kann aktiviert oder deaktiviert werden.
Programm entfernen	Berechtigung zum Deinstallieren von Kaspersky Security 10.1 für Windows Server.
Lesen von Benutzerrechten	Berechtigung zum Anzeigen der Benutzerlisten von Kaspersky Security 10.1 für Windows Server und der Zugriffsrechte der einzelnen Benutzer

Zugriffsrechte	Beschreibung
Ändern von Rechten	Berechtigungen: • Liste der Benutzer ändern, die Zugriff auf die Programmverwaltung haben • Benutzerzugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server bearbeiten

Über die Rechte zur Verwaltung des Dienstes Kaspersky Security Service

Bei der Installation registriert Kaspersky Security 10.1 für Windows Server in Windows den Dienst von Kaspersky Security Service (KAVFS), da dieser die Komponenten beinhaltet, die beim Hochfahren des Betriebssystems gestartet werden. Um die Gefahr des Zugriffs Unbefugter auf die Programmfunktionen und Sicherheitseinstellungen auf dem geschützten Server über die Verwaltung von Kaspersky Security Service zu reduzieren, können Sie die Rechte zur Verwaltung von Kaspersky Security Service mithilfe der lokalen Konsole für Kaspersky Security 10.1 oder des Verwaltungs-Plug-ins für Kaspersky Security Center beschränken.

Standardmäßig haben diejenigen Benutzer Zugriff auf die Verwaltung von Kaspersky Security Service, die der Gruppe "Administratoren" auf dem geschützten Server angehören, sowie die Systemgruppen "SERVICE" und "INTERACTIVE" mit Leserechten und die Systemgruppe "SYSTEM" mit Rechten zum Lesen und Ausführen.

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

Benutzer, die Zugriff auf Funktionen (siehe Abschnitt "Über Rechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server" auf S. 100) der Stufe "Rechte ändern" haben, können anderen Benutzern, die auf dem geschützten Server 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 Security 10.1 für Windows Server eine der folgenden vordefinierten Stufen des Zugriffs auf die Verwaltung von Kaspersky Security Service auswählen:

- **Vollständige Kontrolle** – Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und Benutzerrechte von Kaspersky Security Service sowie zum Starten und Beenden von Kaspersky Security Service.
- **Lesen** – Berechtigung zum Aufrufen der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
- **Änderung** – Berechtigung zum Aufrufen und Ändern der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
- **Ausführung** – Berechtigung zum Starten und Beenden von Kaspersky Security Service.

Außerdem können Sie erweiterte Einstellungen für die Zugriffsrechte vornehmen: Zugriff auf bestimmte Funktionen von Kaspersky Security 10.1 für Windows Server erlauben oder verbieten (siehe Tabelle unten).

Wenn Sie die Zugriffsrechte für einen Benutzer oder eine Gruppe manuell konfiguriert haben, so wird für diesen Benutzer bzw. diese Gruppe die Zugriffsstufe **Sonderrechte** festgelegt.

Tabelle 18. Differenzierung der Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server

Funktion	Beschreibung
Einstellungen des Dienstes lesen	Berechtigung zum Aufrufen der allgemeinen Einstellungen und der Benutzerrechte von Kaspersky Security Service.
Status des Dienstes beim Service Control Manager abfragen	Berechtigung zur Abfrage des Ausführungsstatus von Kaspersky Security Service beim Service Control Manager von Microsoft Windows
Status beim Dienst abfragen	Berechtigung zur Abfrage des Ausführungsstatus des Dienstes bei Kaspersky Security Service.
Abhängige Dienste auflisten	Berechtigung zum Aufruf einer Liste der Dienste, von denen Kaspersky Security Service abhängt, sowie der Dienste, die von Kaspersky Security Service abhängen.
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 zu Kaspersky Security Service ändern.
Dienst entfernen	Berechtigung zum Entfernen von Kaspersky Security Service aus der Registrierung über den Service Control Manager von Microsoft Windows.
Benutzeranfragen an den Dienst	Berechtigung zur Erstellung und zum Versand von Benutzeranfragen an Kaspersky Security Service.

Über Zugriffsrechte für Kaspersky Security Management Service

Sie können die Liste der Dienste von Kaspersky Security 10.1 für Windows Server überprüfen.

Während der Installation registriert Kaspersky Security 10.1 für Windows Server den Verwaltungsdienst für Kaspersky Security 10.1 für Windows Server (KAVFSGT). Zur Verwaltung des Programms über die auf einem anderen Computer installierte Konsole für Kaspersky Security 10.1 muss das Benutzerkonto, mit dessen Rechten

die Verbindung zu Kaspersky Security 10.1 für Windows Server hergestellt wird, unbeschränkten Zugriff auf den Verwaltungsdienst für Kaspersky Security 10.1 für Windows Server auf dem geschützten Server haben.

Folgende Benutzer besitzen standardmäßig Zugriff zur Verwaltung von Kaspersky Security Management Service: Benutzer, die auf dem geschützten Server zur Gruppe "Administratoren" gehören, und Benutzer der Gruppe KAVWSEE Administrators, die bei der Installation von Kaspersky Security 10.1 für Windows Server auf dem geschützten Server erstellt wird.

Sie können Kaspersky Security Management Service nur über das Snap-In **Dienste** von Microsoft Windows verwalten.

Sie können den Benutzerzugriff auf den Verwaltungsdienst von Kaspersky Security 10.1 für Windows Server nicht durch Anpassen von Kaspersky Security 10.1 für Windows Server erlauben oder verweigern.

Sie können unter dem lokalen Benutzerkonto eine Verbindung mit Kaspersky Security 10.1 für Windows Server herstellen, wenn auf dem geschützten Server das Benutzerkonto mit dem gleichen Namen und dem gleichen Kennwort registriert ist.

Konfiguration der Zugriffsrechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server und Kaspersky Security Service

Sie können die Liste der Benutzer und Benutzergruppen ändern, denen der Zugriff auf die Funktionen von Kaspersky Security 10.1 für Windows Server und die Verwaltung von Kaspersky Security Service erlaubt ist, sowie die Zugriffsrechte dieser Benutzer und Benutzergruppen ändern.

► *Gehen Sie wie folgt vor, um Benutzer oder Gruppen zur Liste hinzuzufügen oder aus dieser zu entfernen:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Server Sie die Programmeinstellungen konfigurieren möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Richtlinieneinstellungen für eine Gruppe von Servern anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie **<Name der Richtlinie> > Eigenschaften**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, öffnen Sie die gewünschten Einstellungen in den **Programmeinstellungen** (siehe Abschnitt "**Konfiguration von lokalen Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center**" auf S. 125).
3. Führen Sie im Abschnitt **Einstellungen** eine der folgenden Aktionen aus:
   - Wählen Sie **Benutzerrechte für die Programmverwaltung ändern** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Security 10.1 für Windows Server haben.
   - Wählen Sie den Punkt **Benutzerrechte für die Verwaltung von Kaspersky Security Service ändern** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung des Programms mithilfe von Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Security 10.1 für Windows Server** wird geöffnet.

4. Im sich öffnenden Fenster gehen Sie wie folgt vor:
   - Um einen Benutzer oder eine Gruppe zur Benutzerliste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie den Benutzer oder die Gruppe aus, dem bzw. der Sie die Rechte zuweisen möchten.
   - Wählen Sie den Benutzer oder die Gruppe aus, für die Sie den Zugriff beschränken möchten, und klicken Sie auf **Löschen**, um einen Benutzer oder eine Gruppe aus der Liste zu löschen.
5. Klicken Sie auf die Schaltfläche **Übernehmen**.

Die ausgewählten Benutzer (Gruppen) werden hinzugefügt bzw. entfernt.

► *Gehen Sie wie folgt vor, um die Rechte eines Benutzers oder einer Gruppe zur Verwaltung von Kaspersky Security 10.1 für Windows Server oder von Kaspersky Security Service zu ändern:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Server Sie die Programmeinstellungen konfigurieren möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Einstellungen einer Richtlinie anzupassen, wählen Sie in der Verwaltungskonsole von Kaspersky Security Center in der Gruppe "Computer" die Registerkarte **Richtlinien** aus und öffnen Sie **<Name der Richtlinie> > Optionen**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, öffnen Sie die gewünschten Einstellungen in den **Programmeinstellungen** (siehe Abschnitt "**Konfiguration von lokalen Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center**" auf S. 125).
3. Führen Sie im Abschnitt **Einstellungen** eine der folgenden Aktionen aus:
   - Wählen Sie **Benutzerrechte für die Programmverwaltung ändern** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung der Funktionen von Kaspersky Security 10.1 für Windows Server haben.
   - Wählen Sie den Punkt **Benutzerrechte für die Verwaltung von Kaspersky Security Service ändern** aus, wenn Sie die Liste der Benutzer ändern möchten, die Zugriff auf die Verwaltung des Programms mithilfe von Kaspersky Security Service haben.

     Das Gruppenfenster **Rechte für Kaspersky Security 10.1 für Windows Server** wird geöffnet.
4. Wählen Sie im folgenden Fenster in der Liste **Gruppen** oder Benutzer den Benutzer oder die Benutzergruppe aus, dessen bzw. deren Rechte Sie ändern möchten.
5. Aktivieren Sie im Block **Berechtigungen für die Gruppe „<Benutzer (Gruppe)>"** die Kontrollkästchen **Erlauben** oder **Sperren** für die folgenden Zugriffsstufen:
   - **Vollständige Kontrolle**: Uneingeschränkte Rechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server oder Kaspersky Security Service.
   - **Lesen**:
     - Folgende Rechte für die Verwaltung von Kaspersky Security 10.1 für Windows Server: **Statistik abrufen**, **Einstellungen lesen**, **Berichte lesen** und **Rechte lesen**
     - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Lesen der Einstellungen des Dienstes**, **Statusanfrage für den Dienst beim Service Control Manager**, **Statusanfrage beim Dienst**, **Abhängige Dienste auflisten**, **Rechte lesen**.

- **Änderung**:
  - Alle Rechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server mit Ausnahme von **Rechte ändern**.
  - Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Einstellungen des Dienstes anpassen, Rechte lesen**.
- **Ausführung**: Folgende Rechte für die Verwaltung von Kaspersky Security Service: **Dienst starten**, **Dienst beenden**, **Dienst anhalten/fortsetzen**, **Rechte lesen**, **Benutzeranfragen an den Dienst**.

6. Wenn Sie eine erweiterte Konfiguration der Rechte für einen Benutzer oder eine Gruppe vornehmen möchten (**Sonderrechte**), klicken Sie auf **Erweitert**.
   a. Wählen Sie im folgenden Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Security 10.1 für Windows Server** den jeweiligen Benutzer oder die jeweilige Gruppe aus.
   b. Klicken Sie auf **Ändern**.
   c. Klicken Sie im folgenden Fenster auf den Link **Sonderrechte anzeigen**.
   d. Wählen Sie in der Dropdown-Liste im oberen Fensterbereich die Art der Zugriffskontrolle aus (**Erlauben oder Verbieten**).
   e. Aktivieren Sie die Kontrollkästchen neben denjenigen Funktionen, die Sie dem betreffenden Benutzer bzw. der betreffenden Gruppe erlauben oder verbieten möchten.
   f. Klicken Sie auf **OK**.
   g. Klicken Sie im Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Security 10.1 für Windows Server** auf **OK**.
7. Klicken Sie im Gruppenfenster **Rechte für Kaspersky Security 10.1 für Windows Server** auf die Schaltfläche **Übernehmen**.

Die konfigurierten Rechte für die Verwaltung von Kaspersky Security 10.1 für Windows Server oder Kaspersky Security Service werden gespeichert.

Passwortgeschützter Zugang zu den Funktionen von Kaspersky Security 10.1 für Windows Server

Sie können den Zugriff auf die Verwaltung des Programms und der registrierten Dienste mithilfe der Einstellungen der Rechte der Benutzer (siehe Abschnitt "Über Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server" auf Seite 100) beschränken. Außerdem können Sie den Zugriff auf die Ausführung kritischer Vorgänge zusätzlich schützen, indem Sie in den Einstellungen von Kaspersky Security 10.1 für Windows Server einen Kennwortschutz einrichten.

Kaspersky Security 10.1 für Windows Server verlangt die Eingabe eines Kennworts beim Zugriff auf die folgenden Programmfunktionen:

- Verbindung zu einer lokalen Konsole für Kaspersky Security 10.1
- Deinstallation von Kaspersky Security 10.1 für Windows Server
- Änderung der Einstellungen von Kaspersky Security 10.1 für Windows Server

In der Benutzeroberfläche von Kaspersky Security 10.1 für Windows Server wird das angegebene Kennwort auf dem Bildschirm verborgen. Kaspersky Security 10.1 für Windows Server speichert das eingegebene Kennwort in Form einer Prüfsumme, die bei der Erstellung des Kennworts berechnet wird.

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

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

► *Um den Zugriff auf die Funktionen von Kaspersky Security 10.1 für Windows Server zu schützen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Server Sie die Programmeinstellungen konfigurieren möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Richtlinieneinstellungen für eine Gruppe von Servern anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie **<Name der Richtlinie> > Eigenschaften**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, öffnen Sie die gewünschten Einstellungen in den **Programmeinstellungen** (siehe Abschnitt "**Konfiguration von lokalen Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center**" auf S. 125).
3. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf die Schaltfläche **Einstellungen**.

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

   Die Felder **Kennwort** und **Kennwort bestätigen** werden aktiv.
5. Geben Sie im Feld **Kennwort** den Wert ein, den Sie für den Schutz des Zugriffes auf die Funktionen von Kaspersky Security 10.1 für Windows Server verwenden möchten.
6. Geben Sie im Feld **Kennwort bestätigen** das Kennwort erneut ein.
7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert. Kaspersky Security 10.1 für Windows Server fragt das festgelegte Kennwort beim Zugriff auf die geschützten Funktionen ab.

Das festgelegte Kennwort kann nicht wiederhergestellt werden. Wenn Sie das Kennwort verlieren, führt das zum vollständigen Verlust der Kontrolle über das Programm. Darüber hinaus kann das Programm nicht vom geschützten Server entfernt werden.

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

► *Um das festgelegte Kennwort zurückzusetzen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Server Sie die Programmeinstellungen konfigurieren möchten.

2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Um die Richtlinieneinstellungen für eine Gruppe von Servern anzupassen, wählen Sie die Registerkarte **Richtlinien** und öffnen Sie **<Name der Richtlinie> > Eigenschaften**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, öffnen Sie die gewünschten Einstellungen in den **Programmeinstellungen** (siehe Abschnitt "**Konfiguration von lokalen Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center**" auf S. 125).
3. Klicken Sie im Block **Sicherheit und Zuverlässigkeit** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Sicherheitseinstellungen** wird geöffnet.
4. Deaktivieren Sie im Block **Kennworteinstellungen** das Kontrollkästchen **Kennwortschutz verwenden**.

   Die Felder **Kennwort** und **Kennwort bestätigen** werden zurückgesetzt und deaktiviert.
5. Klicken Sie auf **OK**.

Der Kennwortschutz ist deaktiviert. Kaspersky Security 10.1 für Windows Server löscht die Prüfsumme des alten Kennworts aus den Programmeinstellungen.

Netzwerkverbindungen für den Dienst Kaspersky Security Management Service erlauben

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

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

1. Wählen Sie auf einem geschützten Server unter Microsoft Windows Server den Punkt **Start > Systemsteuerung > Sicherheit > Windows-Firewall**.
2. Wählen Sie im Fenster **Einstellungen für Windows-Firewall** den Punkt **Einstellungen ändern** aus.
3. Aktivieren Sie auf der Registerkarte **Ausnahmen** in der Liste mit vordefinierten Ausnahmen die Kontrollkästchen **COM + Netzwerkzugriff, Windows Management Instrumentation (WMI)** und **Remote Administration**.
4. Klicken Sie auf die Schaltfläche **Programm hinzufügen**.
5. Wählen Sie im Fenster **Programm hinzufügen** die Datei kavfsgt.exe aus. Diese Datei befindet sich im Ordner, den Sie bei der Installation der Konsole für Kaspersky Security 10.1 als Zielordner angegeben haben.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Einstellungen für Windows-Firewall** auf die Schaltfläche **OK**.

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

Erstellen und Einrichten von Richtlinien

Dieser Abschnitt bietet Informationen über die Anwendung der Richtlinien von Kaspersky Security Center für die Verwaltung von Aufgaben von Kaspersky Security 10.1 für Windows Server auf mehreren Servern.

In diesem Kapitel

Über Richtlinien

Sie können in Kaspersky Security Center einheitliche Richtlinien erstellen, um den Schutz auf mehreren Server zu verwalten, auf denen Kaspersky Security 10.1 für Windows Server installiert ist.

Eine Richtlinie übernimmt die in ihr eingetragenen Einstellungen, Funktionen und Aufgaben für Kaspersky Security 10.1 für Windows Server auf allen geschützten Servern 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-Bericht von Kaspersky Security 10.1 für Windows Server protokolliert. Diese Informationen stehen in der Konsole für Kaspersky Security 10.1 unter dem Knoten **Systemaudit-Bericht** zur Verfügung.

In Kaspersky Security Center existiert eine einzige Methode zur Übernahme von Richtlinien auf lokalen Computern: *Änderung von Einstellungen verbieten*. Nach der Übernahme der Richtlinie übernimmt Kaspersky Security 10.1 für Windows Server die Einstellungswerte auf den lokalen Computern, neben denen Sie in den Richtlinieneigenschaften das Symbol 🔒 gesetzt haben, anstatt der vor Übernahme der Richtlinie lokal festgelegten Einstellungswerte. Einstellungswerte der aktiven Richtlinie, neben denen in den Richtlinieneigenschaften das Zeichen 🔓 gesetzt ist, werden von Kaspersky Security 10.1 für Windows Server nicht übernommen.

Ist eine Richtlinie aktiv, so werden die Werte der Einstellungen, die in der Richtlinie mit dem Symbol 🔒 markiert sind, in der Konsole für Kaspersky Security 10.1 angezeigt, können jedoch nicht bearbeitet werden. Die Werte der restlichen Einstellungen (die in der Richtlinie mit dem Symbol 🔓 markiert sind) können in der Konsole für Kaspersky Security 10.1 bearbeitet werden.

Die in der aktiven Richtlinie festgelegten und mit dem Symbol 🔒 markierten Einstellungen blockieren auch die Bearbeitung der Einstellungen in Kaspersky Security Center für einen einzelnen Computer aus dem Fenster **Eigenschaften: <Computername>**.

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

Wenn die Richtlinie Einstellungen für eine der Aufgaben zum Echtzeitschutz oder für die Aufgaben zum Schutz für Netzwerkspeicher festlegt und diese Aufgabe ausgeführt wird, so werden die durch die Richtlinie definierten

Einstellungen sofort nach der Übernahme der Richtlinie geändert. Wenn die Aufgabe nicht ausgeführt wird, werden die Parameter aus der Richtlinie beim nächsten Aufgabenstart übernommen.

Richtlinie erstellen

Das Erstellen einer neuen Richtlinie umfasst folgende Etappen:

1. Erstellung einer Richtlinie mit dem Assistenten für die Erstellung von Richtlinien. In den Fenstern des Assistenten können Sie die Parameter für Echtzeitschutz anpassen.
2. Anpassung der Richtlinieneinstellungen. Im Fenster **Eigenschaften:<Name der Richtlinie>** der erstellten Richtlinie können Sie Folgendes anpassen: Einstellungen für den Echtzeitschutz, allgemeine Einstellungen für Kaspersky Security 10.1 für Windows Server, Einstellungen für Quarantäne und Backup-Einstellungen, Genauigkeitsstufe für Berichte über Aufgabenausführung sowie Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Security 10.1 für Windows Server.

► *Gehen Sie folgendermaßen vor, um eine Richtlinie für eine Gruppe von Servern zu erstellen, auf denen Kaspersky Security 10.1 für Windows Server installiert ist:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole den Knoten **Verwaltete Geräte** und wählen Sie anschließend die Administrationsgruppe aus, für deren Server Sie eine Richtlinie anlegen möchten.
2. Öffnen Sie im Ergebnisfenster der ausgewählten Administrationsgruppe die Registerkarte **Richtlinien** und klicken Sie dort auf den Link **Richtlinie erstellen**, um den Richtlinien-Assistenten zu öffnen.
3. Geben Sie im Fenster **Name der Gruppenrichtlinie für das Programm festlegen** im Eingabefeld **Name** einen Namen für die neue Richtlinie an. Die Namen von Richtlinien dürfen keines der folgenden Symbole enthalten: `" * < : > ? \ / |)`
4. Wählen Sie im Fenster **Programm zum Erstellen der Gruppenrichtlinie auswählen** in der Liste **Programmname** den Kaspersky Security 10.1 für Windows Server aus.
5. Wählen Sie im Fenster **Vorgangsart auswählen** eine der folgenden Optionen aus:
   - **Erstellen**, um eine neue Richtlinie mit den Standardeinstellungen für neue Richtlinien zu erstellen.
   - **Richtlinie importieren, die mit einer früheren Version von Kaspersky Security für Windows Server** erstellt wurde, um die Richtlinie dieser Version als Vorlage zu verwenden.

     Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie die Konfigurationsdatei aus, in der Sie die vorhandene Richtlinie gespeichert haben.
6. Passen Sie im Fenster **Echtzeitschutz** bei Bedarf die Einstellungen der Aufgaben Echtzeitschutz für Dateien und die Verwendung von KSN Ihren Bedürfnissen entsprechend an. Erlauben oder verbieten Sie die Übernahme konfigurierter Aufgaben in der Richtlinie in den lokalen Computernetzwerken:
   - Klicken Sie auf 🔒, um die Konfiguration der Einstellungen einer Aufgabe auf den Computern des Netzwerks zu erlauben und die Übernahme der in der Richtlinie konfigurierten Aufgabeneinstellungen zu verbieten.
   - Klicken Sie auf 🔓, um die Konfiguration der Einstellungen einer Aufgabe auf den Computern des Netzwerks zu verbieten und die Übernahme der in der Richtlinie konfigurierten Aufgabeneinstellungen zu erlauben.

   In neu erstellten Richtlinien gelten für die Parameter der Aufgaben zum Echtzeitschutz die Standardeinstellungen.

- Wenn Sie die standardmäßig festgelegten Einstellungen der Aufgabe Echtzeitschutz für Dateien ändern möchten, klicken Sie im Block **Echtzeitschutz für Dateien** auf **Einstellungen**. Passen Sie im erscheinenden Fenster **Einstellungen** 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 Block **Verwendung von KSN**. Passen Sie im erscheinenden Fenster **Einstellungen** die Aufgabeneinstellungen Ihren Bedürfnissen entsprechend an. Klicken Sie auf **OK**.

Die Aufgabe Verwendung von KSN steht dann zur Verfügung, wenn die KSN-Erklärung akzeptiert wurde.

7. Wählen Sie im Fenster **Gruppenrichtlinie für das Programme erstellen** eine der folgenden Statusvarianten für die Richtlinie aus:
   - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie sofort nach dem Erstellen in Kraft tritt. Wenn in der Gruppe bereits eine aktive Richtlinie existiert, dann wird diese existierende Richtlinie außer Kraft treten, und die neu erstellte wird zur aktiven Richtlinie.
   - **Inaktive Richtlinie**, wenn Sie nicht möchten, dass die Richtlinie sofort angewendet wird. Sie können diese Richtlinie später aktivieren.
8. Im Fenster **Beenden** klicken Sie auf die Schaltfläche **Fertig**.

Die erstellte Richtlinie wird in der Richtlinienliste auf der Registerkarte **Richtlinien** der ausgewählten Administrationsgruppe angezeigt. Im Fenster **Eigenschaften: <Name der Richtlinie>** können Sie andere Einstellungen, Aufgaben und Funktionen von Kaspersky Security 10.1 für Windows Server anpassen.

Richtlinie anpassen

Im Fenster **Eigenschaften:<Name der Richtlinie>** einer vorhandenen Richtlinie können Sie folgende Einstellungen anpassen: allgemeine Einstellungen von Kaspersky Security 10.1 für Windows Server, Einstellungen für Quarantäne und Backup-Einstellungen, Einstellungen für die vertrauenswürdige Zone, Einstellungen für den Echtzeitschutz, Überwachung der Server-Aktivitäten, Genauigkeitsstufe für Berichte über Aufgabenausführung, Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Security 10.1 für Windows Server, Zugriffsrechte für die Verwaltung des Programms und von Kaspersky Security Service, Einstellungen für die Übernahme von Richtlinienprofilen.

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

1. Erweitern Sie den Knoten **Verwaltete Geräte** in der Struktur der Verwaltungskonsole von Kaspersky Security Center.
2. Erweitern Sie die Administrationsgruppe, für die Sie die zugehörigen Richtlinieneinstellungen anpassen möchten, und öffnen Sie den untergeordneten Knoten **Richtlinien** im Ergebnisfenster.
3. Wählen Sie eine Richtlinie, die Sie anpassen möchten, und öffnen Sie das Fenster **Eigenschaften: <Name der Richtlinie>** auf eine der folgenden Arten:
   - Wählen Sie im Kontextmenü der Richtlinie die Option **Eigenschaften** aus.
   - Klicken Sie im rechten Ergebnisbereich der ausgewählten Richtlinie auf den Link **Richtlinie anpassen**.
   - Doppelklicken Sie auf die ausgewählte Richtlinie.

4. Aktivieren oder deaktivieren Sie auf der Registerkarte **Allgemein** im Block **Richtlinienstatus** die Richtlinie. Wählen Sie dazu eine der folgenden Varianten:

   - **Aktive Richtlinie**, wenn Sie möchten, dass die Richtlinie auf allen Servern übernommen wird, die zur ausgewählten Administrationsgruppe gehören.
   - **Inaktive Richtlinie**, wenn Sie nicht möchten, dass die Richtlinie auf allen Servern übernommen wird, die zur ausgewählten Gruppe gehören.

   Die Option **Richtlinie für autonome Benutzer** ist bei der Verwendung von Kaspersky Security 10.1 für Windows Server nicht verfügbar.

5. Konfigurieren Sie in den Abschnitten **Benachrichtigung über Ereignisse**, **Programmeinstellungen**, **Berichte und Benachrichtigungen**, **Zusätzlich** und **Revisionsverlauf** die allgemeinen Einstellungen der Programmausführung (s. Tabelle unten).
6. Konfigurieren Sie in den Abschnitten **Echtzeitschutz**, **Überwachung der Server-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 Servern, die zu einer Administrationsgruppe gehören, mithilfe einer Richtlinie von Kaspersky Security Center aktivieren und deaktivieren.
   Sie können die Übernahme der in der Richtlinie festgelegten Einstellungen auf allen Computern des Netzwerks für jede einzelne Programmkomponente festlegen.

7. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen werden in der Richtlinie übernommen.

Eine Anleitung für die Konfiguration der Aufgaben und Programmfunktionen in der Konsole für Kaspersky Security 10.1 finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

Abschnitte mit Richtlinieneinstellungen für Kaspersky Security 10.1 für Windows Server

Allgemein

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

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

Ereignisbenachrichtigungen

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

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

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

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

Programmeinstellungen

Tabelle 19. Einstellungen des Abschnitts "Programmeinstellungen"

Abschnitt	Einstellungen
Skalierbarkeit und Oberfläche	Im Block **Skalierbarkeit und Oberfläche** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Auswahl der automatischen oder manuellen Konfiguration der Skalierbarkeitseinstellungen • Einstellungen für die Anzeige des Programmsymbols
Sicherheit	Im Block **Sicherheit** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Einstellungen der Aufgabenausführung anpassen • Aktionen des Programms beim Wechsel des Servers in den USV-Akkubetrieb angeben • Kennwortschutz der Programmfunktionen aktivieren und deaktivieren
Verbindungen	Im Block **Verbindungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Proxyserver-Einstellungen für die Verbindung mit den Update-Servern, den Aktivierungsservern und KSN konfigurieren: • Festlegung der Proxyserver-Einstellungen • Geben Sie die Einstellungen für die Authentifizierung auf dem Proxyserver an.
Start von Systemaufgaben	Im Abschnitt **Start von Systemaufgaben** können Sie über die Schaltfläche **Einstellungen** den Start der folgenden Systemaufgaben nach einem auf den lokalen Computern festgelegten Zeitplan erlauben oder verbieten: • Aufgabe zur Untersuchung auf Befehl • Update-Aufgabe und Aufgabe zur Update-Verteilung

Zusätzlich

Tabelle 20. Einstellungen des Abschnitts "Zusätzlich"

Abschnitt	Einstellungen
Vertrauenswürdige Zone	Im Block **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 Block **Untersuchung von Wechseldatenträgern** können Sie über die Schaltfläche **Einstellungen** die Untersuchungseinstellungen für USB-Wechseldatenträger anpassen.
Benutzerrechte für die Programmverwaltung	Im Block **Benutzerrechte für die Programmverwaltung** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Security 10.1 für Windows Server anpassen.
Benutzerrechte für die Verwaltung von Security Service	Im Block **Benutzerrechte für die Verwaltung von Security Service** können Sie die Zugriffsrechte und Gruppenzugriffsrechte für die Verwaltung von Kaspersky Security Service anpassen.
Speicher	Im Block **Speicher** können Sie über die Schaltfläche **Einstellungen** folgende Einstellungen für Quarantäne, Backup und blockierte Geräte 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 • Anpassen der Einstellungen für die Computersperrung

Echtzeitschutz

Tabelle 21. Einstellungen des Abschnitts "Echtzeitschutz"

Abschnitt	Einstellungen
Echtzeitschutz für Dateien	Im Block **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 Block **Verwendung von KSN** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Aktionen für Objekte, die in KSN nicht vertrauenswürdig sind, angeben • Leistung der Aufgabe anpassen • Einstellungen für die Verwendung von Kaspersky Security Center als KSN-Proxyserver anpassen • KSN-Erklärung akzeptieren • Einstellungen für den Aufgabenstart festlegen
Exploit-Prävention	Im Block **Exploit-Prävention** können Sie über die Schaltfläche **Einstellungen** die folgenden Parameter für die Aufgabenausführung konfigurieren: • Schutzmodus des Prozess-Arbeitsspeichers auswählen • Aktionen zur Minderung des Exploit-Risikos angeben • Liste der geschützten Prozesse ergänzen und bearbeiten
Skript-Untersuchung	In der Aufgabe **Skript-Untersuchung** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Ausführen von potentiell gefährlichen Skripten erlauben oder sperren • Verwendung der heuristischen Analyse anpassen • Verwendung der vertrauenswürdigen Zone anpassen • Einstellungen der Aufgabenausführung anpassen

Überwachung der Server-Aktivitäten

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

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

Netzwerküberwachung

Tabelle 23. Einstellungen des Blocks "Netzwerküberwachung"

Abschnitt	Einstellungen
Firewall-Verwaltung	Im Block **Firewall-Verwaltung** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Firewall-Regeln anpassen • Einstellungen für den Aufgabenstart festlegen
Schutz vor Verschlüsselung	Im Block **Schutz vor Verschlüsselung** können Sie über die Schaltfläche **Einstellungen** die folgenden Aufgabeneinstellungen anpassen: • Schutzbereich für den Schutz vor Verschlüsselung angeben • Einstellungen für den Aufgabenstart festlegen

System-Diagnose

Tabelle 24. Einstellungen des Abschnitts "System-Diagnose"

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

Berichte und Benachrichtigungen

Tabelle 25. Einstellungen des Abschnitts "Berichte und Benachrichtigungen"

Abschnitt	Einstellungen
Berichte über Aufgabenausführung	Im Block **Berichte über Aufgabenausführung** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Ereigniskategorie protokollierter Ereignisse für die ausgewählten Programmkomponenten angeben • Speicherdauer für Berichte über Aufgabenausführung festlegen • Konfiguration der SIEM-Integration in Kaspersky Security Center.
Ereignisbenachrichtigungen	Im Block **Ereignisbenachrichtigungen** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Benachrichtigung der Benutzer über das Ereignis *Objekt gefunden* • Benachrichtigung des Administrators über ein beliebiges ausgewähltes Ereignis aus der Liste der Ereignisse im Block **Benachrichtigungen anpassen**
Interaktion mit dem Administrationsserver	Im Block **Interaktion mit dem Administrationsserver** können Sie über die Schaltfläche **Einstellungen** die Typen der Objekte auswählen, über die Kaspersky Security 10.1 für Windows Server Informationen an den Administrationsserver übergeben soll.

Schutz für Netzwerkspeicher

Tabelle 26. Einstellungen des Abschnitts "Schutz für Netzwerkspeicher"

Abschnitt	Einstellungen
Echtzeitschutz für Dateien (RPC)	Im Block **Echtzeitschutz für Dateien (RPC)** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Verwendung der heuristischen Analyse • Einstellungen für die Verbindung mit einem Netzwerkspeicher • Schutzbereich
Echtzeitschutz für Dateien (ICAP)	Im Block **Echtzeitschutz für Dateien (ICAP)** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Einstellungen für die Verbindung mit dem ICAP-Dienst • Integration mit anderen Komponenten • Sicherheitsstufe
Anti-Cryptor für NetApp	Im Block **Anti-Cryptor für NetApp** können Sie über die Schaltfläche **Einstellungen** die folgenden Einstellungen anpassen: • Aufgabenmodus • Verwendung der heuristischen Analyse • Einstellungen für die Verbindung und Authentifizierung • Festlegen von Ausnahmen aus dem Schutzbereich

Ausführliche Informationen über die Aufgaben "Schutz für Netzwerkspeicher" finden Sie im *Implementierungshandbuch zum Schutz für ins Netzwerk eingebundene Speicher für Kaspersky Security 10.1 für Windows Server*.

Revisionsverlauf

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

Zeitplan für den Start von lokalen Systemaufgaben anpassen

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

- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie verboten ist, werden solche Aufgaben nicht auf dem lokalen Computer nach Zeitplan ausgeführt. Sie können lokale Systemaufgaben manuell starten.
- Wenn der Start nach Zeitplan für lokale Systemaufgaben vom festgelegten Typ in einer Richtlinie erlaubt ist, werden solche Aufgaben gemäß den lokal für diese Aufgabe angepassten Zeitplan-Einstellungen ausgeführt.

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

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

Wenn Sie keine Gruppenaufgaben für Updates oder Untersuchungen auf Befehl verwenden, erlauben Sie den Start lokaler Systemaufgaben in einer Richtlinie: Kaspersky Security 10.1 für Windows Server wird Updates der Datenbanken und Programm-Module ausführen und alle lokalen Systemaufgaben zur Untersuchung auf Befehl gemäß den standardmäßigen Zeitplan-Einstellungen starten.

Mithilfe von Richtlinien können Sie den Start folgender lokaler Systemaufgaben nach Zeitplan erlauben oder verbieten:

- Aufgabe zur Untersuchung auf Befehl: Untersuchung wichtiger Bereiche, Untersuchung von Quarantäne-Objekten, Untersuchung beim Hochfahren des Betriebssystems, Integritätsprüfung für Programm-Module
- Aufgaben zum Update: Update der Programm-Datenbanken, Update der Programm-Module und Update-Verteilung.

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

► *Gehen Sie wie folgt vor, um den Start der Systemaufgaben von Kaspersky Security 10.1 für Windows Server nach Zeitplan in einer Richtlinie zu erlauben oder zu verbieten:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole den Knoten **Verwaltete Geräte**, klappen Sie die entsprechende Gruppe auf und öffnen Sie im Ergebnisfenster die Registerkarte **Richtlinien**.
2. Wählen Sie auf der Registerkarte **Richtlinie** im Kontextmenü der Richtlinie, mit deren Hilfe Sie den geplanten Start von Systemaufgaben für Kaspersky Security 10.1 für Windows Server auf der Servergruppe konfigurieren möchten, den Befehl **Eigenschaften**.
3. Öffnen Sie im Fenster **Eigenschaften: <Name der Richtlinie>** den Abschnitt **Eigenschaften des Programms**. Klicken Sie im Block **Start von Systemaufgaben** auf die Schaltfläche **Einstellungen** und gehen Sie wie folgt vor:
   - Aktivieren Sie die Kontrollkästchen **Start von Aufgaben zur Untersuchung auf Befehl zulassen** und **Start von Aufgaben zum Update und zur Update-Verteilung zulassen**, um den Start der angeführten Aufgaben nach Zeitplan zu erlauben.
   - Deaktivieren Sie die Kontrollkästchen **Start von Aufgaben zur Untersuchung auf Befehl zulassen** und **Start von Aufgaben zum Update und zur Update-Verteilung zulassen**, um den Start der angeführten Aufgaben nach Zeitplan zu verbieten.

   Das Aktivieren oder Deaktivieren der Kontrollkästchen beeinflusst nicht die Starteinstellungen der lokalen benutzerdefinierten Aufgaben des angegebenen Typs.
4. Vergewissern Sie sich, dass die Richtlinie (siehe Abschnitt "Über Richtlinien" auf Seite 109), die Sie anpassen, aktiv ist und für die Gruppe der Administrationsserver übernommen wurde.
5. Klicken Sie auf **OK**.

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

Erstellung und Konfiguration von Aufgaben in Kaspersky Security Center

Dieser Abschnitt enthält Informationen über Aufgaben von Kaspersky Security 10.1 für Windows Server, ihre Erstellung, die Konfiguration ihrer Ausführung sowie über den Start/die Beendigung von Aufgaben.

In diesem Kapitel

Über die Erstellung von Aufgaben in Kaspersky Security Center

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

- Programm aktivieren
- Update-Verteilung
- Update der Programm-Datenbanken
- Update der Programm-Module
- Rollback des Datenbanken-Updates
- Untersuchung auf Befehl
- Integritätsprüfung für Programme
- Automatisches Erstellen von Erlaubnisregeln
- Erstellen von Regeln für die Gerätekontrolle

Sie können lokale Aufgaben und Gruppenaufgaben auf folgende Art und Weise erstellen:

- Für einen Computer: im Fenster **Eigenschaften <Computername>** im Block Aufgaben
- Für eine Administrationsgruppe: im Ergebnisbereich des Knotens der ausgewählten Computergruppe auf der Registerkarte **Aufgaben**
- Für eine Auswahl an Computern: im Ergebnisbereich des Knotens **Geräteauswahl**

Mithilfe von Richtlinien können Sie Zeitpläne für lokale Systemaufgaben zum Update und zur Untersuchung auf Befehl (siehe Abschnitt "Zeitgesteuerten Start für lokale Systemaufgaben konfigurieren" auf Seite 118) auf allen geschützten Servern aus derselben Administrationsgruppe deaktivieren.

Allgemeine Informationen über den Aufgaben in Kaspersky Security Center sind im *Hilfesystem von Kaspersky Security Center* zu finden.

Aufgabe mithilfe von Kaspersky Security Center erstellen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

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

1. Starten Sie den Assistenten für neue Aufgaben nach einer der folgenden Methoden:
   - Für das Erstellen einer lokalen Aufgabe:
     a. Erweitern Sie in der Struktur des Administrationsservers von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, zu der der geschützte Server gehört.
     b. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Geräte** das Kontextmenü für die Zeile mit Informationen über den geschützten Server und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im erscheinenden Fenster im Abschnitt **Aufgaben** auf **Hinzufügen**.
   - Für das Erstellen einer Gruppenaufgabe:
     a. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, für die Sie eine Aufgabe erstellen möchten.
     b. Öffnen Sie im Ergebnisfenster das Kontextmenü auf der Registerkarte **Aufgaben** und wählen Sie den Punkt **Erstellen** > **Aufgabe**.
   - Um eine Aufgabe für eine beliebige Auswahl an Computern zu erstellen, öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center den Knoten **Geräteauswahl** und wählen Sie den Punkt **Aufgabe erstellen** aus.

   Darauf öffnet sich der Assistent für neue Aufgaben.
2. Geben Sie im Fenster **Aufgabenname festlegen** einen Aufgabennamen an (maximal 100 Zeichen, wobei folgende Zeichen unzulässig sind: *** < > ? \ / | : "**). Es wird empfohlen, den Aufgabentyp im Namen anzugeben (z. B. "Untersuchung auf Befehl der freigegebenen Ordner").
3. Wählen Sie im Fenster **Aufgabentyp** unter der Überschrift **Kaspersky Security 10.1 für Windows Server** den Typ der zu erstellenden Aufgabe aus.

4. Wenn Sie einen anderen Aufgabentyp als Rollback des Datenbanken-Updates oder Programmaktivierung ausgewählt haben, wird das Fenster **Aufgabeneinstellungen** geöffnet. Je nach Typ der zu erstellenden Aufgabe führen Sie eine der folgenden Aktionen aus:

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

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

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

        Sie können den Untersuchungsbereich ändern: Einzelne vordefinierte Bereiche, Datenträger, Ordner, Netzwerkobjekte oder Dateien in den Untersuchungsbereich aufnehmen und individuelle Sicherheitseinstellungen für die hinzugefügten Bereiche festlegen.

     - Um alle wichtigen Untersuchungsbereiche von der Untersuchung auszuschließen, öffnen Sie nacheinander für jede einzelne Zeile das Kontextmenü und wählen Sie **Bereich löschen**.
     - Um vordefinierte Bereiche, Festplatten, Ordner, Netzwerkobjekte oder Dateien zum Untersuchungsbereich hinzuzufügen, klicken Sie mit der rechten Maustaste auf die Tabelle **Untersuchungsbereich** und wählen Sie Bereich hinzufügen. Wählen Sie im Fenster **Zum Untersuchungsbereich hinzufügen** entweder einen vordefinierten Bereich aus der Liste **Vordefinierter Bereich** aus oder geben Sie eine Festplatte des Computers, einen Ordner, ein Netzwerkobjekt oder eine Datei auf dem Server oder auf einem anderen Computer im Netzwerk an und klicken Sie dann auf **OK**.
     - Um untergeordnete Ordner oder Dateien von der Untersuchung auszuschließen, wählen Sie den hinzugefügten Ordner (die hinzugefügte Festplatte) im Fenster **Untersuchungsbereich** des Assistenten aus, öffnen Sie das Kontextmenü und wählen Sie die Option **Anpassen**. Klicken Sie dann im Fenster Sicherheitsstufe auf **Einstellungen** und deaktivieren Sie im Fenster **Untersuchung auf Befehl** auf der Registerkarte **Allgemein** die Kontrollkästchen **Untergeordnete Ordner** und **Dateien**.
     - Um die Sicherheitseinstellungen für den Untersuchungsbereich zu ändern, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Bereich, dessen Parameter Sie ändern wollen, und wählen Sie **Anpassen**. Wählen Sie im Fenster **Untersuchung auf Befehl** eine der vordefinierten Sicherheitsstufen aus oder klicken Sie auf die Schaltfläche Einstellungen, um die Sicherheitseinstellungen manuell anzupassen. Das Anpassen der Sicherheitseinstellungen wird genauso wie in der Konsole für Kaspersky Security 10.1 durchgeführt.
     - Um eingebettete Objekte aus einem hinzugefügten Untersuchungsbereich auszuschließen, öffnen Sie das Kontextmenü in der Tabelle **Untersuchungsbereich**, klicken Sie auf **Ausnahme hinzufügen** und geben Sie die auszuschließenden Objekte an: Wählen Sie in der Liste Vordefinierter Bereich einen vordefinierten Bereich aus, geben Sie einen Datenträger des Servers, einen Ordner oder eine Datei auf dem Server oder auf einem anderen Computer im Netzwerk an. Klicken Sie dann auf **OK**.
     - Bereiche, die vom Untersuchungsbereich ausgenommen sind, werden in der Tabelle mit dem Symbol ☐ markiert.

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

        Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie Objekte, die in der vertrauenswürdigen Zone von Kaspersky Security 10.1 für Windows Server beschrieben werden, vom Untersuchungsbereich der Aufgabe ausschließen wollen.

        Wenn Sie planen, die zu erstellende Aufgabe als Untersuchung wichtiger Bereiche zu verwenden, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**. Das Programm Kaspersky Security Center berücksichtigt bei der Bewertung des Sicherheitsstatus des Servers (bzw. der Server) die Ergebnisse der Ausführung von Aufgaben

mit dem Status *Aufgabe zur Untersuchung wichtiger Bereiche*, und nicht nur die Ergebnisse der Systemaufgabe **Untersuchung wichtiger Bereiche**. Bei der Erstellung einer lokalen Aufgabe zur Untersuchung auf Befehl ist das Kontrollkästchen nicht verfügbar.

Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Basispriorität **Niedrig** zuzuweisen, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**. Arbeitsprozesse, in denen Aufgaben für Kaspersky Security 10.1 für Windows Server ausgeführt werden, haben standardmäßig die Priorität **Mittel** (Normal). Wenn die Priorität eines Prozesses gesenkt wird, erhöht sich dadurch die Ausführungsdauer der Aufgabe und die Ausführungsgeschwindigkeit der Prozesse anderer aktiver Anwendungen wird gesteigert.

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

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

  b. Klicken Sie auf **LAN-Einstellungen**. Das Fenster **Verbindungseinstellungen** wird geöffnet.

  c. Gehen Sie auf der Registerkarte **Verbindungseinstellungen** wie folgt vor:

  Geben Sie den Modus des FTP-Servers für die Verbindung mit einem geschützten Server 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 Server(s) an, um den Update-Download zu optimieren.

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

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

  b. Wenn Sie **Wichtige Updates der Programm-Module verteilen und installieren** ausgewählt haben, kann zum Übernehmen der installierten Programm-Module ein Neustart des Servers erforderlich sein. Damit Kaspersky Security 10.1 für Windows Server den Computer nach Abschluss der Aufgabe automatisch neu startet, aktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**. Um den Neustart des Servers nach Abschluss der Aufgabe zu verhindern, deaktivieren Sie das Kontrollkästchen **Neustart des Betriebssystems zulassen**.

  c. Wenn Sie Informationen über Upgrades der Module von Kaspersky Security 10.1 für Windows Server erhalten möchten, aktivieren Sie das Kontrollkästchen **Über verfügbare planmäßige Updates der Programm-Module informieren**.

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

- *Wenn Sie die Aufgabe Update-Verteilung erstellen*, geben Sie im Fenster **Einstellungen für die Update-Verteilung** die Zusammensetzung der Updates und den Ordner der lokalen Update-Quelle an, in der das Update gespeichert wird.

- *Wenn Sie die Aufgabe Programmaktivierung erstellen*, verwenden Sie im Fenster **Aktivierungsparameter** die Schlüsseldatei oder den Aktivierungscode, mit deren bzw. dessen Hilfe Sie

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

- *Wenn Sie die Aufgabe "Automatisches Erstellen von Erlaubnisregeln" oder die Aufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellen*, geben Sie im Fenster **Einstellungen** die Parameter an, auf deren Grundlage die Liste der Erlaubnisregeln erstellt wird:

  a. Geben Sie den Präfix für die Namen der Regeln an (nur für die Aufgabe "Automatisches Erstellen von Erlaubnisregeln").

  b. Passen Sie die Einstellungen des Gültigkeitsbereichs der Erlaubnisregeln mit dem Status "erlaubt" (nur für die Aufgabe "Automatisches Erstellen von Erlaubnisregeln") an. Klicken Sie auf **Weiter**.

  c. Legen Sie die Aktionen fest, die die Aufgabe während der Erstellung von Erlaubnisregeln (nur für die Aufgabe "Automatisches Erstellen von Erlaubnisregeln") und nach ihrem Abschluss ausführen soll.

5. Passen Sie die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen). Gehen Sie im Fenster **Zeitplan** wie folgt vor:

   a. Um den Zeitplan zu aktivieren, aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.

   b. Legen Sie eine Frequenz für den Aufgabenstart fest: Wählen Sie in der Liste **Startintervall** einen der folgenden Werte aus: **Stündlich**, **Täglich**, **Wöchentlich**, **Bei Programmstart**, **Nach dem Update der Programm-Datenbanken** (in den Gruppenaufgaben "Update der Programm-Datenbanken", "Update der Programm-Module" können Sie zusätzlich die Frequenz **Nach Update-Download durch den Administrationsserver** angeben):

      - Wenn Sie **Stündlich** gewählt haben, geben Sie in der Optionsgruppe **Einstellungen für den Aufgabenstart** im Feld Alle **<Anzahl> Stunde(n)** die Anzahl der Stunden an.
      - Wenn Sie **Täglich** gewählt haben, geben Sie in der Optionsgruppe **Einstellungen für den Aufgabenstart** im Feld Alle **<Anzahl> Tag(e)** die Anzahl der Tage an.
      - Wenn Sie **Wöchentlich** gewählt haben, geben Sie in der Optionsgruppe **Einstellungen für den Aufgabenstart** im Feld **Alle <Anzahl> Woche(n)** die Anzahl der Wochen an. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet wird (standardmäßig wird eine Aufgabe montags gestartet).

   c. Geben Sie im Feld **Startzeit** die Startzeit der Aufgabe ein, und geben Sie im Feld **Beginnen am** das Datum, an dem der Zeitplan in Kraft tritt.

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

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

Aktivieren Sie das Kontrollkästchen **Startzeit für Aufgaben verteilen auf ein Intervall von** und geben Sie einen Wert in Minuten an.

e. Klicken Sie auf **OK**.

6. Wenn die zu erstellende Aufgabe eine Aufgabe für eine zufällige Zusammenstellung von Computern ist, wählen Sie die Netzwerkcomputer (Gruppen) aus, an denen die Aufgabe ausgeführt werden soll.
7. Legen Sie im Fenster **Benutzerkonto für den Aufgabenstart auswählen** das Benutzerkonto fest, mit dessen Rechten Sie die Aufgabe ausführen möchten.
8. Aktivieren Sie im Fenster **Erstellung der Aufgabe fertig stellen** das Kontrollkästchen **Aufgabe nach Abschluss des Assistenten starten**, wenn Sie möchten, dass die Aufgabe nach ihrer Erstellung gestartet wird. Klicken Sie auf **Fertig**.

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

Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen

► *Um lokale Aufgaben oder allgemeine Programmeinstellungen im Fenster Programmeinstellungen für einen einzelnen Server im Netzwerk anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur des Administrationsservers von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Geräte** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Computername>** zu öffnen:
   - Doppelklicken Sie auf den Namen des geschützten Servers.
   - Öffnen Sie das Kontextmenü für den Namen des geschützten Servers und wählen Sie den Punkt **Eigenschaften**.

   Das Fenster **Eigenschaften: <Computername>** wird geöffnet.
4. Um die lokalen Aufgabeneinstellungen anzupassen, gehen Sie wie folgt vor:
   a. Wechseln Sie in den Abschnitt **Aufgaben**.
      - Wählen Sie in der Aufgabenliste die lokale Aufgabe aus, deren Einstellungen Sie anpassen möchten.
      - Doppelklicken Sie den Aufgabennamen in der Liste der Aufgaben.
      - Wählen Sie den Aufgabennamen aus und klicken Sie auf die Schaltfläche **Eigenschaften**.
      - Anschließend wählen Sie den Punkt **Eigenschaften** im Kontextmenü der ausgewählten Aufgabe.
5. Um die Programmeinstellungen anzupassen, gehen Sie wie folgt vor:
   a. Wechseln Sie zum Block **Programme**.
      - Wählen Sie in der Liste der installierten Programme das Programm aus, das Sie anpassen möchten.
      - Doppelklicken Sie in der Liste der installierten Programme auf den Programmnamen.
      - Wählen Sie den Programmnamen in der Liste der installierten Programme aus und klicken Sie

auf die Schaltfläche **Eigenschaften**.

- Öffnen Sie in der Liste der installierten Programme das Kontextmenü für den Programmnamen und wählen Sie den Punkt **Eigenschaften**.

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

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

Gruppenaufgaben in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen anpassen möchten.
2. Öffnen Sie im Ergebnisbereich der ausgewählten Administrationsgruppe die Registerkarte **Aufgaben**.
3. Wählen Sie in der Liste der bereits erstellten Gruppenaufgaben diejenige Aufgabe aus, deren Einstellungen Sie anpassen möchten. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen: <Aufgabenname>** zu öffnen:
   - Doppelklicken Sie in der Liste der erstellten Aufgaben auf den Aufgabennamen.
   - Markieren Sie den Aufgabennamen in der Liste der erstellten Aufgaben und betätigen Sie den Link **Aufgabeneinstellungen ändern**
   - Öffnen Sie in der Liste der erstellten Aufgaben das Kontextmenü für den Aufgabennamen und wählen Sie den Punkt **Eigenschaften**.
4. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.

Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

5. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie eine Aufgabe zur Untersuchung auf Befehl konfigurieren:
     a. Legen Sie im Abschnitt **Einstellungen** den Untersuchungsbereich fest.
     b. Konfigurieren Sie im Abschnitt **Einstellungen** die Integration in andere Programmkomponenten sowie die Aufgabenpriorität.
   - Wenn Sie eine der Update-Aufgaben konfigurieren, aktivieren Sie die gewünschten Aufgabenparameter nach Ihren Bedürfnissen:
     a. Passen Sie im Block **Update-Quelle** die Einstellungen für die Update-Quelle an und optimieren Sie die Nutzung des Laufwerk-Subsystems.
     b. Konfigurieren Sie über die Schaltfläche **Verbindungseinstellungen** die allgemeinen Verbindungseinstellungen sowie die Einstellungen für die Verbindungsaufnahme mit der Update-Quelle.
   - Wenn Sie die Aufgabe "Update der Programm-Module" anpassen, wählen Sie im Abschnitt **Einstellungen für das Update der Programm-Module anpassen** die Aktion aus, die ausgeführt werden soll: wichtige Updates der Programm-Module kopieren und installieren oder nur auf Vorhandensein prüfen.
   - Wenn Sie die Aufgabe Update-Verteilung konfigurieren, geben Sie im Abschnitt **Einstellungen für die Update-Verteilung** die Zusammensetzung der Updates und den Ordner der lokalen Update-Quelle an, in der die Updates gespeichert werden sollen.
   - Wenn Sie die Aufgabe **Programm aktivieren** konfigurieren, verwenden Sie im Block **Aktivierungsparameter** die Schlüsseldatei oder den Aktivierungscode, mit deren bzw. dessen Hilfe Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen Als Reserve-Aktivierungscode oder Reserveschlüssel verwenden, wenn Sie einen Aktivierungscode oder einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.
   - Wenn Sie die Aufgabe Erstellen von Regeln für die Kontrolle des Programmstart für die Server-Kontrolle anpassen, geben Sie im Abschnitt **Einstellungen** die Einstellungen an, auf deren Grundlage die Liste der Erlaubnisregeln erstellt werden soll.
6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
8. Geben Sie bei Bedarf im Abschnitt **Ausnahmen vom Gültigkeitsbereich** der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
9. Klicken Sie im Fenster **Eigenschaften <Name der Aufgabe>** auf **OK**.

Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

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

Tabelle 27. Einstellungen für Gruppenaufgaben in Kaspersky Security 10.1 für Windows Server

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
Automatisches Erstellen von Regeln (Aufgabe "Automatisches Erstellen von Erlaubnisregeln" und Aufgabe "Erstellen von Regeln für die Gerätekontrolle").	**Einstellungen**	Beim Anpassen der Einstellungen der Aufgabe "Automatisches Erstellen von Erlaubnisregeln" können Sie: • den Schutzbereich ändern, indem Sie Ordnerpfade und Dateitypen hinzufügen oder löschen und Dateitypen angeben, für die der Start durch automatisch erstellte Regeln erlaubt ist. • gestartete Programme berücksichtigen oder nicht berücksichtigen.
	Einstellungen	Sie können Aktionen festlegen, die bei der Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen: • **Digitales Zertifikat verwenden** Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts das Vorhandensein eines digitalen Zertifikats als Auslösekriterium für die Regel angegeben. Anschließend erlaubt das Programm den Start von Programmen mithilfe von Dateien, die über ein digitales Zertifikat verfügen. Diese Option empfiehlt sich, wenn Sie den Start beliebiger Programme erlauben möchten, die im Betriebssystem als vertrauenswürdig eingestuft sind. • **Header und Fingerabdruck des digitalen Zertifikats verwenden** Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers und des Fingerabdrucks des digitalen Zertifikats der Datei als Auslösekriterium für die Erlaubnisregeln für die Kontrolle des Programmstarts. Die Aktivierung dieses Kontrollkästchens ermöglicht die Festlegung strengerer Bedingungen für die Untersuchung digitaler Zertifikate.

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
		Ist das Kontrollkästchen aktiviert, werden die Werte des Headers und des Fingerabdrucks des digitalen Zertifikats der Dateien, für welche die Regeln erstellt werden, als Kriterium für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts festgelegt. Kaspersky Security 10.1 für Windows Server erlaubt Programme, die mithilfe von Dateien mit einem angegebenen Fingerabdruck: und Header gestartet werden. Die Verwendung dieses Kontrollkästchens stellt die strengste Einschränkung für das Auslösen von Erlaubnisregeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles fälschungssicheres Identifikationsmerkmal eines digitalen Zertifikats handelt. Ist das Kontrollkästchen deaktiviert, so wird als Kriterium für das Auslösen der Erlaubnisregeln zur Kontrolle des Programmstarts das Vorliegen eines beliebigen digitalen Zertifikats festgelegt, das im Betriebssystem als vertrauenswürdig eingestuft ist. Das Kontrollkästchen ist aktiv, wenn die Option **Digitales Zertifikat verwenden** ausgewählt ist. Das Kontrollkästchen ist in der Grundeinstellung aktiviert. • **Falls kein Zertifikat vorhanden, Folgendes verwenden** Dropdown-Liste, welche die Auswahl der Kriterien für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts für den Fall erlaubt, dass die Datei, auf deren Grundlage die Regel erstellt wird, über kein digitales Zertifikat verfügt. • **SHA256-Hash verwenden** Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts die Prüfsumme der Datei, auf deren Grundlage die Regel erstellt wird, als Auslösekriterium für die Regel angegeben. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit den angegebenen Werten der Prüfsumme. Diese Option wird empfohlen, wenn maximal

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
		sichere Regeln erstellt werden müssen: Die Prüfsumme, die nach dem Algorithmus SHA256 berechnet wird, ist eine eindeutige ID der Datei. Die Verwendung der erhaltenen SHA256-Prüfsumme als Auslösekriterium für die Regel engt den Gültigkeitsbereich der Regel bis auf eine Datei ein. Diese Variante gilt als Standard.
		• **Regeln für Benutzer oder Benutzergruppe erstellen** Feld, in dem der Benutzer und/oder die Benutzergruppe angegeben sind. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer und/oder die angegebene Benutzergruppe. Standardmäßig ist die Gruppe **Alle** eingestellt. Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen, die von Kaspersky Security 10.1 für Windows Server nach Abschluss der Aufgaben erstellt werden.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Programm aktivieren	**Programmeinstel-lungen**	Sie können für die Programmaktivierung oder für die Verlängerung der Lizenzlaufzeit einen Aktivierungscode oder einen Schlüssel hinzufügen.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Update-Verteilung	**Update-Quelle**	Sie können den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen. Sie können die Verwendung der Kaspersky-Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
	Fenster **Verbindungseinstellungen** ► *Um das Fenster **Verbindungseinstellungen** zu öffnen,* klicken Sie auf die Schaltfläche **Verbindungseinstellungen** im Block **Update-Quelle**.	Im Block **Einstellungen für die Verbindung mit Update-Quellen** können Sie festlegen, ob eine Verbindung zu den Kaspersky-Lab-Update-Servern oder anderen Servern über einen Proxyserver hergestellt werden soll.
	Einstellungen für die Update-Verteilung	Sie können die Zusammensetzung der zu kopierenden Updates festlegen. Geben Sie im Feld **Ordner für die lokale Speicherung kopierter Updates** den Ordnerpfad an, in dem Kaspersky Security 10.1 für Windows Server die kopierten Updates speichern soll.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
Update der Programm-Datenbanken	**Update-Quelle**	Im Block **Update-Quelle** können Sie den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen. Sie können die Verwendung der Kaspersky-Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind. Im Block Optimierung der Nutzung des Festplatten-Subsystems können Sie die Funktion zur Verringerung der Auslastung des Festplatten-Subsystems anpassen: • **Belastung des Festplatten-Subsystems verringern** Dieses Kontrollkästchen aktiviert oder deaktiviert die Funktion zur Optimierung des Festplatten-Subsystems durch Ablage der Update-Dateien auf einer virtuellen Festplatte im Arbeitsspeicher. Ist das Kontrollkästchen aktiviert, so ist die Funktion aktiv. Das Kontrollkästchen ist standardmäßig deaktiviert. • **Für die Optimierung genutztes Arbeitsspeichervolumen (MB)**
Größe des Arbeitsspeichers (in MB), den das Programm für die Speicherung der Update-Dateien verwendet. Standardmäßig ist ein Arbeitsspeichervolumen von 512 MB eingestellt.	Fenster **Verbindungseinstellungen** ► *Um das Fenster **Verbindungseinstellungen** zu öffnen,* klicken Sie auf die Schaltfläche **Verbindungseinstellungen** im Block **Update-Quelle**.	Im Block **Einstellungen für die Verbindung mit Update-Quellen** können Sie festlegen, ob eine Verbindung zu den Kaspersky-Lab-Update-Servern oder anderen Servern über einen Proxyserver hergestellt werden soll.
	Zeitplan	Sie können die Einstellungen für den Start einer geplanten Aufgabe anpassen.

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
Update der Programm-Module	**Update-Quelle**	Sie können den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen. Sie können die Verwendung der Kaspersky-Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.
	Fenster **Verbindungseinstellungen** ► *Um das Fenster **Verbindungseinstellungen** zu öffnen,* klicken Sie auf die Schaltfläche **Verbindungseinstellungen** im Block **Update-Quelle**.	Im Block **Einstellungen für die Verbindung mit Update-Quellen** können Sie festlegen, ob eine Verbindung zu den Kaspersky-Lab-Update-Servern oder anderen Servern über einen Proxyserver hergestellt werden soll.
	Einstellungen für das Update der Programm-Module anpassen	Sie können die Aktionen angeben, die Kaspersky Security 10.1 für Windows Server bei Vorliegen kritischer Updates der Programm-Module und bei Vorliegen von Informationen über verfügbare planmäßige Updates ausführen soll, sowie auch das Verhalten von Kaspersky Security 10.1 für Windows Server nach Abschluss der Installation kritischer Updates anpassen.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Untersuchung auf Befehl	**Einstellungen**	Sie können einen Untersuchungsbereich für die Aufgabe zur Untersuchung auf Befehl festlegen sowie zur Einstellung der Sicherheitsstufe wechseln.

Aufgabentyp in Kaspersky Security 10.1 für Windows Server	Abschnitt im Eigenschaften-fenster: <Aufgabenname>	Aufgabeneinstellungen
	Fenster **Untersuchung auf Befehl anpassen** ► *Um das Fenster **Untersuchung auf Befehl anpassen** zu öffnen,* klicken Sie auf die Schaltfläche **Anpassen** im Block **Untersuchungs-bereich**.	Sie können eine der vordefinierten Sicherheitsstufen wählen oder die Einstellungen einer benutzerdefinierten Sicherheitsstufe manuell anpassen.
	Einstellungen	Im Block **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. Im Block **Erweiterte Einstellungen** können Sie die folgenden Parameter anpassen: • Verwendung der vertrauenswürdigen Zone in den Aufgaben zur Untersuchung auf Befehl • Verwendung von KSN in den Aufgaben zur Untersuchung auf Befehl • Priorität der Aufgabe zur Untersuchung auf Befehl angeben: Aufgabe im Hintergrundmodus ausführen (niedrige Priorität) oder Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten.
	Zeitplan	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Integritätsprüfung von Programm-Modulen	**Zeitplan**	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Für Aufgaben des Typs Rollback des Datenbanken-Updates können Sie nur die durch Kaspersky Security Center geregelten Standard-Einstellungen in den Abschnitten **Benachrichtigungen** und **Ausnahmen vom Gültigkeitsbereich** anpassen. Eine ausführliche Anleitung zur Konfiguration der Einstellungen in diesen Abschnitten finden Sie im *Hilfesystem von Kaspersky Security Center*.

In diesem Abschnitt

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

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen anpassen 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. Öffnen Sie das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.
4. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.
5. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
6. Im Abschnitt **Einstellungen** können Sie die folgenden Einstellungen konfigurieren:
   - den Schutzbereich ändern, indem Sie Ordnerpfade und Dateitypen hinzufügen oder löschen und Dateitypen angeben, für die der Start durch automatisch erstellte Regeln erlaubt ist.
   - gestartete Programme berücksichtigen oder nicht berücksichtigen.
7. Im Abschnitt **Einstellungen** können Sie Aktionen festlegen, die bei der Erstellung von Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden sollen:
   - **Digitales Zertifikat verwenden**

     Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts das Vorhandensein eines digitalen Zertifikats als Auslösekriterium für die Regel angegeben. Anschließend erlaubt das Programm den Start von Programmen mithilfe von Dateien, die über ein digitales Zertifikat verfügen. Diese Option empfiehlt sich, wenn Sie den Start beliebiger Programme erlauben möchten, die im Betriebssystem als vertrauenswürdig eingestuft sind.
   - **Header und Fingerabdruck des digitalen Zertifikats verwenden**

     Dieses Kontrollkästchen aktiviert oder deaktiviert die Verwendung des Headers und des Fingerabdrucks des digitalen Zertifikats der Datei als Auslösekriterium für die Erlaubnisregeln für die Kontrolle des Programmstarts. Die Aktivierung dieses Kontrollkästchens ermöglicht die Festlegung strengerer Bedingungen

für die Untersuchung digitaler Zertifikate.

Ist das Kontrollkästchen aktiviert, werden die Werte des Headers und des Fingerabdrucks des digitalen Zertifikats der Dateien, für welche die Regeln erstellt werden, als Kriterium für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts festgelegt. Kaspersky Security 10.1 für Windows Server erlaubt Programme, die mithilfe von Dateien mit einem angegebenen Fingerabdruck: und Header gestartet werden.

Die Verwendung dieses Kontrollkästchens stellt die strengste Einschränkung für das Auslösen von Erlaubnisregeln für den Programmstart anhand eines digitalen Zertifikats dar, da es sich beim Fingerabdruck um ein individuelles fälschungssicheres Identifikationsmerkmal eines digitalen Zertifikats handelt.

Ist das Kontrollkästchen deaktiviert, so wird als Kriterium für das Auslösen der Erlaubnisregeln zur Kontrolle des Programmstarts das Vorliegen eines beliebigen digitalen Zertifikats festgelegt, das im Betriebssystem als vertrauenswürdig eingestuft ist.

Das Kontrollkästchen ist aktiv, wenn die Option **Digitales Zertifikat verwenden** ausgewählt ist.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Falls kein Zertifikat vorhanden, Folgendes verwenden**

  Dropdown-Liste, welche die Auswahl der Kriterien für das Auslösen der Erlaubnisregeln für die Kontrolle des Programmstarts für den Fall erlaubt, dass die Datei, auf deren Grundlage die Regel erstellt wird, über kein digitales Zertifikat verfügt.

  - **SHA256-Hash**. Als Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird die Prüfsumme der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit der angegebenen Prüfsumme.
  - **Dateipfad**. Als Kriterium der Erlaubnisregel für die Kontrolle des Programmstarts wird der Pfad der Datei festgelegt, auf deren Grundlage die Regel erstellt wird. Danach erlaubt das Programm den Start von Programmen mithilfe von Dateien, die sich in den Ordnern befinden, die in der Tabelle "Erlaubnisregeln für Programme aus folgenden Ordnern erstellen" angegeben wurden.

- **SHA256-Hash verwenden**

  Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts die Prüfsumme der Datei, auf deren Grundlage die Regel erstellt wird, als Auslösekriterium für die Regel angegeben. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit den angegebenen Werten der Prüfsumme.

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

  Diese Variante gilt als Standard.

- **Regeln für Benutzer oder Benutzergruppe erstellen**

  Feld, in dem der Benutzer und/oder die Benutzergruppe angegeben sind. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer und/oder die angegebene Benutzergruppe.

  Standardmäßig ist die Gruppe **Alle** eingestellt.

Sie können die Einstellungen für die Konfigurationsdateien mit Listen von Erlaubnisregeln anpassen,

die von Kaspersky Security 10.1 für Windows Server nach Abschluss der Aufgaben erstellt werden.

8. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
9. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
10. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

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

    Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Aufgabe Programm aktivieren

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen anpassen 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. Öffnen Sie das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.
4. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.
5. Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
6. Wenden Sie im Abschnitt **Aktivierungsparameter** die Schlüsseldatei an, mit der Sie das Programm aktivieren möchten. Aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**, wenn Sie einen Schlüssel zur Verlängerung der Lizenz hinzufügen möchten.
7. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
9. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

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

    Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Update-Aufgaben

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen anpassen 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. Öffnen Sie das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.
4. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.

   > Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.
5. Je nach Typ der zu konfigurierenden Aufgabe führen Sie eine der folgenden Aktionen aus:
   - Passen Sie im Block **Update-Quelle** die Einstellungen für die Update-Quelle an und optimieren Sie die Nutzung des Laufwerk-Subsystems.
     a. Im Block **Update-Quelle** können Sie den Administrationsserver von Kaspersky Security Center oder die Kaspersky-Lab-Update-Server als Update-Quelle für die Programmaktualisierung angeben. Darüber hinaus können Sie eine benutzerdefinierte Liste mit Update-Quellen erstellen und andere HTTP-, FTP-Server oder Netzwerkressourcen manuell hinzufügen und als Update-Quellen festlegen.

        Sie können die Verwendung der Kaspersky-Lab-Update-Server konfigurieren, falls die manuell angegebenen Server nicht verfügbar sind.

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

        - **Belastung des Festplatten-Subsystems verringern**

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

          Ist das Kontrollkästchen aktiviert, so ist die Funktion aktiv.

          Das Kontrollkästchen ist standardmäßig deaktiviert.

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

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

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

- Im Abschnitt **Einstellungen für das Update der Programm-Module anpassen** der Aufgabe zum Update der Programm-Module können Sie die Aktionen angeben, die Kaspersky Security 10.1 für Windows Server bei Vorliegen kritischer Updates der Programm-Module und bei Vorliegen von Informationen über verfügbare planmäßige Updates ausführen soll. Außerdem können Sie das Verhalten von Kaspersky Security 10.1 für Windows Server nach Abschluss der Installation wichtiger Updates konfigurieren.
- Geben Sie im Abschnitt **Einstellungen für die Update-Verteilung** der Aufgabe zur **Update-Verteilung** die Zusammensetzung der Updates und den Ordner der lokalen Update-Quelle an, in der die Updates gespeichert werden sollen.

6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
8. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

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

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

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

Integritätsprüfung von Programm-Modulen

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen anpassen 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. Öffnen Sie das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.
4. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.

> Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

5. Wählen Sie im Abschnitt **Geräte** die Geräte aus, für die Sie die Aufgabe zur Integritätsprüfung der Programm-Module ausführen möchten.
6. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
7. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
8. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

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

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

   Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

Erstellen einer Aufgabe zur Untersuchung auf Befehl

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

1. Starten Sie den Assistenten für neue Aufgaben nach einer der folgenden Methoden:
   - Für das Erstellen einer lokalen Aufgabe:
     a. Erweitern Sie in der Struktur des Administrationsservers von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, zu der der geschützte Server gehört.
     b. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Geräte** das Kontextmenü für die Zeile mit Informationen über den geschützten Server und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im erscheinenden Fenster im Abschnitt **Aufgaben** auf **Hinzufügen**.
   - Für das Erstellen einer Gruppenaufgabe:
     a. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Gruppe aus, für die Sie eine Richtlinie erstellen möchten.
     b. Öffnen Sie im Ergebnisfenster das Kontextmenü auf der Registerkarte **Aufgaben** und wählen Sie den Punkt **Erstellen → Aufgabe**.
   - Um eine Aufgabe für eine beliebige Auswahl an Computern zu erstellen, öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center den Knoten **Geräteauswahl** und wählen Sie den Punkt **Aufgabe erstellen** aus.

   Darauf öffnet sich der Assistent für neue Aufgaben.
2. Geben Sie im Fenster **Aufgabenname festlegen** einen Aufgabennamen an (maximal 100 Zeichen, wobei

folgende Zeichen unzulässig sind: **I * < > ? \ / | :)**. Es wird empfohlen, den Aufgabentyp im Namen anzugeben (z. B. "Untersuchung auf Befehl der freigegebenen Ordner").

3. Wählen Sie im Fenster **Aufgabentyp** unter der Überschrift **Kaspersky Security 10.1 für Windows Server** die Aufgabe **Untersuchung auf Befehl** aus und klicken Sie auf **Weiter**.
4. Erstellen Sie im Fenster **Untersuchungsbereich** einen Untersuchungsbereich:

   Standardmäßig gehören zum Untersuchungsbereich wichtige Bereiche des Servers. 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**.
     b. Wählen Sie im Fenster **Zum Untersuchungsbereich hinzufügen** entweder einen vordefinierten Bereich aus der Liste **Vordefinierter Bereich** aus oder geben Sie eine Festplatte des Computers, einen Ordner, ein Netzwerkobjekt oder eine Datei auf dem Server oder auf einem anderen Computer im Netzwerk an und klicken Sie dann auf **OK**.
   - Um Unterordner oder Dateien von der Untersuchung auszuschließen, wählen Sie den hinzugefügten Ordner (das hinzugefügte Laufwerk) im Fenster **Untersuchungsbereich** des Assistenten aus:
     a. Öffnen Sie das Kontextmenü und wählen Sie die Option **Anpassen**.
     b. Klicken Sie auf die Schaltfläche **Einstellungen** im Fenster **Sicherheitsstufe**.
     c. Deaktivieren Sie auf der Registerkarte **Allgemein** im Fenster **Untersuchung auf Befehl** die Kontrollkästchen **Untergeordnete Ordner** und **Dateien**.
   - Um die Sicherheitseinstellungen des Untersuchungsbereichs zu ändern, gehen Sie wie folgt vor:
     a. Öffnen Sie das Kontextmenü für den Bereich, dessen Einstellungen Sie ändern wollen, und wählen Sie **Anpassen**.
     b. Wählen Sie im Fenster **Untersuchung auf Befehl** eine der vordefinierten Sicherheitsstufen aus oder klicken Sie auf die Schaltfläche **Einstellungen**, um die Sicherheitseinstellungen manuell anzupassen.

        Das Anpassen der Sicherheitseinstellungen wird genauso wie in der Konsole für Kaspersky Security 10.1 durchgeführt.
   - Um eingebettete Objekte in hinzugefügten Untersuchungsbereich zu überspringen, gehen Sie wie folgt vor:
     a. Öffnen Sie das Kontextmenü für die Tabelle **Untersuchungsbereich** und wählen Sie **Ausnahme hinzufügen**.
     b. Geben Sie die Objekte an, die ausgeschlossen werden sollen: Wählen Sie den vordefinierten Gültigkeitsbereich in der Liste **Vordefinierter Bereich** aus, geben Sie das Computerlaufwerk, den Ordner, das Netzwerkobjekt bzw. die Datei auf dem Server oder einem anderen Computer im

Netzwerk an.

c. Klicken Sie auf **OK**.

5. Passen Sie im Fenster **Einstellungen** die heuristische Analyse und Integration mit anderen Komponenten an:.

- Passen Sie die Verwendung der heuristischen Analyse an (siehe Abschnitt "Verwendung der heuristischen Analyse" auf Seite 182).
- Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone anwenden**, wenn Sie Objekte, die in der vertrauenswürdigen Zone von Kaspersky Security 10.1 für Windows Server beschrieben werden, vom Untersuchungsbereich der Aufgabe ausschließen möchten.

  Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

  Ist das Kontrollkästchen aktiviert, fügt Kaspersky Security 10.1 für Windows Server die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

  Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Security 10.1 für Windows Server die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs in der Aufgabe Echtzeitschutz für Dateien.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Aktivieren Sie das Kontrollkästchen **KSN zur Überprüfung verwenden**, wenn Sie die Cloud-Dienste von Kaspersky Security Network für die Aufgabe nutzen möchten.

  Mithilfe dieses Kontrollkästchens wird die Verwendung der Cloud-Dienste von Kaspersky Security Network (KSN) in der Aufgabe aktiviert bzw. deaktiviert.

  Ist das Kontrollkästchen aktiviert, so verwendet das Programm die von den KSN-Diensten übermittelten Daten, was eine schnellere Reaktion des Programms auf neue Bedrohungen gewährleistet und die Wahrscheinlichkeit von Fehlalarmen verringert.

  Ist das Kontrollkästchen deaktiviert, werden die KSN-Dienste von der Aufgabe zur Untersuchung auf Befehl nicht verwendet.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Um einem Arbeitsprozess, in dem eine Aufgabe ausgeführt wird, die Basispriorität **Niedrig** zuzuweisen, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**.

  Dieses Kontrollkästchen ändert die Priorität der Aufgabe.

  Wenn dieses Kontrollkästchen aktiviert ist, wird die Aufgabenpriorität im Betriebssystem gesenkt. Das Betriebssystem stellt Ressourcen zur Verfügung, um die Aufgabe in Abhängigkeit von der Belastung der CPU und des Dateisystems des Computers durch andere Aufgaben von Kaspersky Security 10.1 für Windows Server und Programme auszuführen. Die Aufgabe wird daher bei einer Erhöhung der Belastung langsamer und bei einer Reduzierung der Belastung schneller ausgeführt.

  Wenn dieses Kontrollkästchen deaktiviert ist, wird die Aufgabe mit derselben Priorität ausgeführt wie die übrigen Aufgaben von Kaspersky Security 10.1 für Windows Server und die anderen Programme. In diesem Fall wird die Aufgabe schneller ausgeführt.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

Arbeitsprozesse, in denen Aufgaben für Kaspersky Security 10.1 für Windows Server ausgeführt werden, haben standardmäßig die Priorität **Mittel** (Normal).

- Um die erstellte Aufgabe als Untersuchung wichtiger Bereiche zu verwenden, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten**.

  Dieses Kontrollkästchen ändert die Priorität einer Aufgabe: Es aktiviert oder deaktiviert das Protokollieren des Ereignisses *Untersuchung wichtiger Bereiche* und das Update des Schutzstatus des Servers. Kaspersky Security Center überprüft die Sicherheitsstufe des Servers (der Server) mithilfe der Leistungsergebnisse von Aufgaben mit dem Status *Untersuchung wichtiger Bereiche*. In den Eigenschaften von lokalen System- und benutzerdefinierten Aufgaben von Kaspersky Security 10.1 für Windows Server ist das Kontrollkästchen nicht verfügbar. Sie können den Wert dieser Einstellung nur auf Seiten von Kaspersky Security Center ändern.

  Wenn dieses Kontrollkästchen aktiviert ist, protokolliert der Administrationsserver das Ereignis "Untersuchung wichtiger Bereiche wurde ausgeführt" und aktualisiert den Schutzstatus des Servers anhand der Ergebnisse der Aufgabenausführung. Die Untersuchungsaufgabe hat eine hohe Priorität.

  Ist das Kontrollkästchen deaktiviert, so wird die Untersuchungsaufgabe mit niedriger Priorität ausgeführt.

  Das Kontrollkästchen ist für die Aufgabe "Untersuchung wichtiger Bereiche" standardmäßig aktiviert.

6. Klicken Sie auf **Weiter**.
7. Richten Sie im Fenster **Zeitplan** einen Zeitplan für die Aufgabe ein (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite 148).
8. Geben Sie ein Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll, und legen Sie einen Aufgabennamen fest.
9. Klicken Sie auf **Fertig**.

Die neue Aufgabe zur Untersuchung auf Befehl wird für einen ausgewählten Server oder eine Servergruppe erstellt.

Aufgabe zur Untersuchung auf Befehl konfigurieren

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**. Erweitern Sie die Administrationsgruppe, für deren Computer Sie die Programmeinstellungen anpassen 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. Öffnen Sie das Kontextmenü der Aufgabe und wählen Sie **Eigenschaften** aus.

   Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.
4. Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für Benachrichtigungen über Ereignisse der Aufgabe.

Ausführliche Informationen zur Konfiguration der Einstellungen in diesem Abschnitt finden Sie im *Hilfesystem von Kaspersky Security Center*.

5. Im Abschnitt **Einstellungen** können Sie die folgenden Aktionen vornehmen:
   a. Aktivieren Sie im Block **Untersuchungsbereich** die Kontrollkästchen der Dateiressourcen, die Sie in den Untersuchungsbereich aufnehmen möchten.
   b. Klicken Sie auf die Schaltfläche **Anpassen** und wählen Sie eine Sicherheitsstufe aus.

      Sie können eine der vordefinierten Sicherheitsstufen auswählen oder die Sicherheitsstufe manuell anpassen. Um die Sicherheitsstufe manuell anzupassen, klicken Sie im Fenster **Untersuchung auf Befehl anpassen** auf die Schaltfläche **Einstellungen**.
6. Im Abschnitt **Einstellungen** können Sie die folgenden Aktionen vornehmen:
   a. Im Block **Heuristische Analyse** können Sie die Verwendung der heuristischen Analyse aktivieren oder deaktivieren und die Analysetiefe mithilfe eines Schiebereglers im Block **Heuristische Analyse** anpassen.
   b. **Erweiterte Einstellungen** anpassen (siehe Abschnitt "**Erstellen einer Aufgabe zur Untersuchung auf Befehl**" auf S. 140).
7. Passen Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen mit Ausnahme der Aufgabe Rollback des Datenbanken-Updates anpassen).
8. Geben Sie im Abschnitt **Benutzerkonto** das Konto an, mit dessen Rechten Sie die Aufgabe ausführen möchten.
9. Geben Sie bei Bedarf im Abschnitt **Ausnahmen** vom Gültigkeitsbereich der Aufgabe diejenigen Objekte an, die Sie aus dem Gültigkeitsbereich der Aufgabe ausschließen möchten.

   Ausführliche Informationen zum Anpassen der Einstellungen in diesen Blöcken finden Sie im *Hilfesystem von Kaspersky Security Center.*
10. Klicken Sie im Fenster **Eigenschaften <Name der Aufgabe>** auf **OK**.

    Die vorgenommenen Einstellungen für die Gruppenaufgaben werden gespeichert.

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

In der Grundeinstellung weist Kaspersky Security Center einem Server den Status *Warnung* zu, wenn die Aufgabe "Untersuchung wichtiger Bereiche" seltener ausgeführt wird als durch die Einstellung **Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt** von Kaspersky Security 10.1 für Windows Server angegeben ist.

► *Gehen Sie folgendermaßen vor, um die Untersuchung aller Server anzupassen, die zu einer Administrationsgruppe gehören:*

1. Erstellen Sie eine Gruppenaufgabe zur Untersuchung auf Befehl.
2. Aktivieren Sie im Fenster **Einstellungen** des Assistenten für die Aufgabenerstellung das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten**. Die von Ihnen angegebenen

Aufgabenparameter, nämlich der Untersuchungsbereich und die Parameter für Sicherheit, sind für alle Computer der Gruppe gleich. Stellen Sie den Aufgabenzeitplan ein.

Sie können das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten** im Fenster **Eigenschaften: <Aufgabenname>** entweder bei der Erstellung einer Aufgabe zur Untersuchung auf Befehl für eine Computergruppe oder für eine Auswahl von Computern oder zu einem späteren Zeitpunkt aktivieren.

3. Deaktivieren Sie mit Hilfe einen neuen oder vorhandenen Richtlinie den Start von Systemaufgaben zur Untersuchung nach Zeitplan (siehe Abschnitt "Zeitplan für den Start von lokalen Systemaufgaben anpassen" auf S. 118) auf den Servern der Gruppe.

Von diesem Zeitpunkt an berücksichtigt der Kaspersky Security Center-Administrationsserver bei der Bewertung des Sicherheitszustands des geschützten Servers und bei der Benachrichtigung darüber die Ergebnisse der letzten Ausführung der Aufgabe mit dem Aufgabenstatus "Untersuchung wichtiger Bereiche", und nicht die Ausführungsergebnisse der Systemaufgabe *Untersuchung wichtiger Bereiche*.

Sie können den Status *Aufgabe zur Untersuchung wichtiger Bereiche* nicht nur Gruppenaufgaben, sondern auch Aufgaben für Zusammenstellungen von Computern zur Untersuchung auf Befehl zuweisen.

In der Konsole für Kaspersky Security 10.1 können Sie überprüfen, ob eine Aufgabe zur Untersuchung auf Befehl als Aufgabe zur Untersuchung wichtiger Bereiche betrachtet wird.

In der Konsole für Kaspersky Security 10.1 wird das Kontrollkästchen **Aufgabenausführung als Untersuchung wichtiger Bereiche betrachten** in den Aufgabeneigenschaften nur angezeigt und kann nicht geändert werden.

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

Wenn bei der Arbeit von Kaspersky Security 10.1 für Windows Server ein Problem auftreten sollte (z. B. Kaspersky Security 10.1 für Windows Server stürzt ab) und Sie möchten das Problem diagnostizieren, können Sie die Erstellung von Protokolldateien und einer Dump-Datei für die Prozesse von Kaspersky Security 10.1 für Windows Server aktivieren und diese Dateien zur Analyse an den Technischen Support von Kaspersky Lab übermitteln.

Kaspersky Security 10.1 für Windows Server versendet Protokoll- oder Dump-Dateien nicht automatisch. Nur ein Benutzer mit entsprechenden Rechten kann Diagnosedaten versenden.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server verwaltet. Sie können die Zugriffsrechte konfigurieren (s. Abschnitt "Über Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server" auf S. 100) und nur bestimmten Benutzern Zugriff auf Berichte, Protokoll- und Dump-Dateien gewähren.

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

1. Öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf S. 125).
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 Security 10.1 für Windows Server die Protokolldateien speichern soll.
     - Passen Sie die Genauigkeitsstufe für die Debug-Informationen an.

       In dieser Dropdown-Liste können Sie die Genauigkeitsstufe für die Debug-Informationen auswählen, die Kaspersky Security 10.1 für Windows Server in der Protokolldatei speichert.

       Sie können eine der folgenden Genauigkeitsstufen auswählen:

       - **Kritische Ereignisse** – Kaspersky Security 10.1 für Windows Server speichert nur Informationen über kritische Ereignisse in der Protokolldatei.
       - **Fehler** – Kaspersky Security 10.1 für Windows Server speichert Informationen über kritische Ereignisse und Fehler in der Protokolldatei.
       - **Wichtige Ereignisse** – Kaspersky Security 10.1 für Windows Server speichert Informationen über kritische Ereignisse, Fehler und wichtige Ereignisse in der Protokolldatei.
       - **Informative Ereignisse** – Kaspersky Security 10.1 für Windows Server speichert Informationen über kritische Ereignisse, Fehler, wichtige Ereignisse und informative Ereignisse in der Protokolldatei.
       - **Debug-Informationen** – Kaspersky Security 10.1 für Windows Server speichert sämtliche Debug-Informationen in der Protokolldatei.

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

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

       Die Dropdown-Liste ist verfügbar, wenn das Kontrollkästchen **Debug-Informationen in Protokolldatei speichern** aktiviert ist.
     - Geben Sie die maximale Größe der Protokolldateien an.
     - Geben Sie die Komponenten für das Debuggen an. Komponentencodes müssen durch einen Strichpunkt getrennt werden. Bei den Codes muss die Groß- und Kleinschreibung beachtet werden (siehe Tabelle unten).

Tabelle 28. Subsystemcodes in Kaspersky Security 10.1 für Windows Server

Code des Subsystems	Name des Subsystems
*	Alle Komponenten.
gui	Subsystem der Benutzeroberfläche, Snap-In von Kaspersky Security 10.1 für Windows Server in der Microsoft Management Console.
ak_conn	Subsystem zur Integration des Administrationsagenten von Kaspersky Security Center.
bl	Steuerungsprozess, implementiert Steuerungsaufgaben von Kaspersky Security 10.1 für Windows Server
wp	Arbeitsprozess, der die Aufgaben zum Antiviren-Schutz realisiert
blgate	Prozess zur Fernverwaltung von Kaspersky Security 10.1 für Windows Server
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 Security 10.1 für Windows Server (gui) und das Verwaltungs-Plug-in von Kaspersky Security 10.1 für Windows Server für Kaspersky Security Center (ak_conn) werden nach dem Neustart dieser Komponenten übernommen. Die Einstellungen für die Protokollierung des Subsystems zur SNMP-Unterstützung (snmp) werden nach dem Neustart des SNMP-Dienstes übernommen. Die Trace-Parameter für das Subsystem der Leistungsindikatoren (perfcount) werden nach einem Neustart aller Prozesse angewandt, die die Leistungsindikatoren verwenden. Die Einstellungen für die Protokollierung der übrigen Subsysteme von Kaspersky Security 10.1 für Windows Server werden sofort nach dem Speichern der Einstellungen für die Fehlerdiagnose wirksam.

Standardmäßig werden in Kaspersky Security 10.1 für Windows Server sämtliche Debug-Informationen für alle Komponenten von Kaspersky Security 10.1 für Windows Server protokolliert.

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

- Wenn Sie eine Dump-Datei erstellen möchten, aktivieren Sie das Kontrollkästchen **Bei Absturz Dump-Datei erstellen**.
  - Geben Sie im Feld unten den Ordner an, in dem Kaspersky Security 10.1 für Windows Server die Dump-Datei speichern soll.

3. Klicken Sie auf **OK**.

Die festgelegten Programmeinstellungen werden auf dem geschützten Server übernommen.

Arbeit mit dem Aufgabenzeitplan

Sie können den Start der Aufgaben von Kaspersky Security 10.1 für Windows Server nach Zeitplan einrichten sowie die diesbezüglichen Einstellungen anpassen.

In diesem Abschnitt

Zeitplan-Einstellungen für den Aufgabenstart anpassen

In der Konsole für Konsole für Kaspersky Security 10.1 können Sie einen Startzeitplan für lokale Systemaufgaben und benutzerdefinierten Aufgaben erstellen. Für den Start von Gruppenaufgaben kann kein Zeitplan erstellt werden.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole für Kaspersky Security Center den Knoten **Verwaltete Geräte** und gehen Sie wie folgt vor:
   - Um die Einstellungen einer Richtlinie anzupassen, wählen Sie in der Gruppe der Computer **Richtlinie > <Name der Richtlinie> > <Abschnitt> > Einstellungen > Aufgabenverwaltung** aus.
   - Um die Aufgabeneinstellungen für einen Computer über Kaspersky Security Center anzupassen, öffnen Sie in Kaspersky Security Center das Fenster **Aufgabeneinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf S. 125).

     Das Fenster **Einstellungen** wird geöffnet.
2. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Zeitplan** das Kontrollkästchen **Aufgabe nach Zeitplan starten**.

   Die Felder mit den Zeitplan-Einstellungen der Aufgabe zur Untersuchung auf Befehl und der Update-Aufgabe stehen nicht zur Verfügung, wenn der Start der Aufgabe durch eine Richtlinie von Kaspersky Security Center verboten ist.
3. Passen Sie die Zeitplaneinstellungen entsprechend an. Gehen Sie hierzu wie folgt vor:
   a. Wählen Sie in der Liste **Startintervall** einen der folgenden Werte aus:
      - **Stündlich**, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Stunden gestartet wird, wobei Sie die Anzahl der Stunden im Feld **Alle <Anzahl> Std.** eingeben müssen.
      - **Täglich**, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl an Tagen gestartet wird, wobei Sie die Anzahl der Tage im Feld **Alle <Anzahl> Tage**

eingeben müssen.

- **Wöchentlich**, wenn Sie möchten, dass die Aufgabe jeweils nach der von Ihnen angegebenen Anzahl von Wochen gestartet wird, wobei Sie die Anzahl der Wochen im Feld **Alle <Anzahl> Wochen** eingeben müssen. Legen Sie fest, an welchen Wochentagen die Aufgabe gestartet werden soll (Standardmäßig werden Aufgaben montags gestartet).
- **Bei Programmstart**, wenn Sie möchten, dass die Aufgabe bei jedem Start von Kaspersky Security 10.1 für Windows Server ausgeführt wird.
- **Nach dem Update der Programm-Datenbanken**, wenn Sie möchten, dass die Aufgabe nach jedem Update der Programm-Datenbanken gestartet wird.

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

c. Tragen Sie im Feld **Beginnen am** das Startdatum des Zeitplans ein.

Nachdem Sie das Startintervall der Aufgabe, die Uhrzeit für den erstmaligen Aufgabenstart und das Datum, ab dem der Zeitplan gelten soll, angegeben haben, wird im oberen Bereich des Fensters im Feld **Nächster Start** der berechnete Zeitpunkt des nächsten Aufgabenstarts angezeigt. Aktualisierte Informationen über die Zeit, die bis zum nächsten Start verbleibt, werden jedes Mal angezeigt, wenn Sie das Fenster **Aufgabeneinstellungen** auf der Registerkarte **Zeitplan** öffnen.
Der Wert **Durch Richtlinie verboten** wird im Feld **Nächster Start** angezeigt, wenn der Start zeitgesteuerter Systemaufgaben durch die Einstellungen der aktiven Richtlinie für Kaspersky Security Center verboten ist (siehe Abschnitt "Zeitplan für den Start von lokalen Systemaufgaben anpassen" auf S. 118).

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

- Im Block **Einstellungen für das Anhalten der Aufgabe**:

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

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

- Im Block **Erweiterte Einstellungen**:

  a. Aktivieren Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und geben Sie das Datum an, ab dem der Zeitplan ungültig werden soll.

  b. Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, wenn Sie den Start übersprungener Aufgaben ermöglichen möchten.

  c. Aktivieren Sie das Kontrollkästchen **Zeitabstände für den Start** und geben Sie einen Wert in Minuten ein.

5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Einstellungen für den Aufgabenstart zu speichern.

Start nach Zeitplan aktivieren und deaktivieren

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

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

1. Öffnen Sie in der Struktur der Konsole für Kaspersky Security 10.1 das Kontextmenü für den Aufgabennamen, für den Sie den Startzeitplan anpassen möchten.
2. Wählen Sie den Menüpunkt **Eigenschaften**.

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

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

Die angepassten Zeitplan-Einstellungen für den Aufgabenstart werden gespeichert.

Programmeinstellungen verwalten

Dieser Abschnitt enthält Informationen über die Konfiguration der allgemeinen Einstellungen von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center.

In diesem Kapitel

Über die Methoden zur Verwaltung von Kaspersky Security 10.1 für Windows Server durch Kaspersky Security Center

Sie können mehrere Server, auf denen Kaspersky Security 10.1 für Windows Server installiert ist und die Teil einer Administrationsgruppe sind, mithilfe des Plug-ins für Kaspersky Security Center zentral verwalten. Ferner erlaubt Kaspersky Security Center ein separates Anpassen der Betriebseinstellungen für jeden in der Administrationsgruppe enthaltenen Servers.

Die *Administrationsgruppe* wird auf Seiten von Kaspersky Security Center manuell erstellt und beinhaltet mehrere Server, auf denen Kaspersky Security 10.1 für Windows Server installiert ist, und für die Sie einheitliche Verwaltungs- und Schutzeinstellungen festlegen möchten. Ausführliche Informationen über die Verwendung von Administrationsgruppen finden Sie im *Hilfesystem von Kaspersky Security Center*.

Die Programmeinstellungen für einen Computer sind nicht verfügbar, wenn die Arbeit von Kaspersky Security 10.1 für Windows Server auf diesem Server durch die aktive Richtlinie von Kaspersky Security Center kontrolliert wird.

Sie können Kaspersky Security 10.1 für Windows Server 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 Servergruppen per Fernzugriff zu konfigurieren. Die in der aktiven Richtlinie festgelegten Aufgabeneinstellungen haben Priorität vor den Aufgabeneinstellungen, die lokal in der Konsole für Kaspersky Security 10.1 oder per Remote-Zugriff im Fenster **Eigenschaften: <Computername>** von Kaspersky Security Center konfiguriert wurden.

  Mithilfe von Richtlinien können Sie allgemeine Programmeinstellungen , Einstellungen für Aufgaben zum Echtzeitschutz, Einstellungen für die Überwachung der Server-Aktivitäten, Einstellungen für den Schutz für Netzwerkspeichern, Einstellungen zum Start von Systemaufgaben nach Zeitplan und Einstellungen für die Verwendung von Profilen 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 Servergruppen per Fernzugriff.

Mithilfe von Gruppenaufgaben können Sie das Programm aktivieren sowie die Einstellungen der Aufgaben zur Untersuchung auf Befehl, der Update-Aufgaben und der Aufgaben zur automatischen Erstellung von Erlaubnisregeln konfigurieren.

- **Mithilfe von Aufgaben für eine Auswahl von Geräten**. Aufgaben für eine Auswahl von Geräten ermöglichen die Konfiguration einheitlicher Einstellungen für Aufgaben mit begrenzter Ausführungsdauer und für Server, die nicht einer der erstellten Administrationsgruppen zugeordnet sind, per Fernzugriff.
- **Mithilfe des Konfigurationsfensters für einen einzelnen Computer**. Im Fenster **Eigenschaften: <Computername>** können Sie die Aufgabeneinstellungen für einen einzelnen Server, der einer Administrationsgruppe zugeordnet ist, per Fernzugriff konfigurieren. Sie können sowohl allgemeine Programmeinstellungen als auch Einstellungen für alle Aufgaben von Kaspersky Security 10.1 für Windows Server anpassen, wenn der ausgewählte Server sich nicht unter der Verwaltung der aktiven Richtlinie von Kaspersky Security Center befindet.

Kaspersky Security Center ermöglicht die Anpassung der Programmeinstellungen, der erweiterten Optionen und der Ausführung der Berichte und Benachrichtigungen. Sie können diese Einstellungen sowohl für Servergruppen als auch für einen einzelnen Server anpassen.

Über die Konfiguration der allgemeinen Programmeinstellungen in Kaspersky Security Center

Sie können die allgemeinen Einstellungen von Kaspersky Security 10.1 für Windows Server für Servergruppen und für einen einzelnen Server über Kaspersky Security Center konfigurieren.

In diesem Abschnitt

Skalierbarkeit und Schnittstelle in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

► *Um die Einstellungen der Skalierbarkeit und der Programmoberfläche zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Skalierbarkeit und Oberfläche** auf die Schaltfläche **Einstellungen**.
4. Konfigurieren Sie im Fenster **Skalierbarkeit und Oberfläche** auf der Registerkarte **Allgemein** die folgenden Einstellungen:
   - Passen Sie im Block **Skalierbarkeitseinstellungen** die Einstellungen an, durch die die Anzahl der von Kaspersky Security 10.1 für Windows Server verwendeten Arbeitsprozesse festgelegt wird:
     - **Skalierbarkeitseinstellungen automatisch ermitteln**

       Die Zahl der verwendeten Prozesse wird von Kaspersky Security 10.1 für Windows Server automatisch geregelt.

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

       Die Zahl der aktiven Arbeitsprozesse wird von Kaspersky Security 10.1 für Windows Server gemäß den angegebenen Werten geregelt.

       - **Maximale Anzahl aktiver Prozesse**

         Die maximale Anzahl der von Kaspersky Security 10.1 für Windows Server verwendeten Prozesse. Das Eingabefeld ist verfügbar, wenn die Variante **Anzahl der Arbeitsprozesse manuell angeben** ausgewählt wurde.
       - **Anzahl der Prozesse für den Echtzeitschutz**

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

         Die maximale Anzahl von Prozessen, die durch die Komponente der Untersuchung auf Befehl bei der Ausführung der Aufgaben zur Untersuchung auf Befehl im Hintergrundmodus verwendet werden. Das Eingabefeld ist verfügbar, wenn die Variante

Anzahl der Arbeitsprozesse manuell angeben ausgewählt wurde.

- Passen Sie im Block **Interaktion mit dem Benutzer** die Anzeige des Symbols von Kaspersky Security 10.1 für Windows Server im Infobereich der Taskleiste an: Deaktivieren oder aktivieren Sie das Kontrollkästchen **Programmsymbol in der Taskleiste anzeigen**.

5. Wählen Sie auf der Registerkarte **Hierarchischer Speicher** eine der folgenden Einstellungen für den Zugriff auf den hierarchischen Speicher aus:

   - **Kein HSM-System**

     Kaspersky Security 10.1 für Windows Server verwendet beim Ausführen von Aufgaben zur Untersuchung auf Befehl nicht die Einstellungen des HSM-Systems.

     Diese Variante gilt als Standard.

   - **HSM-System verwendet Analysepunkte**

     Kaspersky Security 10.1 für Windows Server verwendet Reparse Points zur Untersuchung von Dateien im Remote-Speicher beim Ausführen von Aufgaben zur Untersuchung auf Befehl.

   - **HSM-System verwendet erweiterte Dateiattribute**

     Pfad des Ordners, in den Objekte wiederhergestellt werden, im UNC-Format (Universal Naming Convention).

     Standardmäßig ist der folgende Pfad eingestellt: C:\ProgramData\Kaspersky Lab\Kaspersky Security for Windows Server\10.0\Restored\.

   - **Unbekanntes HSM-System**

     Kaspersky Security 10.1 für Windows Server untersucht beim Ausführen von Aufgaben zur Untersuchung auf Befehl alle Dateien als Dateien im Remote-Speicher.

     Die Verwendung dieser Variante wird nicht empfohlen.

   Wenn Sie kein HSM-System verwenden, belassen Sie den Standardwert für die Einstellungen des HSM-Systems (Kein HSM-System).

6. Klicken Sie auf **OK**.

Die vorgenommenen Programmeinstellungen werden gespeichert.

Sicherheitseinstellungen in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

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

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

Verwaltete Geräte und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Sicherheit und Zuverlässigkeit** auf die Schaltfläche **Einstellungen**.
4. Konfigurieren Sie im Fenster **Sicherheitseinstellungen** die folgenden Einstellungen:

   - Passen Sie im Block **Einstellungen für Zuverlässigkeit** die Wiederherstellungseinstellungen für die Aufgaben von Kaspersky Security 10.1 für Windows Server bei Störungen oder einer fehlerhaften Beendigung des Programms an.
     - **Wiederherstellen von Aufgaben ausführen**

       Dieses Kontrollkästchen aktiviert oder deaktiviert die Wiederherstellung der Aufgaben von Kaspersky Security 10.1 für Windows Server nach einer Störung bzw. einer fehlerhaften Beendigung des Programms.

       Ist das Kontrollkästchen aktiviert, stellt Kaspersky Security 10.1 für Windows Server die Aufgaben von Kaspersky Security 10.1 für Windows Server nach einer Störung oder einer fehlerhaften Beendigung automatisch wieder her.

       Ist das Kontrollkästchen deaktiviert, stellt Kaspersky Security 10.1 für Windows Server die Aufgaben von Kaspersky Security 10.1 für Windows Server nach einer Störung oder einer fehlerhaften Beendigung nicht wieder her.

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     - **Maximale Anzahl der Wiederherstellungsversuche für Aufgaben zur Untersuchung auf Befehl**

Die Anzahl versuchter Wiederherstellungen der Aufgaben zur Untersuchung auf Befehl nach einer Störung von Kaspersky Security 10.1 für Windows Server. Das Eingabefeld ist verfügbar, wenn das Kontrollkästchen **Wiederherstellen von Aufgaben ausführen** aktiviert ist.

   - Legen Sie im Block **Aktionen beim Wechsel in den USV-Akkubetrieb** die von Kaspersky Security 10.1 für Windows Server beim Wechsel auf eine USV-Quelle erzeugte Belastungsbeschränkung auf den Server fest:
     - **Aufgaben zur Untersuchung nach Zeitplan nicht starten**

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

       Ist dieses Kontrollkästchen aktiviert, startet Kaspersky Security 10.1 für Windows Server

beim Wechsel auf eine USV-Quelle bis zur Wiederherstellung des Standardbetriebs keine Aufgaben zur Untersuchung nach Zeitplan.

Ist das Kontrollkästchen deaktiviert, startet Kaspersky Security 10.1 für Windows Server die Aufgaben zur Untersuchung nach Zeitplan unabhängig vom Stromversorgungsmodus.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Laufende Untersuchungsaufgaben anhalten**

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

  Ist dieses Kontrollkästchen aktiviert, hält Kaspersky Security 10.1 für Windows Server beim Wechsel des Computers auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben an.

  Ist dieses Kontrollkästchen deaktiviert, setzt Kaspersky Security 10.1 für Windows Server beim Wechsel des Computers auf eine USV-Quelle die Ausführung der gestarteten Untersuchungsaufgaben fort.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Legen Sie im Block **Einstellungen für Kennwortanwendung** das Kennwort für den Schutz des Zugriffs auf die Funktionen von Kaspersky Security 10.1 für Windows Server fest.

1. Klicken Sie auf **OK**.

Die konfigurierten Sicherheitseinstellungen werden gespeichert.

Verbindungseinstellungen über Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

Die angepassten Verbindungseinstellungen werden für die Verbindungsaufnahme von Kaspersky Security 10.1 für Windows Server mit den Update- und Aktivierungsservern sowie bei der Integration des Programms in die KSN-Dienste verwendet.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte

Geräte und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Programmeinstellungen** im Block **Proxyserver** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Verbindungseinstellungen** wird geöffnet.

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

   - Nehmen Sie im Block **Proxyserver-Einstellungen** die Einstellungen für die Verwendung eines Proxyservers vor:
     - **Keinen Proxyserver verwenden**

       Ist diese Einstellung ausgewählt, verwendet Kaspersky Security 10.1 für Windows Server keinen Proxyserver zur Verbindungsaufnahme mit den KSN-Diensten, sondern stellt die Verbindung direkt her.

     - **Proxyserver-Einstellungen automatisch ermitteln**.

       Ist diese Einstellung ausgewählt, ermittelt Kaspersky Security 10.1 für Windows Server die Einstellungen für die Verbindungsaufnahme mit den KSN-Diensten mithilfe des Protokolls Web Proxy Auto-Discovery Protocol (WPAD) automatisch.

       Diese Variante gilt als Standard.

     - **Einstellungen des angegebenen Proxyservers verwenden**

       Ist diese Einstellung ausgewählt, verwendet Kaspersky Security 10.1 für Windows Server für die Verbindungsaufnahme mit KSN die manuell eingegebenen Proxyserver-Einstellungen.

     - IP-Adresse oder symbolischer Name des Proxyservers und Portnummer.
     - **Für lokale Adressen keinen Proxyserver verwenden**.

       Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Nutzung eines Proxyservers für Anfragen an Computer aus dem Netzwerk, zu dem auch der Computer gehört, auf dem Kaspersky Security 10.1 für Windows Server installiert ist.

       Ist das Kontrollkästchen aktiviert, wird aus dem Netzwerk, zu dem der Computer mit installiertem Kaspersky Security 10.1 für Windows Server gehört, direkt auf Computer zugegriffen. Es wird kein Proxyserver verwendet.

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

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Legen Sie im Block **Einstellungen für die Authentifizierung auf dem Proxyserver** die Authentifizierungseinstellungen fest:
     - Wählen Sie in der Dropdown-Liste die Einstellungen für die Authentifizierung aus.
       - **Authentifizierung nicht verwenden** – es erfolgt keine Authentizitätsprüfung. Dieser Modus gilt als Standard.

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

- Geben Sie bei Bedarf Benutzername und Kennwort an.

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

5. Klicken Sie auf **OK**.

Die vorgenommenen Verbindungseinstellungen werden gespeichert.

Über die Konfiguration erweiterter Programmoptionen

Sie können über Kaspersky Security Center erweiterte Optionen für Kaspersky Security 10.1 für Windows Server für Computergruppen und für einzelne Computer anpassen.

In diesem Abschnitt

Einstellungen für die vertrauenswürdige Zone in Kaspersky Security Center anpassen

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

► *Zur Konfiguration der vertrauenswürdigen Zone gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte

Geräte und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

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

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

4. Geben Sie auf der Registerkarte **Ausnahmen** die Objekte an, die Kaspersky Security 10.1 für Windows Server bei der Untersuchung überspringen soll:

   - Klicken Sie auf die Schaltfläche **Empfohlene Ausnahmen hinzufügen**, wenn Sie die empfohlenen Ausnahmen hinzufügen möchten.

     Bei Anklicken dieser Schaltfläche werden der Liste mit den Ausnahmen von Microsoft empfohlene Ausnahmen und von Kaspersky Lab empfohlene Ausnahmen hinzugefügt.

   - Um Ausnahmen zu importieren, klicken Sie auf **Import** und wählen Sie im folgenden Fenster die Dateien aus, die Kaspersky Security 10.1 für Windows Server als vertrauenswürdig betrachten soll.

   - Wenn Sie die Bedingungen, bei deren Vorliegen eine Datei als vertrauenswürdig eingestuft werden soll, manuell angeben möchten, klicken Sie auf **Hinzufügen**. Geben Sie im erscheinenden Fenster folgende Einstellungen an:

     - **Zu untersuchendes Objekt**

       Name oder Namensmaske der Datei, lokale Festplatte oder Wechseldatenträger des Computers, lokaler oder Netzwerkordner, ein vordefinierter Bereich.

     - **Erkannte Objekte**

       Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Seite der Viren-Enzyklopädie.

       Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server die angegebenen gefundenen Objekte bei der Untersuchung.

       Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Security 10.1 für Windows Server alle Objekte, die im Programm standardmäßig angegeben sind.

       Das Kontrollkästchen ist standardmäßig deaktiviert.

     - **Gültigkeitsbereich der Ausnahme**

       Name der Aufgabe von Kaspersky Security 10.1 für Windows Server, in der die Regel angewendet wird.

     - Geben Sie im Feld **Kommentar** bei Bedarf zusätzlich erläuternde Informationen zur Ausnahme an.

5. Geben Sie im Fenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** die Prozesse an, die Kaspersky Security 10.1 für Windows Server bei der Untersuchung überspringen soll:

   - **Datei-Operationen bei Backup-Operationen nicht untersuchen**

     Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Untersuchung der Lesevorgänge für Dateien, wenn diese Vorgänge von den auf dem Server installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server bei der Untersuchung die Lesevorgänge für Dateien,

die von den auf dem Server installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server bei der Untersuchung die Lesevorgänge für Dateien, die von den auf dem Server installierten Funktionen zum Verschieben ins Backup ausgeführt werden.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

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

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

  Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server bei der Untersuchung die Dateivorgänge vertrauenswürdiger Prozesse.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server die Dateivorgänge vertrauenswürdiger Prozesse.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

6. Falls erforderlich, fügen Sie Prozesse hinzu, deren Datei-Aktivität Sie nicht untersuchen möchten (siehe Abschnitt "vertrauenswürdige Prozesse hinzufügen" auf Seite 160), indem Sie auf die Schaltfläche **Hinzufügen** klicken.
7. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf **OK**, um die Änderungen zu speichern.

Vertrauenswürdige Prozesse hinzufügen

► *Um einen oder mehrere Prozesse zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
4. Wählen Sie auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Aktivität**

der angegebenen Prozesse nicht untersuchen.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.
6. Wählen Sie aus dem Kontextmenü der Schaltfläche eine der Einstellungen aus:

   - **Mehrere Prozesse**.

     Nehmen Sie im nächsten Fenster **Hinzufügen von vertrauenswürdigen Prozessen** folgende Einstellungen vor:

     a. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Security 10.1 für Windows Server den vollständigen Ordnerpfad, um den Status der Vertrauenswürdigkeit des Prozesses zu bestimmen.

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

        Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

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

        Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Security 10.1 für Windows Server den Hashwert der ausgewählten Datei, um den Status der Vertrauenswürdigkeit des Prozesses zu bestimmen.

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

        Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     c. Klicken Sie auf die Schaltfläche **Durchsuchen**, um Daten auf der Grundlage ausführbarer Prozesse hinzuzufügen.

     d. Wählen Sie im folgenden Fenster eine ausführbare Datei aus.

        Sie können jeweils nur eine ausführbare Datei hinzufügen. Wiederholen Sie die Schritte c-d, um weitere ausführbare Dateien hinzuzufügen.

     e. Klicken Sie auf die Schaltfläche **Prozesse**, um Daten auf der Grundlage laufender Prozesse hinzuzufügen.

     f. Wählen Sie im folgenden Fenster Prozesse aus. Um mehrere Prozesse auszuwählen, halten Sie die **STRG**-Taste gedrückt, während Sie auswählen.

     g. Klicken Sie auf **OK**.

Das Benutzerkonto, mit dessen Berechtigungen die Aufgabe zum Echtzeitschutz für Dateien gestartet wird, muss auf dem Server, auf dem Kaspersky Security 10.1 für Windows Server installiert ist, über Administratorrechte verfügen, damit die Liste der aktiven Prozesse angezeigt werden kann. Sie können die Prozesse in der Liste der aktiven Prozesse nach Dateinamen, PID oder Pfad der ausführbaren Prozessdatei auf dem lokalen Server sortieren. Beachten Sie, dass Sie laufende Prozesse nur dann auswählen können, indem Sie auf die Schaltfläche **Prozesse** klicken, wenn Sie die Konsole für Kaspersky Security 10.1 auf einem lokalen Server oder den Einstellungen des betreffenden Computers in Kaspersky Security Center verwenden.

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

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

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

  b. Klicken Sie auf **OK**.

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

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

  a. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie einen Prozess aus.

  b. **Vollständigen Prozesspfad auf Laufwerk zur Bestimmung der Vertrauenswürdigkeit verwenden**

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Security 10.1 für Windows Server den vollständigen Ordnerpfad, um den Status der Vertrauenswürdigkeit des Prozesses zu bestimmen.

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

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

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

     Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Security 10.1 für Windows Server den Hashwert der ausgewählten Datei, um den Status der Vertrauenswürdigkeit des Prozesses zu bestimmen.

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

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  d. Klicken Sie auf **OK**.

Um den ausgewählten Prozess zur Liste der vertrauenswürdigen Prozesse hinzuzufügen, muss mindestens ein Kriterium für Vertrauenswürdigkeit ausgewählt sein.

7. Klicken Sie im Fenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **OK**.

Die gewählte Datei bzw. der Prozess wird im Fenster **Vertrauenswürdige Zone** zur Liste der vertrauenswürdigen Prozesse hinzugefügt.

Anwenden der Not-a-virus-Maske

Die Not-a-virus-Maske erlaubt es, während der Untersuchung legitime Softwaredateien und Webressourcen, die als schädlich eingestuft werden, zu überspringen. Die Maske wirkt sich auf folgende Aufgaben aus:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Skript-Untersuchung
- Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern
- Schutz des Datenverkehrs

Wenn die Maske nicht zur Liste mit Ausnahmen hinzugefügt wird, dann wird Kaspersky Security 10.1 für Windows Server die Aktion anwenden, die in den Aufgabeneinstellungen der Software oder der Webressource, die zu dieser Kategorie gehört, festgelegt sind.

► *Um die Not-a-virus-Maske zu verwenden, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.
4. Scrollen Sie auf der Registerkarte **Ausnahmen** nach unten und wählen Sie die Zeile mit dem Wert **not-a-virus:*** aus, wenn das Kontrollkästchen deaktiviert ist.
5. Klicken Sie auf **OK**.

Die neue Konfiguration wird übernommen.

Untersuchung von Wechseldatenträgern

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

Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server ohne Antiviren-Datenbanken installiert haben, ist die Untersuchung von Wechseldatenträgern nicht verfügbar.

Kaspersky Security 10.1 für Windows Server startet die Untersuchung von über USB angeschlossenen Wechseldatenträgern, wenn diese sich im Betriebssystem als Massenspeichergeräte (USB Mass Storage Device) registrieren. Das Programm führt keine Untersuchung des Wechseldatenträgers durch, wenn sein Anschluss von der Aufgabe zur Gerätekontrolle blockiert wird. Das Programm führt keine Untersuchung von MTP-Mobilgeräten durch.

Kaspersky Security 10.1 für Windows Server erlaubt den Zugriff auf Wechseldatenträger während der Untersuchung.

Die Ergebnisse der Untersuchung jedes Wechseldatenträgers werden im Bericht über die Ausführung der Aufgabe zur Untersuchung auf Befehl gespeichert, die beim Anschließen des jeweiligen Datenträgers erstellt wurde.

Sie können die Einstellungswerte der Komponente Wechseldatenträger untersuchen bearbeiten (s. Tabelle unten).

Tabelle 29. Einstellungen der Untersuchung von Wechseldatenträgern

Einstellung	Standardwert	Beschreibung
Wechseldatenträger beim Anschließen über USB untersuchen	Kontrollkästchen ist deaktiviert	Sie können die Untersuchung von Wechseldatenträgern bei ihrem Anschluss über USB an den geschützten Server aktivieren und deaktivieren.
Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)	1024 MB	Sie können den Bereich, in dem die Komponente aktiviert wird, reduzieren, indem Sie die Höchstmenge der Daten auf dem Wechseldatenträger angeben. Kaspersky Security 10.1 für Windows Server wird einen Wechseldatenträger nicht untersuchen, wenn die Menge der darauf gespeicherten Daten den angegebenen Wert übersteigt.
Untersuchung starten mit Sicherheitsstufe	Maximale Sicherheit	Sie können die Einstellungen der zu erstellenden Aufgaben zur Untersuchung auf Befehl anpassen, indem Sie eine der folgenden drei Sicherheitsstufen wählen: • Maximale Sicherheit • Empfohlen • Maximale Leistung Der Algorithmus der Aktionen beim Entdecken infizierter, möglicherweise infizierter und anderer Objekte, sowie andere Untersuchungseinstellungen für jede Sicherheitsstufe entsprechen den vorinstallierten Sicherheitsstufen in den Aufgaben zur Untersuchung auf Befehl.

Um die Einstellungen der Untersuchung von Wechseldatenträgern beim Anschließen anzupassen, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Untersuchung von Wechseldatenträgern** wird geöffnet.

4. Im Block **Einstellungen für Untersuchung beim Anschließen** gehen Sie wie folgt vor:
   - Aktivieren Sie das Kontrollkästchen **Wechseldatenträger beim Anschließen über USB untersuchen**, wenn Sie möchten, dass Kaspersky Security 10.1 für Windows Server automatisch eine Untersuchung der Wechseldatenträger bei ihrem Anschluss ausführt.
   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Untersuchen, wenn die Datenmenge auf dem Datenträger kleiner ist als (MB)** und geben Sie den Grenzwert der maximalen Datenmenge im Feld rechts davon an.
   - Geben Sie in der Dropdown-Liste **Untersuchung starten mit Sicherheitsstufe** die Sicherheitsstufe an, auf der die Untersuchung von Wechseldatenträgern ausgeführt werden soll.
5. Klicken Sie auf **OK**.

   Die vorgenommenen Einstellungen werden gespeichert und übernommen.

Zugriffsrechte in Kaspersky Security Center anpassen

Sie können die Rechte für den Zugriff auf die Programmverwaltung und die Verwaltung von Kaspersky Security Service in Kaspersky Security Center für Computergruppen und für einzelne Computer konfigurieren.

> Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server.
> Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

► *Gehen Sie wie folgt vor, um die Zugriffsrechte für die Programmverwaltung und die Verwaltung des Dienstes von Kaspersky Security Service zu konfigurieren:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

     > Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Öffnen Sie den Abschnitt **Zusätzlich** und gehen Sie wie folgt vor:
   - Wenn Sie die Zugriffsrechte zur Verwaltung von Kaspersky Security 10.1 für Windows Server für Benutzer oder eine Benutzergruppe konfigurieren möchten, klicken Sie im Block **Benutzerrechte**

für die Programmverwaltung auf die Schaltfläche Einstellungen.

- Wenn Sie die Zugriffsrechte zur Verwaltung von Kaspersky Security Service für Benutzer oder eine Benutzergruppe konfigurieren möchten, klicken Sie im Block **Benutzerrechte für die Verwaltung von Security Service** auf die Schaltfläche **Einstellungen**.

4. Passen Sie im folgenden Fenster die Zugriffsrechte (siehe Abschnitt "Über Zugriffsrechte für die Funktionen von Kaspersky Security 10.1 für Windows Server" auf Seite 100) entsprechend Ihren Bedürfnissen an.

Die vorgenommenen Einstellungen werden gespeichert.

Quarantäne- und Backup-Einstellungen in Kaspersky Security Center anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

     Wenn eine aktive Richtlinie von Kaspersky Security Center auf das Gerät angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthält, können diese Einstellungen nicht im Fenster **Programmeinstellungen** geändert werden.
3. Klicken Sie im Abschnitt **Zusätzlich** auf die Schaltfläche **Einstellungen** im Block **Speicher**.
4. Passen Sie im Fenster **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 Servers aus oder geben Sie seinen vollständigen Pfad an.
   - Um die maximale Größe des **Backups** festzulegen, aktivieren Sie das Kontrollkästchen **Maximale Größe des Backups (MB)** und tragen Sie im Eingabefeld den entsprechenden Wert in MB ein.
   - Um einen Grenzwert für freien Speicherplatz im Backup festzulegen, definieren Sie den Wert

der Einstellung **Maximale Größe des Backups (MB)**, aktivieren Sie das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz (MB)** und geben Sie den Mindestwert für den freien Speicher im **Backup** in MB an.

- Um einen anderen Wiederherstellungsordner anzugeben, wählen Sie in den Einstellungen für die Wiederherstellung von Objekten den entsprechenden Ordner auf einem lokalen Laufwerk des geschützten Servers aus oder geben Sie im Feld **Ordner für die Wiederherstellung von Objekten** den Namen und vollständigen Pfad des Ordners an.

5. Passen Sie im Fenster **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 Servers an.
   - Wenn Sie die maximale Größe der **Quarantäne** festlegen möchten, aktivieren Sie das Kontrollkästchen **Maximale Größe der Quarantäne (MB)** und tragen Sie im Eingabefeld den Wert in MB ein.
   - Wenn Sie die minimale Größe für den freien Speicherplatz in der **Quarantäne** festlegen möchten, aktivieren Sie die Kontrollkästchen **Maximale Größe der Quarantäne (MB)** und **Grenzwert für verfügbaren Speicherplatz (MB)** und tragen Sie im Eingabefeld den Grenzwert in Megabyte ein.
   - Wenn Sie den Ordner ändern möchten, in dem Objekte aus der Quarantäne wiederhergestellt werden, geben Sie im Eingabefeld **Ordner für die Wiederherstellung von Objekten** den vollständigen Pfad zum Ordner auf einem lokalen Laufwerk des geschützten Servers an.
6. Klicken Sie auf **OK**.

Die vorgenommenen Quarantäne- und Backup-Einstellungen werden gespeichert.

Blockierung nicht vertrauenswürdiger Geräte. Liste der nicht vertrauenswürdigen Computer

In diesem Abschnitt wird beschrieben, wie nicht vertrauenswürdige Computer blockiert und die Speichereinstellungen für blockierte Geräte angepasst werden.

In diesem Abschnitt

Über Blockieren des Zugriffs auf Netzwerk-Dateiressourcen

Der Speicher für blockierte Geräte wird standardmäßig während der Installation auf einer der folgenden Komponenten installiert: Echtzeitschutz, Anti-Cryptor für NetApp, Schutz vor Verschlüsselung. Die Komponenten überwachen gemäß der Liste der nicht vertrauenswürdigen Computer die Versuche von Remote-Computern, auf die Netzwerkfreigaben des geschützten Servers oder auf die Ordner des Netzwerkspeichers zuzugreifen. Informationen über blockierte Computer auf allen geschützten Servern werden an das Kaspersky Security Center gesendet. Kaspersky Security 10.1 für Windows Server blockiert für alle Remote-Computer auf der Liste der nicht vertrauenswürdigen Computer den Zugriff auf die Netzwerkfreigaben des Servers oder die Ordner des Netzwerkspeichers.

Der Speicher für blockierte Geräte wird befüllt, wenn zumindest eine der folgenden Aufgaben im aktiven Modus gestartet wird und die festgelegten Bedingungen erfüllt sind:

- Wenn während der Ausführung der Aufgabe zum Echtzeitschutz für Dateien eine bösartige Aktivität eines Computers gefunden wird, der auf einen freigegebenen Netzwerkordner zugreift, und in den Einstellungen der Aufgabe zum Echtzeitschutz für Dateien das Kontrollkästchen **Computer, von denen schädliche Aktivitäten ausgehen, in die Liste der nicht vertrauenswürdigen Computer aufnehmen** aktiviert ist.
- Wenn während der Ausführung der Aufgabe zum Schutz vor Verschlüsselung eine Verschlüsselung durch einen Computer gefunden wird, der auf freigegebene Netzwerkordner zugreift.
- Wenn während der Ausführung der Aufgabe "Anti-Cryptor für NetApp" ein Ransomware-Angriff auf den Netzwerkspeicher gefunden wird.

Nachdem die schädliche Aktivität oder der Verschlüsselungsversuch erkannt wurde, sendet die Aufgabe Informationen über den angreifenden Computer an den Speicher für blockierte Geräte, und das Programm erstellt ein kritisches Ereignis für die Blockierung des Computers. Sämtliche von diesem Computer ausgehenden Zugriffsversuche auf geschützte Netzwerkfreigaben werden blockiert.

Standardmäßig entfernt Kaspersky Security 10.1 für Windows Server nicht vertrauenswürdige Computer innerhalb von 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 nicht vertrauenswürdigen Computer gelöscht wurden. Sie können einen Zeitpunkt angeben, nach dem die blockierten Computer automatisch freigegeben werden.

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 Verschlüsselung
- Anti-Cryptor für NetApp

► *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>** > **Echtzeitschutz** > **Einstellungen** im Block **Echtzeitschutz für Dateien**.

   Das Fenster **Echtzeitschutz** 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 Security 10.1 für Windows Server 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 starten**.
   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.

5. Klicken Sie im Fenster **Echtzeitschutz** auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

► *Aufgabe zum Schutz vor Verschlüsselung 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>** > **Netzwerküberwachung** > **Einstellungen** im Block **Schutz vor Verschlüsselung**.

   Das Fenster **Schutz vor Verschlüsselung** wird geöffnet.
3. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Aufgabenverwaltung**.
   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.
   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.
4. Klicken Sie im Fenster **Schutz vor Verschlüsselung** auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

► *Anti-Cryptor für NetApp 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>** > **Schutz für Netzwerkspeicher** > **Einstellungen** im Block **Anti-Cryptor für NetApp**.

   Das Fenster **Anti-Cryptor für NetApp** wird geöffnet.
3. Wenn die Aufgabe nicht gestartet wurde, öffnen Sie die Registerkarte **Aufgabenverwaltung**.
   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.
   b. Wählen Sie die Frequenz **Bei Programmstart** in der Dropdown-Liste aus.
4. Klicken Sie im Fenster **Anti-Cryptor für NetApp** auf **OK**.

Kaspersky Security 10.1 für Windows Server blockiert den Zugriff auf freigegebene Netzwerkordner für Computer, auf denen schädliche oder Verschlüsselungsaktivitäten festgestellt werden.

Einstellungen für blockierte Geräte anpassen

► *Um die Einstellungen für blockierte Geräte anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center das Fenster Programmeinstellungen (siehe Abschnitt "Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen" auf S. 125).
2. Klicken Sie im Abschnitt **Zusätzlich** auf die Schaltfläche **Einstellungen** im Block **Speicher**.

   Das Fenster **Speichereinstellungen** wird geöffnet.

Sie können die Einstellungen für die Computersperrung für die Gruppe der verwalteten Server über die Richtlinieneinstellungen anpassen. Um die Einstellungen für die Computersperrung anzupassen, öffnen Sie **<Name der Richtlinie>** > **Erweitert** und klicken Sie auf die Schaltfläche **Einstellungen**. Passen Sie auf der Registerkarte **Liste der nicht vertrauenswürdigen Computer** die Einstellungen für die Computersperrung an. Die Liste der nicht vertrauenswürdigen Computer ist in den Richtlinieneinstellungen nicht verfügbar.

3. Öffnen Sie die Registerkarte **Liste der nicht vertrauenswürdigen Computer**.
4. Geben Sie im Block **Einstellungen für die Computersperrung** die Anzahl der Tage, Stunden und Minuten an, nach deren Ablauf die blockierten Computer wieder Zugriff auf die freigegebenen Netzwerkordner erhalten sollen.
5. Klicken Sie auf die Schaltfläche **Liste der nicht vertrauenswürdigen Computer**.
6. Führen Sie eine der Aktionen durch:
   - Wählen Sie im folgenden Fenster **Liste der nicht vertrauenswürdigen Computer** die Computer aus, für die Sie den Zugriff wieder freigeben möchten, und klicken Sie auf die Schaltfläche **Aus Liste löschen**.
   - Klicken Sie auf **Gesamte Liste leeren**, um Computer aus der Liste der nicht vertrauenswürdigen Computer zu entfernen und den Zugriff für alle blockierten Computer wieder freizugeben.
7. Klicken Sie auf **OK**.

   Die ausgewählten Computer werden freigegeben und aus der Liste der nicht vertrauenswürdigen Computer gelöscht.
8. Klicken Sie im Fenster **Speichereinstellungen** auf **OK**.

Die vorgenommenen Einstellungen für nicht vertrauenswürdige Computer werden gespeichert.

Über die Konfiguration von Berichten und Benachrichtigungen

In der Verwaltungskonsole von Kaspersky Security Center können Sie die Benachrichtigung an den Administrator und an die Benutzer für folgende Ereignisse anpassen, die mit der Arbeit von Kaspersky Security 10.1 für Windows Server und dem Status des Antiviren-Schutzes für den geschützten Server zusammenhängen:

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

Sie können die Ereignisbenachrichtigungen für Kaspersky Security 10.1 für Windows Server entweder für einen Computer im Fenster **Eigenschaften: <Computername>**oder für eine Computergruppe im Fenster **Eigenschaften: <Name der Richtlinie>** der ausgewählten Administrationsgruppe anpassen.

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

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

- Im Fenster **Benachrichtigungen anpassen** können Sie Benachrichtigungen sowohl für den Administrator als auch für Benutzer einstellen.

  Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

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

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

In diesem Abschnitt

Protokolleinstellungen anpassen

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

► *Um die Berichte für Kaspersky Security 10.1 für Windows Server anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.

- Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Berichte und Benachrichtigungen** im Block **Berichte über Aufgabenausführung** auf die Schaltfläche **Einstellungen**.
4. Passen Sie im Fenster **Einstellungen für Berichte** die folgenden Eigenschaften für Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server, deren Genauigkeitsstufe für Ereignisse Sie festlegen möchten.
     b. Um eine Genauigkeitsstufe in den Berichten über Aufgabenausführung und im Systemaudit-Bericht einer bestimmten Komponente anzugeben, wählen Sie die entsprechende Stufe in der Liste **Ereigniskategorie** aus.
   - Um den Standardordner für Berichten zu ändern, geben Sie den Ordnerpfad an oder wählen Sie den Ordner mit Hilfe der Schaltfläche **Durchsuchen** aus.
   - Geben Sie an, wie viele Tage die Berichte über Aufgabenausführung gespeichert bleiben sollen.
   - Geben Sie an, wie viele Tage die im Knoten **Systemaudit-Bericht** angezeigten Informationen gespeichert werden sollen.
5. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für Berichte werden gespeichert.

Sicherheits-Ereignisbericht

Kaspersky Security 10.1 für Windows Server führt einen Sicherheits-Ereignisbericht über Ereignisse, die mit einer Verletzung der Sicherheit oder einer versuchten Verletzung der Sicherheit auf dem geschützten Server verbunden sind. In diesem Bericht werden folgende Ereignisse registriert:

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

Sie können den Sicherheits-Ereignisbericht wie auch den Systemaudit-Bericht leeren. Dabei registriert Kaspersky Security 10.1 für Windows Server ein Ereignis des Systemaudits über das Leeren des Sicherheits-Ereignisberichts.

Anpassen der Einstellungen der SIEM-Integration

Um die Belastung für leistungsschwache Geräte zu reduzieren und die Gefahr eines Abfalls der Systemleistung infolge eines zu großen Umfangs der Programmberichte zu verringern, können Sie die Veröffentlichung

der Audit-Ereignisse und der Ereignisse der Aufgabenausführung über das Protokoll syslog auf dem *syslog-Server* einrichten.

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

Sie können die SIEM-Integration in zwei Modi verwenden:

- Ereignisse auf dem syslog-Server duplizieren: In diesem Modus wird davon ausgegangen, dass alle Ereignisse der Aufgabenausführung, deren Veröffentlichung in den Berichtseinstellungen konfiguriert wurde, sowie alle Ereignisse des Systemaudits nach dem Versand an SIEM auch weiterhin auf dem lokalen Computer gespeichert werden.

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

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

  Das Programm löscht niemals lokale Versionen des Berichts für Sicherheitsverletzungen.

Kaspersky Security 10.1 für Windows Server kann die Ereignisse in den Programmberichten in die vom syslog-Server unterstützten Formate konvertieren, damit sie von SIEM empfangen und erfolgreich identifiziert werden können. Das Programm unterstützt die Konvertierung von Ereignissen in ein Format für strukturierte Daten und in das JSON-Format.

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

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

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

Tabelle 30. Einstellungen für die SIEM-Integration

Einstellung	Standardwert	Beschreibung
Ereignisse über das syslog-Protokoll an den externen syslog-Server senden	Wird nicht verwendet	Sie können die SIEM-Integration mithilfe dieses Kontrollkästchens aktivieren und deaktivieren.
Lokale Kopien von Ereignissen beim Schreiben auf einen externen syslog-Server löschen	Wird nicht verwendet	Sie können die Speicherung lokaler Kopien der Berichte nach ihrem Versand an SIEM mithilfe dieses Kontrollkästchens konfigurieren.

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

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Berichte und Benachrichtigungen** im Block **Berichte über Aufgabenausführung** auf die Schaltfläche **Einstellungen**.

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

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

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

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

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

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

   Das Kontrollkästchen ist standardmäßig deaktiviert.

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

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

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

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

   Das Kontrollkästchen ist standardmäßig deaktiviert.

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

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

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

8. Gehen Sie im Block **Verbindungseinstellungen** wie folgt vor:

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

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

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

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

9. Klicken Sie auf **OK**.

Die angepassten Einstellungen der SIEM-Integration werden übernommen.

Benachrichtigungseinstellungen anpassen

► *Um die Benachrichtigungen für Kaspersky Security 10.1 für Windows Server anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Berichte und Benachrichtigungen** im Block **Ereignisbenachrichtigungen** auf die Schaltfläche **Einstellungen**.
4. Passen Sie im Fenster **Benachrichtigungen anpassen** die folgenden Eigenschaften für Kaspersky Security 10.1 für Windows Server gemäß Ihren Anforderungen an:
   - Wählen Sie in der Liste **Benachrichtigungen anpassen** den Benachrichtigungstyp aus, dessen Einstellungen Sie anpassen möchten.
   - Passen Sie im Block **Benachrichtigung für die Benutzer** die Methode für die Benachrichtigung der Benutzer an. Geben Sie bei Bedarf einen Benachrichtigungstext ein.
   - Passen Sie im Block **Benachrichtigung für die Administratoren** die Methode für die Benachrichtigung von Administratoren an. Geben Sie bei Bedarf einen Benachrichtigungstext ein. Passen Sie bei Bedarf die erweiterten Benachrichtigungseinstellungen über die Schaltfläche **Einstellungen** an.
   - Geben Sie im Block **Grenzwerte für Ereigniserstellung** die Zeitintervalle an, nach deren Ablauf Kaspersky Security 10.1 für Windows Server die Ereignisse *"Programm-Datenbanken sind veraltet", "Programm-Datenbanken sind stark veraltet"* und *"Untersuchung wichtiger Bereiche des Computers wurde lange nicht ausgeführt"* protokolliert.
     - **Programm-Datenbanken sind veraltet (Tage)**

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

Der Standardwert beträgt 7 Tage.

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

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

  Der Standardwert beträgt 14 Tage.

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

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

  Der Standardwert beträgt 30 Tage.

5. Klicken Sie auf **OK**.

Die festgelegten Benachrichtigungseinstellungen werden gespeichert.

Interaktion mit dem Administrationsserver konfigurieren

► *Um die Typen der Objekte auszuwählen, über die Kaspersky Security 10.1 für Windows Server Informationen an den Kaspersky Security Center-Administrationsserver übergeben soll, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Netzwerklisten des Administrationsservers** wird geöffnet.
4. Wählen Sie im folgenden Fenster die Objekttypen aus, über die Kaspersky Security 10.1 für Windows Server Informationen an den Kaspersky Security Center-Administrationsserver übergeben soll:
   - Daten zu Quarantäne-Objekten
   - Daten zu Backup-Objekten
   - Informationen zu nicht vertrauenswürdigen Computern
5. Klicken Sie auf **OK**.

Kaspersky Security 10.1 für Windows Server wird Informationen über die ausgewählten Objekttypen an den Administrationsserver übertragen.

Echtzeitschutz

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

In diesem Kapitel

Echtzeitschutz für Dateien

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

In diesem Abschnitt

Über die Aufgabe zum Echtzeitschutz für Dateien

Bei Ausführung der Aufgabe zum Echtzeitschutz für Dateien untersucht Kaspersky Security 10.1 für Windows Server folgende Objekte des geschützten Servers, wenn auf diese zugegriffen wird:

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

Wenn ein Programm eine Datei auf dem Server speichert oder eine Datei vom Server abruft, fängt Kaspersky Security 10.1 für Windows Server diese Datei ab, untersucht sie auf Bedrohungen und führt bei gefundenen Bedrohungen die in den Einstellungen der Aufgabe festgelegten bzw. standardmäßigen Aktionen aus: Es wird

versucht, die Datei zu desinfizieren, die Datei in die Quarantäne zu verschieben oder sie zu löschen. Kaspersky Security 10.1 für Windows Server gibt die Datei dem Programm zurück, wenn sie nicht infiziert ist oder erfolgreich desinfiziert wurde.

Kaspersky Security 10.1 für Windows Server fängt Dateioperationen ab, die in Containern von Windows Server 2016 ausgeführt werden.

Ein Container ist eine isolierte Umgebung, in der Programme ausgeführt werden können, ohne sich auf das Betriebssystem auszuwirken oder von diesem beeinträchtigt zu werden. Wenn der Container sich innerhalb des Schutzbereichs der Aufgabe befindet, untersucht Kaspersky Security 10.1 für Windows Server die Container-Dateien, auf die zugegriffen wird, auf Bedrohungen der Computer-Sicherheit. Wenn eine Bedrohung gefunden wird, versucht das Programm, den Container zu desinfizieren. Ist der Versuch erfolgreich, setzt der Container seine Ausführung fort; misslingt die Desinfektion, so wird der Container deaktiviert.

Kaspersky Security 10.1 für Windows Server erkennt außerdem Schadsoftware für Prozesse, die unter Windows Subsystem for Linux® laufen. Bei solchen Prozessen wendet die Aufgabe "Echtzeitschutz für Dateien" die von der aktuellen Konfiguration festgelegte Aktion an.

Aufgabe zum Echtzeitschutz für Dateien anpassen

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

Tabelle 31. Standardeinstellungen der Aufgabe Echtzeitschutz für Dateien

Einstellung	Standardwert	Beschreibung
Schutzbereich	Gesamter Computer ohne virtuelle Festplatten	Sie können den Schutzbereich beschränken.
Sicherheitsstufe	Einheitlich für den gesamten Schutzbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Sie können für bestimmte Knoten in der Dateistruktur des Computers: • Eine andere vordefinierte Sicherheitsstufe übernehmen. • Sicherheitsstufe manuell ändern. • Sicherheitseinstellungen des ausgewählten Knotens in eine Vorlage speichern, um sie später für andere Knoten zu übernehmen.
Schutzmodus für Objekte	Beim Öffnen und Ändern	Sie können den Schutzmodus für Objekte festlegen, also die Zugriffsart angeben, bei der Objekte von Kaspersky Security 10.1 für Windows Server 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.
Verwendung von KSN	Wird verwendet	Sie können Ihren Computer durch die Nutzung der Cloud-Dienste von Kaspersky Security Network effektiver schützen.

Einstellung	Standardwert	Beschreibung
Zeitplan für den Aufgabenstart	Bei Programmstart	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.
Computer, von denen schädliche Aktivitäten ausgehen, in die Liste der nicht vertrauenswürdigen Computer aufnehmen	Wird nicht verwendet	Sie können das Hinzufügen von Computern, bei denen schädliche Aktivitäten festgestellt wurden, in die Liste der nicht vertrauenswürdigen Computer aktivieren.

► *Um die Aufgabe Echtzeitschutz für Dateien zu konfigurieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Echtzeitschutz für Dateien** wird geöffnet.
4. Konfigurieren Sie folgende Aufgabeneinstellungen:
   - Auf der Registerkarte **Allgemein**:
     - Schutzmodus (siehe Abschnitt "Schutzmodus auswählen" auf S. 183)
     - Heuristische Analyse verwenden (auf Seite 182)
     - Einstellungen für die Integration mit anderen Komponenten von Kaspersky Security 10.1 für Windows Server
   - Auf der Registerkarte **Aufgabenverwaltung**:
     - Einstellungen für den Start der Aufgabe nach Zeitplan (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite. 148).
5. Wählen Sie die Registerkarte **Schutzbereich** aus und gehen Sie wie folgt vor:
   - Klicken Sie auf die Schaltfläche **Hinzufügen** oder **Ändern**, um den Schutzbereich zu ändern (siehe Abschnitt "Schutzbereich für die Aufgabe Echtzeitschutz für Dateien" auf Seite 184).
     - Wählen Sie im geöffneten Fenster alles aus, was Sie in den Schutzbereich der Aufgabe

aufnehmen wollen:

- **Vordefinierter Bereich**
- **Laufwerk, Ordner oder Netzwerkobjekt**
- **Datei**

- Wählen Sie eine der vordefinierten Sicherheitsstufen aus (siehe Abschnitt "Vordefinierte Sicherheitsstufen wählen" auf Seite. 185) oder passen Sie die Schutzeinstellungen manuell an (siehe Abschnitt "Sicherheitseinstellungen manuell anpassen" auf S. 187).

Um auf die Aufgabe neue Einstellungen des Schutzbereichs anzuwenden, muss die Aufgabe zum Echtzeitschutz für Dateien neu gestartet werden.

6. Klicken Sie im Fenster **Echtzeitschutz für Dateien** auf **OK**.

Kaspersky Security 10.1 für Windows Server 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 Bericht über Aufgabenausführung gespeichert.

Heuristische Analyse verwenden

Sie können die heuristische Analyse verwenden und die Analysestufe für Aufgaben von Kaspersky Security 10.1 für Windows Server anpassen.

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

1. Öffnen Sie die Programmeinstellungen (siehe Abschnitt "Über die Methoden zur Verwaltung von Kaspersky Security 10.1 für Windows Server durch Kaspersky Security Center" auf Seite 151) oder Richtlinieneinstellungen (siehe Abschnitt "Richtlinie anpassen" auf Seite 111), für die Sie die heuristische Analyse anpassen möchten.
2. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der heuristischen Analyse bei der Objektuntersuchung.

   Wenn dieses Kontrollkästchen aktiviert ist, ist die heuristische Analyse aktiviert.

   Wurde dieses Kontrollkästchen deaktiviert, ist die heuristische Analyse deaktiviert.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
3. Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.

   Mit dem Schieberegler lässt sich die Stufe die Ebene der heuristischen Analyse regulieren. Die Genauigkeitsstufe der Untersuchung regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach Bedrohungen, dem Auslastungsniveau der Betriebssystemressourcen und der Untersuchungsdauer.

   Für die Untersuchung sind folgende Genauigkeitsstufen vorgesehen:

   - **Oberflächlich**. Bei der heuristischen Analyse wird eine relativ geringe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. In diesem Modus besteht eine geringere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung beansprucht weniger Systemressourcen und wird

schneller ausgeführt.

- **Mittel**. Die Anzahl der Befehle, die bei der heuristischen Analyse in der ausführbaren Datei ausgeführt werden, richtet sich nach den Empfehlungen der Kaspersky-Lab-Experten.

  Diese Stufe gilt als Standard.

- **Tief**. Bei der heuristischen Analyse wird eine relativ hohe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. Bei dieser Einstellung besteht eine höhere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung benötigt mehr Systemressourcen und mehr Zeit und kann eine erhöhte Anzahl an Fehlalarmen auslösen.

  Der Schieberegler ist aktiv, wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist.

4. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe werden unverzüglich während der Ausführung der Aufgabe angewandt. Wenn die Aufgabe nicht ausgeführt wird, werden die geänderten Einstellungen beim nächsten Aufgabenstart übernommen.

Schutzmodus auswählen

Sie können den Schutzmodus in der Aufgabe Echtzeitschutz für Dateien auswählen. Im Block **Schutzmodus für Objekte** können Sie festlegen, bei welcher Art des Zugriffs auf die Objekte Kaspersky Security 10.1 für Windows Server eine Untersuchung durchführt.

Die Einstellung **Schutzmodus für Objekte** hat einen einheitlichen Wert für den gesamten Schutzbereich, der in der Aufgabe vorgegeben ist. Für diese Einstellung können keine unterschiedlichen Werte für einzelne Knoten des Schutzbereichs festgelegt werden.

► *Um den Schutzmodus für Objekte auszuwählen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

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

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

   - **Intelligenter Modus**

     Kaspersky Security 10.1 für Windows Server wählt die Objekte für die Untersuchung selbstständig aus. Das Objekt wird beim Öffnen untersucht und nochmals nach seiner Speicherung, sofern das Objekt geändert wurde. Wenn ein Prozess mehrmals auf das Objekt zugreift und es verändert, untersucht Kaspersky Security 10.1 für Windows Server das Objekt erst dann erneut, wenn es von diesem Prozess zum letzten Mal gespeichert wird.

   - **Beim Öffnen und Ändern**

     Kaspersky Security 10.1 für Windows Server untersucht ein Objekt beim Öffnen und, falls es verändert wurde, erneut beim Speichern.

     Diese Variante gilt als Standard.

   - **Beim Öffnen**

     Kaspersky Security 10.1 für Windows Server untersucht alle Objekte, wenn diese zum Lesen, zur Ausführung oder zum Ändern geöffnet werden.

   - **Beim Ausführen**

     Kaspersky Security 10.1 für Windows Server untersucht die Datei nur beim Öffnen zum Ausführen.

5. Klicken Sie auf **OK**.

Der ausgewählte Schutzmodus für die Objekte wird eingestellt.

Schutzbereich für die Aufgabe Echtzeitschutz für Dateien

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

In diesem Abschnitt

Vordefinierte Schutzbereiche

Die Dateiressourcen des geschützten Servers werden in den Einstellungen der Aufgabe **Echtzeitschutz für Dateien** auf der Registerkarte **Schutzbereich** angezeigt.

Die Dateistruktur oder Liste der Dateiressourcen des Computers enthält die Knoten, für die Sie nach den Sicherheitseinstellungen in Microsoft Windows über Leserechte verfügen.

Kaspersky Security 10.1 für Windows Server deckt die folgenden vordefinierten Schutzbereiche ab:

- **Lokale Festplatten**. Kaspersky Security 10.1 für Windows Server schützt Dateien auf den Festplatten des Servers.
- **Wechseldatenträger**. Kaspersky Security 10.1 für Windows Server schützt Dateien auf externen Geräten, z. B. auf CDs oder USB-Laufwerken. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Schutzbereich aufnehmen oder aus diesem ausschließen.
- **Netzwerkumgebung**. Kaspersky Security 10.1 für Windows Server schützt die Dateien, die in Netzwerkordnern gespeichert sind oder aus diesen von auf dem Server laufenden Programmen abgefragt werden. Kaspersky Security 10.1 für Windows Server schützt Dateien in Netzwerkordnern nicht, wenn Programme von anderen Rechnern aus darauf zugreifen.
- **Virtuelle Festplatten**. Sie können in den Schutzbereich dynamische Ordner und Dateien sowie Laufwerke aufnehmen, die vorübergehend auf dem Server eingebunden werden, z. B. gemeinsame Cluster-Laufwerke.

Die vordefinierten Schutzbereiche 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 Schutzbereichs verfügbar.

Standardmäßig sind alle vordefinierten Bereiche mit Ausnahme von virtuellen Festplatten in den Schutzbereich eingeschlossen.

Virtuelle Festplatten, die mit dem Befehl SUBST erzeugt wurden, werden in der Dateistruktur des Servers in der Konsole für Kaspersky Security 10.1 nicht angezeigt. Um Objekte auf einer virtuellen Festplatte in den Schutzbereich aufzunehmen, schließen Sie den Ordner auf dem Server, mit dem diese virtuelle Festplatte verbunden ist, in den Schutzbereich ein.
Verbundene Netzlaufwerke werden nicht in der Dateistruktur des Servers angezeigt. Um Objekte auf einem Netzwerk-Datenträger in den Schutzbereich aufzunehmen, geben Sie den Pfad des Ordners an, der diesem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

Vordefinierte Sicherheitsstufen wählen

Für Knoten, die in der Liste der Dateiressourcen des Computers ausgewählt sind, können Sie eine der folgenden vordefinierten Sicherheitsstufen festlegen: **Maximale Leistung**, **Empfohlen** oder **Maximale Sicherheit**. Jede dieser Stufen besitzt eine eigene Auswahl von Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird empfohlen, wenn es zusätzlich zur Verwendung von Kaspersky Security 10.1 für Windows Server auf Servern und Workstations noch weitere Sicherheitsmaßnahmen innerhalb Ihres Netzwerks gibt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Server. Diese Stufe ist laut Empfehlung der Experten von Kaspersky Lab für den Schutz von Servern in den meisten Unternehmensnetzwerken ausreichend. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximale Sicherheit

Die Sicherheitsstufe **Maximale Sicherheit** wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte

Anforderungen an die Computersicherheit hat.

Tabelle 32. Vordefinierte Sicherheitsstufen und entsprechende Einstellungswerte

Einstellungen	Sicherheitsstufe		
	Maximale Leistung	Empfohlen	Maximale Sicherheit
Schutz von Objekten	Nach Erweiterung	Nach Format	Nach Format
Nur neue und veränderte Dateien schützen	Aktiviert	Aktiviert	Deaktiviert
Aktion für infizierte und andere Objekte	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen	Zugriff verweigern und empfohlene Aktion ausführen	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte	Zugriff verweigern und in die Quarantäne verschieben	Zugriff verweigern und in die Quarantäne verschieben	Zugriff verweigern und in die Quarantäne verschieben
Dateien ausschließen	Nein	Nein	Nein
Nicht erkennen	Nein	Nein	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	60 Sek.	60 Sek.	60 Sek.
Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	8 MB	8 MB	Nicht konfiguriert.
Alternative NTFS-Ströme	Ja	Ja	Ja
Bootsektoren und MBR	Ja	Ja	Ja
Schutz von zusammengesetzten Objekten	• Gepackte Objekte* *Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Nur neue und veränderte	• SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* *Alle Objekte

Die Einstellungen **Schutz von Objekten**, **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden** und **Heuristische Analyse verwenden** sind nicht in den vordefinierten Sicherheitsstufen enthalten. Wenn Sie nach der Auswahl einer der vordefinierten Sicherheitsstufen die Sicherheitseinstellungen für **Schutz von Objekten**, **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden**, **Heuristische Analyse verwenden** verändern, wird dadurch die gewählte voreingestellte Sicherheitsstufe nicht geändert.

► *Um eine vordefinierte Sicherheitsstufe auszuwählen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.

2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

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

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

4. Wählen Sie auf der Registerkarte **Schutzbereich** den Knoten aus, dessen Sicherheitseinstellungen Sie anpassen möchten, und klicken Sie auf die Schaltfläche **Anpassen**.

   Das Fenster **Einstellungen für den Echtzeitschutz für Dateien anpassen** wird geöffnet.

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

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Kaspersky Security 10.1 für Windows Server 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 Bericht über Aufgabenausführung gespeichert.

Sicherheitseinstellungen manuell anpassen

Standardmäßig werden in der Aufgabe Echtzeitschutz für Dateien die gleichen Sicherheitsparameter verwendet wie für den gesamten Schutzbereich. Diese Einstellungen entsprechen den Werten der vordefinierten Sicherheitsstufe "Empfohlen" (siehe Abschnitt "Vordefinierte Sicherheitsstufen wählen" auf S. 185).

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

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

► *Um die Sicherheitsparameter eines bestimmten Knotens manuell anzupassen, gehen Sie wie*

folgt vor:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Echtzeitschutz für Dateien** wird geöffnet.
4. Wählen Sie auf der Registerkarte **Schutzbereich** den Knoten aus, dessen Sicherheitseinstellungen Sie anpassen möchten, und klicken Sie auf die Schaltfläche **Anpassen**.
5. Klicken Sie auf die Schaltfläche **Anpassen**, um die erforderlichen Sicherheitseinstellungen des ausgewählten Knotens nach Bedarf anzupassen. Gehen Sie hierzu wie folgt vor:
   - Konfigurieren Sie bei Bedarf auf der Registerkarte **Allgemein** folgende Parameter:

     Geben Sie im Block **Schutz von Objekten** die Objekte an, die Sie in den Schutzbereich einschließen möchten:
     - **Alle Objekte**

       Kaspersky Security 10.1 für Windows Server untersucht alle Objekte.
     - **Objekte, die nach Format untersucht werden**

       Kaspersky Security 10.1 für Windows Server untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats.

       Die Liste der Dateiformate wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Security 10.1 für Windows Server enthalten.
     - **Objekte, die nach der Erweiterungsliste aus den Antiviren-Datenbanken untersucht werden**

       Kaspersky Security 10.1 für Windows Server untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung.

       Die Erweiterungsliste wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Security 10.1 für Windows Server enthalten.
     - **Objekte, die nach der angegebenen Erweiterungsliste untersucht werden**

       Kaspersky Security 10.1 für Windows Server untersucht Dateien auf der Grundlage der Dateierweiterung. Die Dateierweiterungsliste können Sie im Fenster **Erweiterungsliste** mithilfe der Schaltfläche **Ändern** manuell anpassen.

- **Bootsektoren und MBR**

  Aktivierung des Schutzes für Laufwerk-Bootsektoren und Master Boot Records (MBR)

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server die Bootsektoren und Master Boot Records auf Festplatten und Wechseldatenträgern des Servers.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Alternative NTFS-Ströme**

  Untersuchung zusätzlicher Ströme von Dateien und Ordnern auf den Laufwerken des NTFS-Dateisystems.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server zusätzliche Ströme von Dateien und Ordnern.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Aktivieren oder deaktivieren Sie im Block **Optimierung** das Kontrollkästchen

- **Nur neue und veränderte Dateien schützen**

  Mit diesem Kontrollkästchen werden die Untersuchung und der Schutz von Dateien, die Kaspersky Security 10.1 für Windows Server als neu oder seit der letzten Untersuchung geändert erkennt, aktiviert oder deaktiviert.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht und schützt Kaspersky Security 10.1 für Windows Server nur die Dateien, die als neu oder seit der letzten Untersuchung verändert erkannt wurden.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht und schützt Kaspersky Security 10.1 für Windows Server alle Dateien.

  Das Kontrollkästchen ist für die Sicherheitsstufe **Maximale Leistung** standardmäßig aktiviert. Wurde die Sicherheitsstufe **Empfohlen** oder **Maximale Sicherheit** ausgewählt, ist das Kontrollkästchen deaktiviert.

Geben Sie im Block **Schutz von zusammengesetzten Objekten** die zusammengesetzten Objekte an, die Sie in den Schutzbereich einschließen möchten:

- **Alle / nur neue Archive**

  Untersuchung von Archiven in den Formaten ZIP, CAB, RAR, ARJ u. a.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Archive.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

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

  Selbstentpackende Archive untersuchen.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server SFX-Archive.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

Diese Einstellung ist aktiv, wenn das Kontrollkästchen **Archive** deaktiviert ist.

- **Alle / Nur neue E-Mail-Datenbanken**

  Dateien in Mail-Datenbanken für Microsoft Outlook und Microsoft Outlook Express werden untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Mail-Datenbankdateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Mail-Datenbankdateien von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle / nur neue gepackte Objekte**

  Untersuchung von ausführbaren Dateien, die mit Packprogrammen für Binärcode wie beispielsweise UPX oder ASPack gepackt wurden.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server ausführbare Dateien, die mit Packprogrammen gepackt wurden.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden ausführbare Dateien, die mit Packprogrammen gepackt wurden, von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle / nur neue Dateien in Mail-Formaten**

  Dateien in Mail-Formaten werden untersucht. Dazu zählen beispielsweise Nachrichten der Formate Microsoft Outlook und Microsoft Outlook Express.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Dateien in Mail-Formaten.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Dateien in Mail-Formaten von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

- **Alle / Nur neue eingebettete OLE-Objekte**

  Untersuchung von Objekten, die in eine Datei eingebettet sind (beispielsweise Excel-Tabellen, Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten).

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Objekte, die in eine Datei eingebettet sind.

  Wenn dieses Kontrollkästchen deaktiviert ist, werden Objekte, die in eine Datei eingebettet sind, von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

  Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

Sie können den Schutz aller oder nur neuer zusammengesetzter Objekte auswählen, wenn das Kontrollkästchen **Nur neue und veränderte Dateien schützen** aktiviert ist. Ist das Kontrollkästchen **Nur neue und veränderte Dateien schützen** deaktiviert, schützt Kaspersky Security 10.1 für Windows Server alle angegebenen zusammengesetzten Objekte.

- Konfigurieren Sie bei Bedarf auf der Registerkarte **Aktionen** folgende Parameter:
  - Wählen Sie die Aktion für infizierte und andere gefundene Objekte aus.
  - Wählen Sie eine Aktion für möglicherweise infizierte Objekte
  - Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an.
  - Wählen Sie Aktionen für nicht desinfizierbare zusammengesetzte Objekte Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Nicht desinfizierbare zusammengesetzte Objekte vollständig entfernen, wenn eingebettete infizierte oder andere Objekte gefunden werden**.

    Dieses Kontrollkästchen aktiviert bzw. deaktiviert das erzwungene Löschen einer übergeordneten Containerdatei, wenn ein eingebettetes infiziertes oder sonstiges Objekt gefunden wird.

    Wenn das Kontrollkästchen aktiviert ist und als Aktion für infizierte und möglicherweise infizierte Objekte die Aktion **Zugriff verweigern und löschen** ausgewählt wurde, erzwingt Kaspersky Security 10.1 für Windows Server das Löschen des gesamten übergeordneten Containers, wenn darin ein schädliches oder ein sonstiges Objekt gefunden wird. Das erzwungene Löschen eines übergeordneten Containers mit seinem Gesamtinhalt wird ausgeführt, wenn es dem Programm nicht gelingt, nur das eingebettete gefundene Objekt zu löschen (z. B. wenn der übergeordnete Container nicht bearbeitet werden kann).

    Wenn das Kontrollkästchen deaktiviert ist und als Aktion für infizierte und möglicherweise infizierte Objekte die Aktion **Zugriff verweigern und löschen** ausgewählt wurde, führt Kaspersky Security 10.1 für Windows Server die festgelegte Aktion für den übergeordneten Container nicht aus, wenn darin ein schädliches oder ein sonstiges Objekt gefunden wird und der übergeordnete Container nicht bearbeitet werden kann.

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

- Konfigurieren Sie bei Bedarf auf der Registerkarte **Optimierung** folgende Parameter:

  Im Block **Ausnahmen**:

  - **Dateien ausschließen**

    Ausnahme von Dateien nach Dateiname oder Dateinamensmaske von der Untersuchung.

    Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server die angegebenen Objekte bei der Untersuchung.

    Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server alle Objekte.

    Das Kontrollkästchen ist standardmäßig deaktiviert.

  - **Nicht erkennen**

    Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Website der Viren-Enzyklopädie https://de.securelist.com/.

    Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server die angegebenen gefundenen Objekte bei der Untersuchung.

    Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Security 10.1 für Windows

Server alle Objekte, die im Programm standardmäßig angegeben sind.

Das Kontrollkästchen ist standardmäßig deaktiviert.

Im Block **Erweiterte Einstellungen**:

- **Untersuchung beenden, wenn sie länger dauert als (Sek.)**

  Beschränkung der Untersuchungsdauer für ein Objekt. Als Standard gilt der Wert 60 Sek.

  Wenn dieses Kontrollkästchen aktiviert ist, wird die maximale Untersuchungsdauer für ein Objekt auf den festgelegten Wert begrenzt.

  Wenn dieses Kontrollkästchen deaktiviert ist, gilt keine Beschränkung für die Untersuchungsdauer.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)**

  Ausnahme zusammengesetzter Objekte, die die maximale Größe übersteigen, von der Untersuchung.

  Wenn dieses Kontrollkästchen aktiviert ist, werden zusammengesetzte Objekte, deren Größe über dem festgelegten Wert liegt, von Kaspersky Security 10.1 für Windows Server bei der Untersuchung auf Viren übersprungen.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server zusammengesetzte Objekte unabhängig von der Größe.

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

- **iChecker-Technologie verwenden**

  Es werden nur neue oder seit der letzten Untersuchung veränderte Dateien untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server nur neue oder seit der letzten Untersuchung veränderte Dateien.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Dateien unabhängig vom Erstellungs- oder Änderungsdatum.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **iSwift-Technologie verwenden**

  Es werden nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems untersucht.

  Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server nur neue oder seit der letzten Untersuchung veränderte Objekte des NTFS-Dateisystems.

  Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Dateien des NTFS-Systems unabhängig vom Erstellungs- oder Änderungsdatum.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Verwendung von KSN

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

In diesem Abschnitt

Über die Aufgabe „Verwendung von KSN"

Kaspersky Security Network (im Weiteren auch KSN) ist eine Infrastruktur von Online-Diensten, die den umfassenden Zugriff auf die Kaspersky-Lab-Wissensdatenbank über die Reputation von Dateien, Web-Ressourcen und Programmen gewährleistet. Die Nutzung der Daten durch Kaspersky Security Network gewährleistet eine schnellere Reaktion von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server erhält von Kaspersky Security Network ausschließlich Informationen über die Reputation von Programmen.

Die Teilnahme von Benutzern an KSN ermöglicht es Kaspersky Lab, schnell Informationen über Typen und Quellen neuer Bedrohungen zu erhalten, Neutralisierungsmethoden zu entwickeln und die Anzahl an Fehlalarmen der Programmkomponenten zu reduzieren.

Ausführliche Informationen über die Übertragung, Verarbeitung, Speicherung und Vernichtung von Daten über die Programmnutzung finden Sie im Fenster "Datenverarbeitung" der Aufgabe "Verwendung von KSN" sowie in der Datenschutzrichtlinie auf der Website von Kaspersky Lab.

Die Teilnahme an Kaspersky Security Network ist freiwillig. Sie können nach der Installation von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server verwendet werden:

- Echtzeitschutz für Dateien
- Untersuchung auf Befehl
- Kontrolle des Programmstarts

- Schutz des Datenverkehrs
- Schutz von per RPC-Protokoll verbundenen Netzwerkspeichern
- Schutz von per ICAP-Protokoll verbundenen Netzwerkspeichern.

Kaspersky Private Security Network

Ausführliche Informationen über die Konfiguration von Kaspersky Private Security Network (im Weiteren "KPSN") finden Sie im *Hilfesystem von Kaspersky Security Center*.

Wenn Sie Kaspersky Private Security Network auf dem geschützten Computer verwenden, können Sie im Fenster **Datenverarbeitung** (s. Abschnitt "Datenverarbeitung konfigurieren" auf S. 197) der Aufgabe "Verwendung von KSN" die KPSN-Erklärung lesen und die Aufgabe jederzeit mithilfe der Option **Ich akzeptiere die Bedingungen zur Teilnahme an Kaspersky Private Security Network** aktivieren. Indem Sie die Bedingungen akzeptieren, erklären Sie sich damit einverstanden, alle in der KPSN-Erklärung angeführten Datentypen (Sicherheitsanfragen, Statistikdaten) automatisch an den KSN-Dienst zu senden.

Nach der Annahme der KPSN-Bedingungen sind die Kontrollkästchen für die Verwendung von Global KSN nicht mehr verfügbar.

Wenn Sie KPSN deaktivieren, während die Aufgabe "Verwendung von KSN" läuft, wird der Fehler *Lizenzverletzung* angezeigt und die Aufgabe beendet. Um den Computer weiterhin zu schützen, müssen Sie die Erklärung zu Global KSN im Fenster **Datenverarbeitung** annehmen und die Aufgabe neu starten.

Konfiguration der Aufgabe Verwendung von KSN

Der Start der Aufgabe Verwendung von KSN ist nicht möglich, wenn die KSN-Erklärung nicht akzeptiert wurde.

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

Tabelle 33. Standardeinstellungen für die Aufgabe "Verwendung von KSN"

Einstellung	Standardwert	Beschreibung
Aktion für Objekte, die in KSN nicht vertrauenswürdig sind	**Löschen**	Sie können die Aktionen festlegen, die Kaspersky Security 10.1 für Windows Server in Bezug auf Objekte ausführen soll, die laut KSN als infiziert eingestuft sind.

Einstellung	Standardwert	Beschreibung
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 Security 10.1 für Windows Server den MD5-Hash für Dateien beliebiger Größe.
Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren	Nicht akzeptiert	Entscheiden Sie nach der Installation, ob Sie an KSN teilnehmen möchten. Sie können Ihre Entscheidung jederzeit ändern.
Der Verarbeitung von Daten als Teil der Statistik in Kaspersky Security Network zustimmen	Nicht akzeptiert	Wenn die KSN-Erklärung akzeptiert wurde, wird die KSN-Statistik automatisch gesendet, wenn Sie dieses Kontrollkästchen nicht deaktivieren.
Bedingungen der Erklärung zu Kaspersky Managed Protection akzeptieren	Nicht akzeptiert	Sie können den KMP-Dienst aktivieren oder deaktivieren. Dieser Dienst ist nur verfügbar, wenn beim Kauf des Programms der entsprechende Lizenzvertrag unterzeichnet wurde.
Aufgabenstart	Der erste Start ist nicht festgelegt.	Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

Um die Einstellungen der Aufgabe Verwendung von KSN zu konfigurieren, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

von KSN.

Das Fenster **Aufgabeneinstellungen** wird geöffnet.

4. Passen Sie auf der Registerkarte **Allgemein** folgende Aufgabenparameter an:

   - Geben Sie im Block **Aktion für Objekte, die in KSN nicht vertrauenswürdig sind** die Aktion an, die Kaspersky Security 10.1 für Windows Server ausführen soll, wenn ein Objekt gefunden wird, das laut KSN als nicht vertrauenswürdig eingestuft ist:

     - **Löschen**

       Kaspersky Security 10.1 für Windows Server löscht Objekte, die laut KSN infiziert sind, und verschiebt eine Kopie davon ins Backup.

       Diese Variante gilt als Standard.

     - **Informationen protokollieren**

       Kaspersky Security 10.1 für Windows Server nimmt Informationen über erkannte Objekte, die laut KSN infiziert sind, in den Bericht über Aufgabenausführung auf. Das infizierte Objekt wird von Kaspersky Security 10.1 für Windows Server nicht gelöscht.

   - Begrenzen Sie im Block **Versand von Daten** die Größe der Dateien, für die eine Prüfsumme berechnet werden soll:

     - Aktivieren oder deaktivieren Sie das Kontrollkästchen **Keine Prüfsumme für den Versand an KSN berechnen für Dateien, die größer sind als (MB)**.

       Über dieses Kontrollkästchen lässt sich die Ermittlung der Prüfsumme von Dateien ab einer bestimmten Größe für den Versand dieser Informationen an die KSN-Dienste aktivieren bzw. deaktivieren.

       Wie viel Zeit die Ermittlung der Prüfsumme beansprucht, hängt von der Dateigröße ab.

       Ist das Kontrollkästchen aktiviert, wird die Prüfsumme für Dateien, deren Größe den in MB festgelegten Wert übersteigt, von Kaspersky Security 10.1 für Windows Server nicht ermittelt.

       Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Security 10.1 für Windows Server die Prüfsumme für Dateien beliebiger Größe.

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     a. Geben Sie bei Bedarf im Feld rechts die maximale Dateigröße an, bis zu der Kaspersky Security 10.1 für Windows Server die Prüfsumme berechnen soll.

     b. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Kaspersky Security Center als KSN-Proxyserver verwenden**.

        Mithilfe dieses Kontrollkästchens können Sie den Versand von Daten vom geschützten Server an KSN verwalten.

        Wenn das Kontrollkästchen deaktiviert ist, werden keine Daten vom Administrationsserver und vom geschützten Server an KSN gesendet. Abhängig von den Einstellungen kann der Sender jedoch Daten direkt an KSN senden (nicht über das Kaspersky Security Center). Die aktive Richtlinie legt fest, welche Datentypen direkt an KSN gesendet werden können.

        Wenn das Kontrollkästchen aktiviert ist, werden alle Daten über das Kaspersky Security Center an KSN gesendet.

        Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

Der KSN-Proxyserver kann nur aktiviert werden, wenn die KSN-Erklärung akzeptiert wurde und Kaspersky Security Center ordnungsgemäß konfiguriert ist. Weitere Informationen finden Sie im *Hilfesystem von Kaspersky Security Center*.

5. Passen Sie bei Bedarf den Zeitplan für den Aufgabenstart auf der Registerkarte **Aufgabenverwaltung** an. Sie können beispielsweise die Aufgabe nach Zeitplan starten und als Intervall **Bei Programmstart** angeben, wenn Sie möchten, dass die Aufgabe nach dem Neustart des Servers automatisch gestartet wird.

   Das Programm startet die Aufgabe Verwendung von KSN zukünftig nach Zeitplan.

6. Konfigurieren Sie die Datenverarbeitung (s. Abschnitt "Datenverarbeitung konfigurieren" auf S. 197), 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 Bericht über Aufgabenausführung gespeichert.

Datenverarbeitung konfigurieren

► *Um festzulegen, welche Daten von den KSN-Diensten verarbeitet werden, und die KSN-Erklärung zu akzeptieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.

   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Echtzeitschutz** auf die Schaltfläche **Datenverarbeitung** im Block **Verwendung von KSN**.

   Das Fenster **Datenverarbeitung** wird geöffnet.

4. Lesen Sie sich auf der Registerkarte **Dienste** die Erklärung durch und aktivieren Sie das Kontrollkästchen **Bedingungen der Erklärung zu Kaspersky Security Network akzeptieren**.

5. Um die Sicherheitsstufe zu erhöhen, werden die folgenden Kontrollkästchen automatisch aktiviert:

   - **Daten über untersuchte Dateien senden**.

     Ist dieses Kontrollkästchen aktiviert, sendet Kaspersky Security 10.1 für Windows Server

die Prüfsumme der untersuchten Dateien an Kaspersky Lab. Die Einstufung der Sicherheit jeder Datei basiert auf der von KSN bereitgestellten Reputation.

Ist dieses Kontrollkästchen deaktiviert, sendet Kaspersky Security 10.1 für Windows Server die Prüfsumme der Dateien nicht an KSN.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- **Daten über die angeforderte URLs senden**.

  Ist dieses Kontrollkästchen aktiviert, sendet Kaspersky Security 10.1 für Windows Server Daten über angeforderte Webressourcen einschließlich Webadressen an Kaspersky Lab. Die Einstufung der Sicherheit der angeforderten Webressourcen basiert auf der von KSN bereitgestellten Reputation.

  Wenn dieses Kontrollkästchen deaktiviert ist, wird die Reputation von URLs von Kaspersky Security 10.1 für Windows Server nicht im KSN überprüft.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

  Dieses Kontrollkästchen beeinflusst die Konfiguration der Aufgabe zum Schutz des Datenverkehrs.

Sie können diese Kontrollkästchen deaktivieren und das Senden zusätzlicher Daten jederzeit unterbinden.

6. Öffnen Sie die Registerkarte **Statistik**. Das Kontrollkästchen **Der Verarbeitung von Daten als Teil der Statistik in Kaspersky Security Network zustimmen** ist standardmäßig aktiviert. Sie können dieses Kontrollkästchen jederzeit deaktivieren, wenn Sie nicht möchten, dass Kaspersky Security 10.1 für Windows Server zusätzliche Statistikdaten an Kaspersky Lab sendet.

   Wenn dieses Kontrollkästchen aktiviert ist, sendet Kaspersky Security 10.1 für Windows Server Statistikdaten, einschließlich in der KSN-Erklärung erläuterte persönliche Daten. Die von Kaspersky Lab erhaltenen Daten werden dazu verwendet, um die Qualität der Programme und das Niveau des Erkennens von Bedrohungen zu steigern.

   Ist das Kontrollkästchen deaktiviert, versendet Kaspersky Security 10.1 für Windows Server keine zusätzlichen Statistikdaten.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

7. Lesen Sie sich auf der Registerkarte **Kaspersky Managed Protection** die Erklärung durch und aktivieren Sie das Kontrollkästchen **Bedingungen der Erklärung zu Kaspersky Managed Protection akzeptieren**.

   Wenn das Kontrollkästchen aktiviert ist, stimmen Sie dem Versand von Statistikdaten über die Aktivität des geschützten Servers an die Spezialisten von Kaspersky Lab zu. Die empfangenen Daten werden für Analysen und Berichte rund um die Uhr verwendet, die zur Vermeidung von Sicherheitsverletzungen erforderlich sind.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Durch die Änderungen des Kontrollkästchens **Bedingungen der Erklärung zu Kaspersky Managed Protection akzeptieren** wird die Verarbeitung der Daten nicht sofort gestartet oder gestoppt. Um die Änderungen zu übernehmen, müssen Sie Kaspersky Security 10.1 für Windows Server neu starten.

Um den KMP-Dienst nutzen zu können, müssen Sie die Servicevereinbarung signieren und Konfigurationsdateien auf einem geschützten Server ausführen.

Um den KMP-Dienst nutzen zu können, müssen die Datenverarbeitungsbedingungen der KSN-Stellungnahme auf den Registerkarten Dienste und Statistiken akzeptiert werden.

8. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen der Datenverarbeitung werden gespeichert.

Exploit-Prävention

Dieser Abschnitt enthält eine Anleitung für die Konfiguration des Schutzes des Prozess-Speichers vor der Ausnutzung von Schwachstellen.

In diesem Kapitel

Über die Aufgabe zur Exploit-Prävention

Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server, das in die geschützten Prozesse eingeschleust wird, um ihre Integrität zu überwachen und die Risiken einer Ausnutzung von Schwachstellen zu mindern.

Das Funktionieren des Agenten innerhalb des geschützten Prozesses ist abhängig vom Start und Beenden dieses Prozesses: Der Agent kann nur bei einem Neustart des Prozesses, der zur Liste der geschützten Prozesse hinzugefügt wurde, erstmals in den Prozess geladen werden. Auch das Entladen des Agenten aus dem Prozess nach seiner Entfernung aus der Liste der geschützten Prozesse ist nur nach einem Neustart des Prozesses möglich.

Das Entladen des Agenten aus den geschützten Prozessen setzt voraus, dass die Prozesse beendet werden: Beim Entfernen der Komponente "Exploit-Prävention" friert das Programm die Umgebung ein und erzwingt das Entladen des Agenten aus den geschützten Prozessen. Wenn der Agent während der Deinstallation der Komponente in einen der geschützten Prozesse eingeschleust wird, müssen Sie den betroffenen Prozess beenden. Möglicherweise muss der Server neu gestartet werden (z. B. wenn der Systemprozess geschützt ist).

Wenn Anzeichen für einen Exploit-Angriff auf den geschützten Prozess gefunden werden, führt Kaspersky Security 10.1 für Windows Server 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 Service Broker Host

Um eine möglichst effektive Nutzung der Funktionen der Komponente "Exploit-Prävention" zu gewährleisten, muss auf dem geschützten Server Kaspersky Security Service Broker Host vorhanden sein. Dieser Dienst ist zusammen mit der Komponente "Exploit-Prävention" Bestandteil der empfohlenen Installation. Während der Installation des Dienstes auf dem geschützten Server 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 Service Broker Host schützt Kaspersky Security 10.1 für Windows Server 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 Risikominderung an, um den Prozess-Speicher zu schützen.

Sollte Kaspersky Security Service Broker Host beendet werden, erhält das Programm nicht länger Daten zu Ereignissen, die für geschützte Prozesse auftreten (darunter auch Daten über Exploit-Angriffe und das Beenden von Prozessen). Der Agent kann auch nicht länger Daten über neue Schutzeinstellungen und über das Hinzufügen neuer Prozesse zur Liste der geschützten Prozesse erhalten.

Modus der Exploit-Prävention

Sie können die Aktionen zur Minderung der Risiken einer Ausnutzung von Schwachstellen in geschützten Prozessen anpassen, indem Sie einen von zwei Modi auswählen:

- **Bei Exploit beenden**: Wenden Sie diesen Modus an, um den Prozess beim Versuch der Ausnutzung einer Schwachstelle zu beenden.

  Wenn eine versuchte Ausnutzung einer Schwachstelle in einem geschützten Prozess gefunden wird, die im Betriebssystem als Kritisch eingestuft ist, beendet Kaspersky Security 10.1 für Windows Server den Prozess nicht – unabhängig vom Modus, der in den Einstellungen der Komponente "Exploit-Prävention" angegeben ist.

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

  In diesem Modus protokolliert Kaspersky Security 10.1 für Windows Server alle Exploit-Versuche in Form von Ereignissen.

Einstellungen zum Schutz des Prozess-Speichers anpassen

► *Um die Einstellungen der Exploit-Prävention für die Prozesse anzupassen, die zur Liste mit geschützten Prozessen hinzugefügt wurden, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Exploit-Prävention** wird geöffnet.
4. Konfigurieren Sie im Block **Modus der Exploit-Prävention** die folgenden Einstellungen:
   - **Exploit von Prozessen mit Schwachstellen verhindern**.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Security 10.1 für Windows Server die Risiken der Ausnutzung von Schwachstellen von Prozessen, die sich in der Liste der geschützten Prozesse befinden.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Server-Prozesse von Kaspersky Security 10.1 für Windows Server nicht vor Exploits geschützt.

     Das Kontrollkästchen ist standardmäßig deaktiviert.
   - **Bei Exploit beenden**.

     In diesem Modus beendet Kaspersky Security 10.1 für Windows Server einen geschützten Prozess beim Fund eines Exploit-Versuchs, wenn ein aktives Verfahren zur Risikominderung angewendet wird.
   - **Über missbräuchlich verwendete Prozesse nur informieren**.

     In diesem Modus benachrichtigt Kaspersky Security 10.1 für Windows Server anhand eines Terminalfensters über Exploits. Der missbräuchlich verwendete Prozess wird auch weiterhin ausgeführt.

     Wenn Kaspersky Security 10.1 für Windows Server während der Ausführung des Programms im Modus **Bei Exploit beenden** einen Exploit in einem kritischen Prozess findet, wechselt die Komponente zwangsläufig in den Modus **Über missbräuchlich verwendete Prozesse nur informieren**.

5. Konfigurieren Sie im Block **Aktionen zur Vorbeugung** die folgenden Einstellungen:

   - **Mit dem Terminaldienst über missbräuchlich verwendete Prozesse informieren.**

     Wenn dieses Kontrollkästchen aktiviert ist, zeigt Kaspersky Security 10.1 für Windows Server ein Terminalfenster mit einer Beschreibung der Ursache für das Auslösen des Schutzes und der Angabe des Prozesses, in dem der Exploit-Versuch gefunden wurde, an.

     Wenn das Kontrollkästchen deaktiviert ist, zeigt Kaspersky Security 10.1 für Windows Server kein Terminalfenster an, wenn ein Exploit-Versuch gefunden oder ein missbräuchlich verwendeter Prozess beendet wurde. Das Terminalfenster wird unabhängig vom Status des Dienstes Kaspersky Security Broker Host angezeigt. Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - **Exploit von Prozessen mit Schwachstellen unabhängig vom Status von Kaspersky Security Service verhindern**.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Security 10.1 für Windows Server die Risiken der Ausnutzung von Schwachstellen von bereits gestarteten Prozessen unabhängig davon, ob der Dienst Kaspersky Security Service läuft. Kaspersky Security 10.1 für Windows Server schützt keine Prozesse, die nach dem Beenden von Kaspersky Security Service hinzugefügt wurden. Nach dem Start des Dienstes wird die Minderung der Exploit-Risiken für alle Prozesse beendet.

     Wenn dieses Kontrollkästchen deaktiviert ist, schützt Kaspersky Security 10.1 für Windows Server keine Prozesse vor Exploits, wenn Kaspersky Security Service beendet wurde.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     Wenn dieses Kontrollkästchen aktiviert ist, reduziert Kaspersky Security 10.1 für Windows Server die Risiken der Ausnutzung von Schwachstellen von Prozessen, die sich in der Liste der geschützten Prozesse befinden.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Server-Prozesse von Kaspersky Security 10.1 für Windows Server nicht vor Exploits geschützt.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

6. Klicken Sie auf **OK**.

Kaspersky Security 10.1 für Windows Server speichert und übernimmt die angepassten Einstellungen zum Schutz des Prozess-Speichers.

Geschützte Prozesse hinzufügen

Die Komponente "Exploit-Prävention" schützt einige Prozesse standardmäßig. 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. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften:**

<Richtlinienname>, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.

- Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Echtzeitschutz** auf die Schaltfläche **Einstellungen** im Block **Exploit-Prävention**.

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

4. Klicken Sie auf der Registerkarte **Geschützte Prozesse** auf die Schaltfläche **Durchsuchen**.

   Es öffnet sich das Microsoft-Windows-Standardfenster **Öffnen**.

5. Wählen Sie den Prozess aus, den Sie zur Liste hinzufügen möchten.
6. Klicken Sie auf **Öffnen**.
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der angegebene Prozess wird zur Liste der geschützten Prozesse hinzugefügt.

8. Wählen Sie den hinzugefügten Prozess aus und klicken Sie auf **Methoden der Exploit-Prävention angeben**.

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

9. Wählen Sie eine der Varianten zur Anwendung der Verfahren zur Risikominderung aus:

   - **Alle verfügbaren Methoden der Exploit-Prävention anwenden**.

     Wenn diese Einstellung ausgewählt ist, kann die Liste nicht geändert werden. Alle Methoden werden standardmäßig übernommen.

   - **Angeführte Methoden der Exploit-Prävention für den Prozess anwenden**.

     Wenn diese Variante ausgewählt ist, können Sie die Liste der angewendeten Verfahren zur Risikominderung bearbeiten:

     a. Aktivieren Sie die Kontrollkästchen der Verfahren, die Sie zum Schutz des ausgewählten Prozesses anwenden möchten.

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

10. Passen Sie die Einstellungen der Ausführung der Verfahren zur Risikominderung Attack Surface Reduction an:

    - Geben Sie die Namen der Module ein, 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 der Internetzone geschieht** die Kontrollkästchen neben jenen Einstellungen, in denen Sie den Start von Modulen erlauben möchten:
      - Internet
      - Intranet

- Vertrauenswürdige Websites
- Websites mit eingeschränktem Zugriff
- Computer

Diese Einstellungen gelten nur für den Internet Explorer®.

11. Klicken Sie auf **OK**.

Der Prozess wird zum Schutzbereich der Aufgabe hinzugefügt.

Verfahren zur Risikominderung

Tabelle 34. Verfahren zur Risikominderung

Verfahren zur Risikominderung	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.
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	Schutz vor Speicherbelegung unter Verwendung von schädlichem Code.
Execution Flow Simulation (Anti Return Oriented Programming)	Erkennen verdächtiger Anweisungsketten (mögliches ROP-Gadget) in der Komponente Windows API.
IntervalProfile Calling Monitor (Ancillary Function Driver Protection (AFDP))	Schutz vor der Ausweitung von Privilegien durch eine Schwachstelle im AFD-Treiber (Ausführen eines zufälligen Codes auf dem Nullring durch den Anruf von QueryIntervalProfile.
Attack Surface Reduction	Blockierung des Starts von Modulen mit etwaigen Schwachstellen über den geschützten Prozess.

Skript-Untersuchung

Dieser Abschnitt informiert über die Aufgabe Skript-Untersuchung und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

Über die Aufgabe Skript-Untersuchung

Bei Ausführung der Aufgabe Skript-Untersuchung kontrolliert Kaspersky Security 10.1 für Windows Server die Ausführung von Skripts, die mit Microsoft Windows Script Technologies (oder Active Scripting) erstellt wurden (z. B. VBScript- oder JScript®-Skripts). Die Ausführung von Skripts wird nur erlaubt, wenn das betreffende Skript von Kaspersky Security 10.1 für Windows Server als sicher eingestuft wurde. Kaspersky Security 10.1 für Windows Server verbietet die Ausführung von Skripts, die als gefährlich eingestuft wurden. Wenn Kaspersky Security 10.1 für Windows Server ein Skript als potenziell gefährlich eingestuft hat, wird die Ausführung des Skripts entsprechend der ausgewählten Aktion verboten oder erlaubt.

Standardmäßig wird die Aufgabe zur Skript-Untersuchung beim Hochfahren von Kaspersky Security 10.1 für Windows Server automatisch gestartet.

Standardmäßig wird die Komponente "Skript-Untersuchung" bei der Programminstallation nicht auf dem Server installiert.

Möglicherweise ist die Verwendung dieser Komponente mit einigen Drittanbieterprogrammen, die auf dem geschützten Server installiert sind, nicht kompatibel. In diesem Fall kann die Überwachung von Drittanbieterskripten zu Fehlern in der Ausführung der Skripte führen. Es wird empfohlen, solche Drittanbieterprogramme nicht zu verwenden oder alternativ die Aufgabe "Skript-Untersuchung" zu deaktivieren. Wenn die Aufgabe deaktiviert wird, steigt das Sicherheitsrisiko, das mit der Ausführung von Skripten verbunden ist.

Wenn Sie die Komponente "Skript-Untersuchung" verwenden möchten, müssen Sie diese während der Installation von Kaspersky Security 10.1 für Windows Server in der Liste der zu installierenden Komponenten manuell auswählen.

Ausführliche Informationen über die Auswahl der Programmkomponenten bei der Installation finden Sie in den *Installationsabschnitten des Administratorhandbuchs für Kaspersky Security 10.1 für Windows Server*.

Sie können die Aufgabeneinstellungen für die Skript-Untersuchung anpassen.

Konfiguration der Aufgabe Skript-Untersuchung

Die Systemaufgabe Skript-Untersuchung weist standardmäßig die in der Tabelle unten beschriebenen Einstellungen auf. Sie können die Werte dieser Parameter ändern.

Tabelle 35. Standardeinstellungen der Aufgabe Skript-Untersuchung

Einstellung	Standardwert	Beschreibung

Einstellung	Standardwert	Beschreibung
Ausführung gefährlicher Skripts	Verboten	Die Ausführung von Skripts, die als gefährlich erkannt werden, wird von Kaspersky Security 10.1 für Windows Server immer verboten.
Ausführung potenziell gefährlicher Skripts	Verboten	Sie können die Aktion festlegen, die ausgeführt werden soll, wenn potenziell gefährliche Skripte gefunden werden: Ausführung blockieren oder erlauben.
Heuristische Analyse	Es wird die Sicherheitsstufe **Mittel** angewendet.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
vertrauenswürdige Zone	Wird verwendet	Einheitliche Liste mit Ausnahmen, die Sie in bestimmten Aufgaben verwenden können.

► *Um die Aufgabe Skript-Untersuchung anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Eigenschaften: Skript-Untersuchung** wird geöffnet.
3. Führen Sie im Block **Aktionen für potentiell gefährliche Skripte** eine der folgenden Aktionen aus:
   - Wenn Sie die Ausführung potenziell gefährlicher Skripte erlauben möchten, wählen Sie **Erlauben**.

     Kaspersky Security 10.1 für Windows Server erlaubt die Ausführung eines potenziell gefährlichen Skripts.
   - Wenn Sie die Ausführung potenziell gefährlicher Skripte verbieten möchten, wählen Sie **Sperren**.

     Kaspersky Security 10.1 für Windows Server blockiert die Ausführung eines potenziell gefährlichen Skripts.

     Diese Variante gilt als Standard.

4. Führen Sie im Block **Heuristische Analyse** eine der folgenden Aktionen aus:

   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.

     Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der heuristischen Analyse bei der Objektuntersuchung.

     Wenn dieses Kontrollkästchen aktiviert ist, ist die heuristische Analyse aktiviert.

     Wurde dieses Kontrollkästchen deaktiviert, ist die heuristische Analyse deaktiviert.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   - Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.

     Mit dem Schieberegler lässt sich die Stufe die Ebene der heuristischen Analyse regulieren. Die Genauigkeitsstufe der Untersuchung regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach Bedrohungen, dem Auslastungsniveau der Betriebssystemressourcen und der Untersuchungsdauer.

     Für die Untersuchung sind folgende Genauigkeitsstufen vorgesehen:

     - **Oberflächlich**. Bei der heuristischen Analyse wird eine relativ geringe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. In diesem Modus besteht eine geringere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung beansprucht weniger Systemressourcen und wird schneller ausgeführt.
     - **Mittel**. Die Anzahl der Befehle, die bei der heuristischen Analyse in der ausführbaren Datei ausgeführt werden, richtet sich nach den Empfehlungen der Kaspersky-Lab-Experten.

       Diese Stufe gilt als Standard.
     - **Tief**. Bei der heuristischen Analyse wird eine relativ hohe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. Bei dieser Einstellung besteht eine höhere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung benötigt mehr Systemressourcen und mehr Zeit und kann eine erhöhte Anzahl an Fehlalarmen auslösen.

       Der Schieberegler ist aktiv, wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist.

5. Aktivieren oder deaktivieren Sie im Block **Vertrauenswürdige Zone** das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.

   Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

   Ist das Kontrollkästchen aktiviert, fügt Kaspersky Security 10.1 für Windows Server die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

   Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Security 10.1 für Windows Server die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs in der Aufgabe Echtzeitschutz für Dateien.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Klicken Sie auf **OK**.

Die neu angepassten Einstellungen werden übernommen.

Schutz des Datenverkehrs

Dieser Abschnitt enthält Informationen über die Aufgabe zum Schutz des Datenverkehrs und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

Über die Aufgabe zum Schutz des Datenverkehrs

Die Komponente "Schutz des Datenverkehrs" verarbeitet den Web-Datenverkehr (einschließlich des Datenverkehrs, der über die Mail-Dienste eingeht) und fängt Objekte ab, die über den Web-Datenverkehr übertragen werden, und untersucht sie, um bekannte Computer- und andere Bedrohungen auf dem geschützten Server zu erkennen. Der ICAP-Dienst untersucht den eingehenden Datenverkehr auf Bedrohungen und sperrt oder erlaubt Datenverkehr abhängig von den Untersuchungsergebnissen und konfigurierten Untersuchungseinstellungen.

Kaspersky Security 10.1 für Windows Server erkennt und fängt außerdem Datenverkehr ab, der von einem beliebigen Prozess unter Windows Subsystem for Linux angefordert wird. Bei solchen Prozessen wendet die Aufgabe "Schutz des Datenverkehrs" die von der aktuellen Aufgabenkonfiguration festgelegte Aktion an.

Der Schutz des Datenverkehrs ist standardmäßig installiert. Wenn die Installation erfolgreich abgeschlossen wurde, werden die folgenden Dienste registriert und gestartet:

- Kaspersky Security Broker Host (KAVFSWH)
- Kaspersky Schutz des Datenverkehrs (KAVFSPROXY)

Diese Komponente bietet die folgenden Schutzarten:

- Schutz vor E-Mail-Bedrohungen
  - Anti-Phishing
  - Schutz vor per E-Mail übermittelter Schadsoftware
- Schutz vor Web-Bedrohungen
  - Anti-Phishing
  - Untersuchung bösartiger URLs
  - Schutz vor webbasierter Schadsoftware

- Web-Kontrolle:
  - Kontrolle von Webadressen
  - Kontrolle von Zertifikaten
  - Kategoriebasierte Web-Kontrolle

Es wird dringend empfohlen, beim Start der Aufgabe "Schutz des Datenverkehrs" die KSN-Dienste zu verwenden, um das Erkennen von Bedrohungen zu verbessern. Die Daten über Webbedrohungen in den KSN-Cloud-Datenbanken sind aktueller als die Daten in den lokalen Antiviren-Datenbanken. Die Analyse mehrerer Kategorien der Web-Kontrolle basiert ausschließlich auf den von den KSN-Diensten bereitgestellten Einstufungen.

Modi für den Schutz des Datenverkehrs

Der Schutz des Datenverkehrs kann in den folgenden Modi betrieben werden:

- **Treiber-Interceptor**: Das Programm fängt Datenverkehr mithilfe eines Netzwerktreibers ab. Es verwendet einen Netzwerk-Kernel-Treiber, um den gesamten eingehenden Datenverkehr für die angegebenen Ports abzufangen und zu analysieren.
- **Redirector**: Das Programm leitet den Datenverkehr mittels einer Konfiguration der Browser um. Eingehender Datenverkehr wird von den Browsern an einen internen Proxyserver in einer geöffneten Terminalsitzung weitergeleitet. Als interner Proxyserver ist Kaspersky Security 10.1 für Windows Server definiert.
- **Externer Proxyserver**: Das Programm verarbeitet den Datenverkehr von einem externen Proxyserver. Der Datenverkehr wird vom externen Proxyserver an Kaspersky Security 10.1 für Windows Server weitergeleitet. Das Programm analysiert den Datenverkehr und empfiehlt dem externen Proxyserver eine Aktion. Kaspersky Security 10.1 für Windows Server ist nur mit Proxys kompatibel, die den Datenverkehr über das ICAP-Protokoll weiterleiten.

Über Regeln zum Schutz des Datenverkehrs

Mit Kaspersky Security 10.1 für Windows Server können Sie Erlaubnis- oder Verbotsregeln für Zertifikate und Webadressen hinzufügen und anpassen und vordefinierte Regeln für Kategorien zum Sperren von unerwünschten Inhalten verwenden. Regeln für Zertifikate können übernommen werden, wenn die Aufgabe im Modus **Treiber-Interceptor** oder **Redirector** ausgeführt wird.

Web-Kontrolle

Diese Art von Kontrolle wird ausgeführt, indem Erlaubnis- und Verbotsregeln für Webadressen und Zertifikate übernommen werden. Erlaubnisregeln haben eine höhere Priorität als Einstufungen von KSN und Signaturanalyse.

Eine URL bzw. ein Zertifikat kann auf der Grundlage von priorisierten Einstufungen (von höchster zu niedrigster) erlaubt oder gesperrt werden:

1. Erlaubnis- oder Verbotsregeln
2. Anti-Phishing- und Antiviren-Datenbanken
3. KSN
4. Kategorien

Kategoriebasierte Web-Kontrolle

Mit Kaspersky Security 10.1 für Windows Server können Sie Webadressen auf der Grundlage von Kategorien sperren. Sie können die Stufe der heuristischen Analyse festlegen, die zur Kategorisierung verwendet wird.
Bei der kategoriebasierten Web-Kontrolle wird für die Analyse die vordefinierte Kategorieliste verwendet. Während die Liste selbst nicht geändert werden kann, können Sie Kategorien von Web-Ressourcen auswählen, die erlaubt oder gesperrt werden sollen, oder die kategoriebasierte Kontrolle ausschalten. Die Kategorie "Andere" enthält alle Webressourcen, die nicht in eine der anderen Kategorien in der Liste fallen. Wenn dieses Kontrollkästchen aktiviert ist, erlaubt Kaspersky Security 10.1 für Windows Server alle Webressourcen, die nicht kategorisiert sind. Ist das Kontrollkästchen deaktiviert, werden alle Webressourcen blockiert.

> Kategorisierung hat die niedrigste Priorität.

Standardmäßig übernimmt Kaspersky Security 10.1 für Windows Server nur eine Regel, nämlich die Verbotsregel für TOR-Zertifikate. Sie können die Regel in den Regeleinstellungen deaktivieren, um TOR-Verbindungen zu erlauben. Wenn die Regel angewendet wird, werden alle eingehenden und ausgehenden TOR-Verbindungen gesperrt.

Der Schutz des Datenverkehrs berücksichtigt auch die Einstufungen für eine `not-a-virus`-Maske, das sind Ressourcen oder Objekte, die an sich keine Viren sind, aber zur Schädigung des geschützten Servers verwendet werden können. Standardmäßig wird die `not-a-virus`-Maske von Kaspersky Security 10.1 für Windows Server nicht für Kategorien übernommen (siehe Abschnitt "Anpassen der kategoriebasierten Web-Kontrolle" auf Seite 228).

Schutz vor E-Mail-Bedrohungen

Die Komponente "Schutz des Datenverkehrs" untersucht E-Mail in Microsoft Outlook (2010, 2013 und 2016, 32-Bit und 64-Bit). Der Schutz vor E-Mail-Bedrohungen wird durch ein Microsoft Outlook-Add-in für Kaspersky Security 10.1 verwirklicht, das getrennt von den Komponenten von Kaspersky Security 10.1 für Windows Server installiert wird.

> Sie können das Microsoft Outlook-Add-in für Kaspersky Security 10.1 nur dann auf dem geschützten Server installieren, wenn Kaspersky Security 10.1 für Windows Server und der Mail-Client Microsoft Outlook installiert sind.

► *Um das Add-in zu installieren, starten die das MSI-Paket ksmail_x86(x64) aus dem Ordner email_plugin.*

Der Schutz vor E-Mail-Bedrohungen umfasst Folgendes:

- Untersuchung von eingehenden E-Mails
- Untersuchung von E-Mails auf Viren
- Untersuchung von Anhängen (einschließlich gepackte Objekte) auf Viren
- Anti-Phishing-Untersuchung von E-Mails
- Untersuchung von Anhängen (einschließlich gepackte Objekte) auf Phishing

Wenn eine Bedrohung gefunden wird, führt Kaspersky Security 10.1 für Windows Server folgende Aktionen aus:

- Anhänge werden gelöscht
- Ändern des Textkörpers der E-Mail
- Das Ereignis *E-Mail-Bedrohung gefunden* wird protokolliert

Kaspersky Security 10.1 für Windows Server untersucht E-Mails, wenn sie geöffnet werden und nicht, wenn sie vom Server empfangen werden. Die Untersuchung findet nur einmalig beim ersten Öffnen statt. Die untersuchten E-Mails und Anhänge werden bis zum Neustart von Outlook im Cache zwischengespeichert. Nach dem Neustart werden alle E-Mail beim Öffnen erneut untersucht.

► *Das Add-in wird beim Start in den Mail-Client Microsoft Outlook geladen. Wenn Sie das Microsoft Outlook-Add-in für Kaspersky Security 10.1 installieren, während Outlook ausgeführt wird, gehen Sie wie folgt vor:*

1. Öffnen Sie **Datei > Einstellungen > Add-ins**.
2. Stellen Sie sicher, dass das Microsoft Outlook-Add-in für Kaspersky Security 10.1 zu einer der Listen hinzugefügt wurde (Aktiv oder Inaktiv).
3. Starten Sie Microsoft Outlook neu.
4. Überprüfen Sie den Status des Microsoft Outlook-Add-ins für Kaspersky Security 10.1 (er sollte *Aktiv* sein).

Anpassen der Aufgabe zum Schutz des Datenverkehrs

Sie können die Standard-Einstellungen der Aufgabe zum Schutz des Datenverkehrs anpassen (siehe Tabelle unten).

Tabelle 36. Standardeinstellung zum Schutz des Datenverkehrs

Tabelle 37.

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	**Externer Proxyserver**	Der ICAP-Dienst verarbeitet den Datenverkehr vom externen Proxyserver.
Netzwerkport	1345	Standard-Portnummer des ICAP-Dienstes.
Dienst-ID	webscan	ID des ICAP-Dienstes für die Adresse des installierten Antiviren-Servers.
Weblinks mittels Datenbank für bösartige Links untersuchen	Wird verwendet	Signaturanalyse für jede URL aktivieren oder deaktivieren
Websites mittels Anti-Phishing-Datenbank untersuchen	Wird verwendet	Anti-Phishing-Untersuchung von URLs auf der Grundlage der heuristischen Analyse aktivieren oder deaktivieren.
KSN zum Schutz verwenden	Wird verwendet	Sie können die Daten über die Reputation des KSN-Programms für den Schutz verwenden, wenn die Aufgabe ausgeführt wird.

Einstellung	Standardwert	Beschreibung
Vertrauenswürdige Zone verwenden	Wird verwendet	Sie können bei Bedarf die vertrauenswürdige Zone verwenden.
Sicherheitsstufe	Empfohlen	Sicherheitsstufe für den Antiviren-Schutz auswählen und anpassen
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe "Schutz des Datenverkehrs" wird nicht automatisch gestartet. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

► *Um die Aufgabe zum Schutz des Datenverkehrs anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Schutz des Datenverkehrs** wird geöffnet.
4. Wählen und konfigurieren Sie auf der Registerkarte **Aufgabenmodus** den Ausführungsmodus der Aufgabe (siehe Abschnitt "Ausführungsmodus von Aufgaben anpassen" auf Seite 213).
5. Passen Sie auf der Registerkarte **URL- und Web-Verarbeitung** die Anti-Phishing-Untersuchung und die Untersuchung auf Viren für URLs an (s. Abschnitt "Anpassen der URL- und Web-Verarbeitung" auf S. 222).
6. Passen Sie auf der Registerkarte **Schutz vor Schadsoftware** die heuristische Analyse und die Sicherheitsstufe an (s. Abschnitt "Anpassen des Schutzes vor webbasierter Schadsoftware" auf S. 218).
7. Starten Sie auf der Registerkarte **Aufgabenverwaltung** die Aufgabe auf der Grundlage eines Zeitplans (siehe Abschnitt "Arbeit mit dem Aufgabenzeitplan" auf Seite 148).
8. Klicken Sie auf **OK**.

Die Aufgabenkonfiguration wird gespeichert.

Funktionsmodus der Aufgabe auswählen

► *Um den Funktionsmodus der Aufgabe anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Schutz des Datenverkehrs** wird geöffnet.
4. Wählen Sie auf der Registerkarte **Allgemein** einen der verfügbaren Modi aus der Dropdown-Liste **Aufgabenmodus**:
   - **Treiber-Interceptor** (siehe Abschnitt "**Treiber-Interceptor-Modus anpassen**" auf Seite 214)
   - **Redirector** (siehe Abschnitt "**Redirector-Modus anpassen**" auf Seite 216)
   - **Externer Proxyserver**
5. Legen Sie die Einstellungen für die Verbindung mit dem ICAP-Dienst fest (für alle drei Modi erforderlich):
   - **Netzwerkport**

     Die Portnummer des ICAP-Dienstes für Kaspersky Security 10.1 für Windows Server.
   - **Dienst-ID**

     ID, der einen Teil des Parameters RESPMOD URI des ICAP-Protokolls darstellt (s. Dokument RFC 3507). RESPMOD URI steht für die Adresse des Anti-Virus-ICAP-Servers, die für den Netzwerkspeicher festgelegt ist.

     Wenn beispielsweise die IP-Adresse des geschützten Servers 192.168.10.10 lautet, die Portnummer 1345 und die ID des ICAP-Dienstes webscan, dann ergibt sich aus diesen Parametern die entsprechende RESPMOD URI Adresse: icap://192.168.10.10/webscan:1345.
6. Passen Sie den ausgewählten Aufgabenmodus an.

   Für den Modus **Externer Proxyserver** ist keine weitere Konfiguration erforderlich. Die Konfiguration erfolgt auf dem externen Proxyserver.
7. Klicken Sie auf **OK**.

Die Konfiguration wird gespeichert.

Treiber-Interceptor-Modus anpassen

► *Gehen Sie im Fenster **Schutz des Datenverkehrs** wie folgt vor:*

1. Wählen Sie die Registerkarte **Allgemein** aus.
2. Wählen Sie den Ausführungsmodus **Treiber-Interceptor** aus.
3. Passen Sie im Block **Einstellungen für den Aufgabenmodus** folgende Einstellungen an:
   - **HTTPS-Datenverkehr untersuchen**.

     Wenn das Kontrollkästchen aktiviert ist, wird der abgefangene verschlüsselte HTTPS-Datenverkehr dekomprimiert und auf Bedrohungen untersucht.

     Ist das Kontrollkästchen deaktiviert, wird der HTTPS-Datenverkehr nicht dekomprimiert.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     > Eine Untersuchung wird nur durchgeführt, wenn der HTTPS-Port geöffnet ist.

   - Wählen Sie die Version des kryptografischen Protokolls aus, das Sie verwenden möchten:
     - **HNAS 1,0**
     - **HNAS 1,1**
     - **HNAS 1,2**

     > Das Kontrollkästchen **TLS 1.0** ist standardmäßig aktiviert und kann nicht geändert werden.

   - **Webservern mit falschem Zertifikat nicht vertrauen**

     Dieses Kontrollkästchen kann aktiviert werden, wenn das Kontrollkästchen **HTTPS-Datenverkehr untersuchen** aktiviert ist.

     Wenn dieses Kontrollkästchen aktiviert ist, wird eine Webseite mit falschem Zertifikat gesperrt (Zertifikat abgelaufen, Signaturüberprüfungsfehler, Zertifikat zurückgezogen usw.).

   - **Sicherheitsport**

     Geben Sie die Portnummer an, die für die Umleitung des Datenverkehrs vom Browser oder Netzwerktreiber zu Kaspersky Security 10.1 für Windows Server verwendet wird, um webbasierte Bedrohungen zu finden. Es wird nicht empfohlen, den Standardport zu ändern. Die Portnummer darf nicht mit anderen Ports übereinstimmen, die für den ICAP-Dienst geöffnet sind. Wenn Sie den Ausführungsmodus **Redirector** verwenden, werden Ports, die bereits verwendet werden, im Feld **HTTPS-Datenverkehr untersuchen** aufgelistet.
4. Wenn Sie Ports zum Interception-Bereich hinzufügen oder davon ausschließen möchten, klicken Sie auf die Schaltfläche **Interception-Bereich anpassen**.

   Das Fenster **Interception-Bereich** wird geöffnet.

5. Wählen Sie auf der Registerkarte **Ports abfangen** eine der folgenden Einstellungen aus:
   - **Alle abfangen**
   - **Angegebene Ports abfangen**:
     a. Geben Sie die Portnummer in das Textfeld ein. Sie können mehrere Ports hinzufügen, indem Sie als Trennzeichen zwischen den Portnummern ein Semikolon verwenden.
     b. Klicken Sie auf **Hinzufügen**.

        Der Port wird zum Interception-Bereich hinzugefügt.

   > Standardmäßig fängt Kaspersky Security 10.1 für Windows Server Datenverkehr ab, der über die folgenden Ports übermittelt wird 80, 8080, 3128, 443.

6. Um Ports anzugeben, die Sie vom Interception-Bereich ausnehmen wollen, gehen Sie auf der Registerkarte **Ports ausschließen** wie folgt vor:
   a. Geben Sie die Portnummer in das Textfeld ein. Sie können mehrere Ports hinzufügen, indem Sie als Trennzeichen zwischen den Portnummern ein Semikolon verwenden.
   b. Klicken Sie auf **Hinzufügen**.

      Der Port wird aus dem Bereich ausgeschlossen.

   > Standardmäßig schließt Kaspersky Security 10.1 für Windows Server Ports aus, die von anderen Programmen verwendet werden und Probleme beim Lesen von Daten, die über eine verschlüsselte Verbindung übertragen werden, verursachen können: 3389, 1723, 13291.

7. Um IP-Adressen aus dem Interception-Bereich auszuschließen, gehen Sie auf der Registerkarte **IP-Adressen ausschließen** wie folgt vor:
   a. Geben Sie IP-Adressen mithilfe des IPv4-Formats oder einer Maske ein.
   b. Klicken Sie auf **Hinzufügen**.
   c. Klicken Sie auf **OK**, um die Änderungen zu speichern.
8. Um einen Prozess oder eine ausführbare Datei, die den Austausch von Datenverkehr erfordert, auszuschließen, gehen Sie auf der Registerkarte **Prozesse ausnehmen** wie folgt vor:
   a. Aktivieren Sie das Kontrollkästchen **Ausnahmen für Prozesse übernehmen**.
   b. Um eine Datei auszuschließen:
      1. Klicken Sie auf **Ausführbare Dateien**.

         Das Microsoft Windows-Standardfenster **Öffnen** wird geöffnet.
      2. Wählen Sie die ausführbare Datei, die Sie ausschließen möchten, und klicken Sie auf **Öffnen**.

c. Um einen Prozess auszuschließen, der auf einem lokalen Computer läuft, gehen Sie wie folgt vor:

1. Klicken Sie auf **Laufende Prozesse**.

   Das Fenster **Aktive Prozesse** wird geöffnet.

2. Wählen Sie einen aktiven Prozess aus und klicken Sie auf **OK**.

> Sie können keine Prozesse in Kaspersky Security Center auswählen.

9. Klicken Sie im Fenster **Schutz des Datenverkehrs** auf die Schaltfläche **OK**.

Die Konfiguration des Ausführungsmodus wird gespeichert.

Redirector-Modus anpassen

► *Gehen Sie im Fenster **Schutz des Datenverkehrs** wie folgt vor:*

1. Wählen Sie die Registerkarte **Allgemein** aus.
2. Wählen Sie den Ausführungsmodus **Redirector**.
3. Passen Sie im Block **Einstellungen für den Aufgabenmodus** folgende Einstellungen an:

- **HTTPS-Datenverkehr untersuchen**.

  Wenn das Kontrollkästchen aktiviert ist, wird der abgefangene verschlüsselte HTTPS-Datenverkehr dekomprimiert und auf Bedrohungen untersucht.

  Ist das Kontrollkästchen deaktiviert, wird der HTTPS-Datenverkehr nicht dekomprimiert.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

> Eine Untersuchung wird nur durchgeführt, wenn der HTTPS-Port geöffnet ist.

- Wählen Sie die Version des kryptografischen Protokolls aus, das Sie verwenden möchten:
  - **HNAS 1,0**
  - **HNAS 1,1**
  - **HNAS 1,2**

> Das Kontrollkästchen **TLS 1.0** ist standardmäßig aktiviert und kann nicht geändert werden.

- **Datenverkehr nach Überprüfung über externen Proxyserver leiten**

  Wenn dieses Kontrollkästchen aktiviert ist, leitet Kaspersky Security 10.1 für Windows Server Datenverkehr, der bereits untersucht wurde, auf einen externen Proxyserver um, beispielsweise einen Unternehmens-Proxyserver, der innerhalb des Unternehmensnetzwerks verwendet wird.

  Ist das Kontrollkästchen deaktiviert, wird der Datenverkehr direkt an einen internen Proxyserver gesendet.

  - **Proxyserver-Adresse**.

    Die Adresse des internen Terminal-Proxyservers, der für die Umleitung verwendet wird.

Geben Sie die Adresse im IPv4-Format ein.

- **Port**

  Die Portnummer für den internen Proxyserver.

- **Sicherheitsport**

  Geben Sie die Portnummer an, die für die Umleitung des Datenverkehrs vom Browser oder Netzwerktreiber zu Kaspersky Security 10.1 für Windows Server verwendet wird, um webbasierte Bedrohungen zu finden. Es wird nicht empfohlen, den Standardport zu ändern. Die Portnummer darf nicht mit anderen Ports übereinstimmen, die für den ICAP-Dienst geöffnet sind. Wenn Sie den Ausführungsmodus **Redirector** verwenden, werden Ports, die bereits verwendet werden, im Feld **HTTPS-Datenverkehr untersuchen** aufgelistet.

Für den Modus **Redirector** muss das Betriebssystem so konfiguriert sein, das verschlüsselter Datenverkehr über den durch Kaspersky Security 10.1 für Windows Server angegebenen Port umgeleitet wird.

4. Klicken Sie auf **OK**.

Die Konfiguration des Ausführungsmodus wird gespeichert.

Einstellungen für vordefinierte Sicherheitsstufen

Für den ausgewählten Knoten in der Struktur der Dateiressourcen des Computers können Sie eine von drei vordefinierten Sicherheitsstufen festlegen: Maximale Leistung, Empfohlen und Maximale Sicherheit. Jede dieser Stufen besitzt eine eigene Auswahl von Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird empfohlen, wenn es zusätzlich zur Verwendung von Kaspersky Security 10.1 für Windows Server auf Servern und Workstations noch weitere Sicherheitsmaßnahmen innerhalb Ihres Netzwerks gibt, beispielsweise Firewalls und bestehende Sicherheitsrichtlinien.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutz und Auswirkung auf die Leistung der geschützten Server. Diese Stufe ist laut Empfehlung der Experten von Kaspersky Lab für den Schutz von Servern in den meisten Unternehmensnetzwerken ausreichend. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximale Sicherheit

Die Sicherheitsstufe **Maximale Sicherheit** wird empfohlen, wenn das Netzwerk Ihres Unternehmens erhöhte Anforderungen an die Computersicherheit hat.

Tabelle 38. Vordefinierte Sicherheitsstufen und entsprechende Sicherheitseinstellungen

Einstellungen	Sicherheitsstufe		
	Maximale Leistung	**Empfohlen**	**Maximale Sicherheit**
Objekte untersuchen	Entsprechend der Erweiterungsliste in der Datenbank	Nach Format	Alle Objekte
Aktion für infizierte und andere Objekte	Sperren	Sperren	Sperren
Nicht erkennen	Nein	Nein	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	60 Sek.	60 Sek.	60 Sek.
Objekte nicht scannen, wenn größer als (MB)	20 MB	20 MB	Nein
Zusammengesetzte Objekte untersuchen	• Gepackte Objekte* * Nur neue und veränderte	• Archive* • SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Nur neue und veränderte	• Archive* • SFX-Archive* • Gepackte Objekte* • Eingebettete OLE-Objekte* * Alle Objekte

‘

Anpassen des Schutzes vor webbasierter Schadsoftware

Die folgenden Schutzeinstellungen wirken sich auch auf den eingehenden E-Mail-Verkehr aus. Die ausgewählten Aktionen auf infizierte und andere erkannte Objekte werden jedoch nur für E-Mail-Anhänge ausgeführt.

► *Um die heuristische Analyse anzupassen, mit der Viren und andere Bedrohungen der Computersicherheit gefunden werden, die über Web-Datenverkehr übertragen werden, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im**

Fenster Programmeinstellungen von Kaspersky Security Center anpassen" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Echtzeitschutz** im Block **Schutz des Datenverkehrs** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Schutz des Datenverkehrs** wird geöffnet.

4. Gehen Sie auf der Registerkarte **Schutz vor Schadsoftware** wie folgt vor:

   - Aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.
   - Legen Sie die erforderliche Stufe der heuristischen Analyse zur Untersuchung von Schadsoftware fest.
   - Wählen Sie die Sicherheitsstufe (siehe Abschnitt "Einstellungen für vordefinierte Sicherheitsstufen" auf Seite 217) aus der Dropdown-Liste aus:
     - **Empfohlen**
     - **Maximale Sicherheit**
     - **Maximale Leistung**
     - **Benutzerdefiniert**

5. Auf der Registerkarte **Beschreibung** darunter können Sie die Einstellungen der ausgewählten Sicherheitsstufe überprüfen.

6. Öffnen Sie die Registerkarte **Allgemein** und geben Sie im Block **Schutz von Objekten** die Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - **Alle Objekte**

     Kaspersky Security 10.1 für Windows Server untersucht alle Objekte.

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

     Kaspersky Security 10.1 für Windows Server untersucht nur infizierbare Dateien auf der Grundlage des Dateiformats.

     Die Liste der Dateiformate wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Security 10.1 für Windows Server enthalten.

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

     Kaspersky Security 10.1 für Windows Server untersucht nur infizierbare Dateien auf der Grundlage der Dateierweiterung.

     Die Erweiterungsliste wird von Kaspersky Lab zusammengestellt. Sie ist in den Datenbanken für Kaspersky Security 10.1 für Windows Server enthalten.

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

     Kaspersky Security 10.1 für Windows Server untersucht Dateien auf der Grundlage der Dateierweiterung. Die Dateierweiterungsliste können Sie im Fenster **Erweiterungsliste** mithilfe der Schaltfläche **Ändern** manuell anpassen.

     a. Klicken Sie auf die Schaltfläche **Ändern**, um die Erweiterungsliste zu ändern.

     b. Geben Sie im folgenden Fenster eine Erweiterung an.

c. Klicken Sie auf **Hinzufügen**.

> Klicken Sie auf die Schaltfläche **Standard**, um die Liste mit der vordefinierten Liste von ausgenommenen Erweiterungen zu füllen.

7. Geben Sie im Block **Schutz von zusammengesetzten Objekten** die zusammengesetzten Objekte an, die Sie in den Untersuchungsbereich einschließen möchten:

   - **Archive**

     Untersuchung von Archiven in den Formaten ZIP, CAB, RAR, ARJ u. a.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Archive von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

   - **SFX-Archive**

     Selbstentpackende Archive untersuchen.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server SFX-Archive.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden SFX-Archive von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

     Diese Einstellung ist aktiv, wenn das Kontrollkästchen **Archive** deaktiviert ist.

   - **Gepackte Objekte**

     Untersuchung von ausführbaren Dateien, die mit Packprogrammen für Binärcode wie beispielsweise UPX oder ASPack gepackt wurden.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server ausführbare Dateien, die mit Packprogrammen gepackt wurden.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden ausführbare Dateien, die mit Packprogrammen gepackt wurden, von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

   - **Eingebettete OLE-Objekte**

     Untersuchung von Objekten, die in eine Datei eingebettet sind (beispielsweise Excel-Tabellen, Microsoft Word-Makros oder Anhänge in E-Mail-Nachrichten).

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Objekte, die in eine Datei eingebettet sind.

     Wenn dieses Kontrollkästchen deaktiviert ist, werden Objekte, die in eine Datei eingebettet sind, von Kaspersky Security 10.1 für Windows Server bei der Untersuchung übersprungen.

     Der Standardwert ist von der aktuellen Sicherheitsstufe abhängig.

8. Wählen Sie auf der Registerkarte **Aktionen** eine Aktion aus, die für infizierte und andere gefundene

Objekte ausgeführt werden soll:

- **Sperren**

  Kaspersky Security 10.1 für Windows Server blockiert das Laden einer Webseite, wenn bösartige Inhalte gefunden werden. Statt der Webseite wird die Ursache für das Sperren der angeforderten Webseite angezeigt.

- **Erlauben**

  Die angeforderte Webseite wird von Kaspersky Security 10.1 für Windows Server nicht gesperrt, das Ereignis über den Fund von bösartigen Inhalten wird jedoch protokolliert.

9. Passen Sie auf der Registerkarte **Optimierung** die folgenden Einstellungen an:

   - Aktivieren oder deaktivieren Sie im Block **Ausnahmen** das Kontrollkästchen **Nicht erkennen**. Um die Liste der ausgenommenen Objekte anzupassen, gehen Sie wie folgt vor:

     Gefundene Objekte nach Name oder Maske des gefundenen Objekts von der Untersuchung ausschließen. Die Liste mit den Namen der gefundenen Objekte finden Sie auf der Website der Viren-Enzyklopädie https://de.securelist.com/.

     Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server die angegebenen gefundenen Objekte bei der Untersuchung.

     Wenn das Kontrollkästchen deaktiviert ist, findet Kaspersky Security 10.1 für Windows Server alle Objekte, die im Programm standardmäßig angegeben sind.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

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

     b. Geben Sie im folgenden Fenster einen Objektnamen oder eine Maske an.

     c. Klicken Sie auf **Hinzufügen**.

   - Beschränken Sie im Block **Erweiterte Einstellungen** den Untersuchungszeitraum und die Objektgröße:

     - **Untersuchung beenden, wenn sie länger dauert als (Sek.)**

       Beschränkung der Untersuchungsdauer für ein Objekt. Als Standard gilt der Wert 60 Sek.

       Wenn dieses Kontrollkästchen aktiviert ist, wird die maximale Untersuchungsdauer für ein Objekt auf den festgelegten Wert begrenzt.

       Wenn dieses Kontrollkästchen deaktiviert ist, gilt keine Beschränkung für die Untersuchungsdauer.

       Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     - **Objekte nicht scannen, wenn größer als (MB)**

       Ausnahme zusammengesetzter Objekte, die die maximale Größe übersteigen, von der Untersuchung.

       Wenn dieses Kontrollkästchen aktiviert ist, werden Objekte, deren Größe über dem festgelegten Wert liegt, von Kaspersky Security 10.1 für Windows Server bei der Untersuchung auf Viren übersprungen.

       Wenn dieses Kontrollkästchen deaktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server Objekte unabhängig von der Größe.

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

10. Klicken Sie im Fenster **Einstellungen für den Schutz gegen Schadsoftware** auf **OK**.

Die Konfiguration der Sicherheitsstufe wird gespeichert.

Anpassen des Schutzes vor E-Mail-Bedrohungen

Um den Schutz vor E-Mail-Bedrohungen verwenden zu können, muss das Microsoft Outlook-Add-in für Kaspersky Security 10.1 installiert und der geschützte Server ordnungsgemäß konfiguriert sein (s. Abschnitt "Schutz vor E-Mail-Bedrohungen" auf S. 210).

► *Um den Schutz vor E-Mail-Bedrohungen zu aktivieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Schutz des Datenverkehrs** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Schutz vor E-Mail-Bedrohungen** das Kontrollkästchen **Schutz vor E-Mail-Bedrohungen aktivieren**.

   Wenn dieses Kontrollkästchen aktiviert ist, führt Kaspersky Security 10.1 für Windows Server mithilfe des Add-ins für Microsoft Outlook eine Untersuchung auf Viren sowie eine Anti-Phishing-Untersuchung aller eingehenden E-Mails durch.

   Ist dieses Kontrollkästchen deaktiviert, werden keine E-Mails untersucht.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
5. Klicken Sie auf **OK**.

Die Änderungen werden gespeichert.

Anpassen der URL- und Web-Verarbeitung

► *Um Webressourcen auf Phishing-Bedrohungen zu untersuchen und Webadressen zu identifizieren,*

die gemäß der Antiviren-Datenbanken und der URL-Reputation von KSN als bösartig eingestuft sind, gehen Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Schutz des Datenverkehrs** wird geöffnet.
4. Wählen und konfigurieren Sie auf der Registerkarte **Aufgabenmodus** den Ausführungsmodus der Aufgabe (siehe Abschnitt "Ausführungsmodus von Aufgaben anpassen" auf Seite 213).
5. Gehen Sie auf der Registerkarte **URL- und Web-Verarbeitung** wie folgt vor:
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Weblinks mittels Datenbank für bösartige Links untersuchen**.

     Wenn dieses Kontrollkästchen aktiviert ist, führt Kaspersky Security 10.1 für Windows Server für jede URL eine Signaturanalyse durch.

     Ist das Kontrollkästchen deaktiviert, wird die Antiviren-Datenbanken nicht zur Untersuchung von URLs verwendet.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Websites mittels Anti-Phishing-Datenbank untersuchen**.

     Wenn dieses Kontrollkästchen aktiviert ist, untersucht Kaspersky Security 10.1 für Windows Server alle URL gegen die Anti-Phishing-Datenbank. Die Anti-Phishing-Untersuchung basiert auf der heuristischen Analyse.

     Ist das Kontrollkästchen deaktiviert, erkennt Kaspersky Security 10.1 für Windows Server Phishing-Angriffe nicht.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     Beachten Sie, dass Anti-Phishing automatisch für E-Mails übernommen wird, wenn Sie die Anti-Phishing-Untersuchung von URLs anpassen.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone verwenden**.

     Mithilfe des Kontrollkästchens wird die Verwendung der vertrauenswürdigen Zone

bei der Ausführung der Aufgabe aktiviert bzw. deaktiviert.

Ist das Kontrollkästchen aktiviert, fügt Kaspersky Security 10.1 für Windows Server die Dateioperationen vertrauenswürdiger Prozesse zu den bei der Konfiguration der Aufgabe festgelegten Ausnahmen von der Untersuchung hinzu.

Ist das Kontrollkästchen deaktiviert, ignoriert Kaspersky Security 10.1 für Windows Server die Dateioperationen vertrauenswürdiger Prozesse bei der Einrichtung eines Schutzbereichs in der Aufgabe Echtzeitschutz für Dateien.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Deaktivieren oder aktivieren Sie das Kontrollkästchen **KSN zum Schutz verwenden**

  Mit diesem Kontrollkästchen wird die Verwendung der KSN-Dienste aktiviert und deaktiviert.

  Wenn das Kontrollkästchen aktiviert ist, verwendet das Programm die Daten von Kaspersky Security Network um sicherzustellen, dass das Programms 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.

Die KSN-Reputation für URLs ist nur verfügbar, wenn die folgenden Bedingungen erfüllt sind:
a. Das Kontrollkästchen **KSN zum Schutz verwenden** ist in den Sicherheitseinstellungen von "Schutz des Datenverkehrs" aktiviert.
b. Die KSN-Erklärung wurde akzeptiert.
c. Das Kontrollkästchen **Daten über angeforderte URLs senden** (siehe Abschnitt "**Konfiguration der Aufgabe Verwendung von KSN**" auf Seite 194) ist aktiviert.
d. Die Aufgabe "Verwendung von KSN" wurde gestartet.

6. Klicken Sie auf **OK**.

Die Konfiguration der URL- und Web-Verarbeitung wird gespeichert.

Hinzufügen von URL-basierten Regeln

Sie können eine URL-basierte Regel hinzufügen, um eine bestimmte URL zu verbieten bzw. zu erlauben. Diese Regeln haben eine höhere Priorität als alle anderen Einstufungen.

► *Um eine neue URL-basierte Regel zu erstellen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.

- Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Block **Schutz des Datenverkehrs** auf die Schaltfläche **Regeln**.

   Das Fenster **Regeln für die Web-Kontrolle** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Web-Kontrolle** das Kontrollkästchen **URL-basierte Regeln übernehmen**, um Regeln zu übernehmen.

   Wenn dieses Kontrollkästchen aktiviert ist, sperrt Kaspersky Security 10.1 für Windows Server HTTPS-Zertifikate, indem benutzerdefinierte Verbotsregeln für Zertifikate übernommen werden.

   Wenn das Kontrollkästchen deaktiviert ist, werden die Regeln nicht angewendet.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

   Das Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen **HTTPS-Datenverkehr untersuchen** aktiviert ist.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel hinzuzufügen.
6. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** die Option **URL-basierte Regel**.
7. Gehen Sie im folgenden Fenster **URL-basierte Regel** wie folgt vor:
   a. Geben Sie den Namen der Regel ein.
   b. Wählen Sie den **Typ** der Regel: **Verbot** oder **Erlaubnis**.
   c. Aktivieren Sie das Kontrollkästchen **Regel übernehmen**.
   d. Geben Sie im darunterliegenden Feld die **URL** an.
   e. Klicken Sie auf **OK**.
8. Um eine Regel zu ändern, wählen Sie eine Regel in der Liste aus und klicken Sie auf **Ändern**.
9. Klicken Sie im Fenster **Regeln für die Web-Kontrolle** auf **OK**.

Die neuen Regeln werden übernommen.

Anpassen der Web-Kontrolle

Sie können die Verwendung der Regeln konfigurieren und die Einstellungen für die Untersuchung von Zertifikaten sowie für die kategoriebasierte Web-Kontrolle verwalten.

In diesem Abschnitt

Anpassen der Untersuchung von Zertifikaten

Mit Kaspersky Security 10.1 für Windows Server können Sie Webressourcen mit ungültigen und abgelaufenen Zertifikaten untersuchen und sperren. Um die Untersuchung von Zertifikaten anzupassen, müssen Sie die folgenden Schritte ausführen:

a. Wählen Sie den Modus **Treiber-Interceptor** oder **Redirector** aus.

b. Passen Sie die Aufgabe zum Schutz des Datenverkehrs an (siehe Abschnitt "Ausführungsmodus auswählen und anpassen" auf Seite 226).

c. Übernehmen Sie Regeln für die Web-Kontrolle.

d. Fügen Sie Regeln für Zertifikate hinzu und übernehmen Sie sie (siehe Abschnitt "Regeln für Zertifikate hinzufügen" auf Seite 227).

Die Regeln für Zertifikate können nur im Modus **Treiber-Interceptor** oder **Redirector** verwendet werden. Standardmäßig erstellt Kaspersky Security 10.1 für Windows Server nur Verbotsregeln für Zertifikate.

Ausführungsmodus auswählen und anpassen

► *Um den Modus für die Arbeit mit Zertifikaten auszuwählen und anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Schutz des Datenverkehrs** wird geöffnet.
4. Wählen Sie auf der Registerkarte **Allgemein** einen Modus aus der Dropdown-Liste **Aufgabenmodus** aus,

in dem die Untersuchung von Zertifikaten unterstützt wird:

- **Treiber-Interceptor** (siehe Abschnitt "**Treiber-Interceptor-Modus anpassen**" auf Seite 214)
- **Redirector** (siehe Abschnitt "Redirector-Modus anpassen" auf Seite 216)

5. Passen Sie im Block **Einstellungen für den Aufgabenmodus** folgende Einstellungen an:
   - **HTTPS-Datenverkehr untersuchen**.

     Wenn das Kontrollkästchen aktiviert ist, wird der abgefangene verschlüsselte HTTPS-Datenverkehr dekomprimiert und auf Bedrohungen untersucht.

     Ist das Kontrollkästchen deaktiviert, wird der HTTPS-Datenverkehr nicht dekomprimiert.

     Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

     Eine Untersuchung wird nur durchgeführt, wenn der HTTPS-Port geöffnet ist.

   - Wählen Sie die Version des kryptografischen Protokolls aus, das Sie verwenden möchten:
     - **HNAS 1,0**
     - **HNAS 1,1**
     - **HNAS 1,2**

     Das Kontrollkästchen **TLS 1.0** ist standardmäßig aktiviert und kann nicht geändert werden.

6. Klicken Sie auf **OK**.

Die Aufgabenkonfiguration wird gespeichert.

Regeln für Zertifikate hinzufügen

Regeln für Zertifikate können nur im Modus **Treiber-Interceptor** oder **Redirector** verwendet werden. Standardmäßig erstellt Kaspersky Security 10.1 für Windows Server nur Verbotsregeln für Zertifikate.

► *Um eine Zertifikatsregel hinzuzufügen oder anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Block **Schutz des Datenverkehrs** auf die Schaltfläche **Regeln**.

   Das Fenster **Regeln für die Web-Kontrolle** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Regeln für die Web-Kontrolle** das Kontrollkästchen **Zertifikatsbasierte Regeln übernehmen**, um Regeln zu übernehmen.

   Wenn dieses Kontrollkästchen aktiviert ist, sperrt Kaspersky Security 10.1 für Windows Server HTTPS-Zertifikate, indem benutzerdefinierte Verbotsregeln für Zertifikate übernommen werden.

   Ist das Kontrollkästchen deaktiviert, werden Zertifikate vom Programm nicht untersucht.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

   Das Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen **HTTPS-Datenverkehr untersuchen** aktiviert ist.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel hinzuzufügen.
6. Wählen Sie im Kontextmenü der Schaltfläche **Hinzufügen** die Option **Zertifikatsbasierte Regel**.
7. Gehen Sie im folgenden Fenster **Zertifikatsbasierte Regel** wie folgt vor:
   a. Geben Sie den Namen der Regel ein.
   b. Aktivieren Sie das Kontrollkästchen **Regel übernehmen**.
   c. Wählen Sie den **Operator-Typ**: **Maske** oder **Regulärer Ausdruck**.
   d. Geben Sie die Maske bzw. den Ausdruck im Feld **Operator** an.
   e. Klicken Sie auf **OK**.
8. Um eine Regel zu ändern, wählen Sie eine Regel in der Liste aus und klicken Sie auf **Ändern**.
9. Klicken Sie im Fenster **Regeln für die Web-Kontrolle** auf **OK**.

Die neuen Regeln werden übernommen.

Anpassen der kategoriebasierten Web-Kontrolle

► *Um eine kategoriebasierte Regel zum Schutz des Datenverkehrs hinzuzufügen oder zu ändern, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte

Geräte und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Block **Schutz des Datenverkehrs** auf die Schaltfläche **Regeln**.

   Das Fenster **Regeln für die Web-Kontrolle** wird geöffnet.

4. Öffnen Sie die Registerkarte **Kategorisierung**.

5. Aktivieren Sie das Kontrollkästchen **Regeln zur Überwachung von Web-Datenverkehr-Kategorien anwenden**.

   Wenn das Kontrollkästchen aktiviert ist, kategorisiert und sperrt Kaspersky Security 10.1 für Windows Server Webressourcen, die unter die ausgewählten Kategorien fallen.

   Ist das Kontrollkästchen deaktiviert, führt Kaspersky Security 10.1 für Windows Server keine Kategorisierung durch.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

   Die Einstellungen für die Überwachung von Kategorien werden verfügbar.

6. Aktivieren oder deaktivieren Sie die folgenden Kontrollkästchen:

   - **Zugriff erlauben, wenn die Webseite nicht kategorisiert werden kann**
   - **Zugriff auf legitime Webressourcen erlauben, die von Hackern zur Schädigung Ihres Servers verwendet werden können**.
   - **Zugriff auf legitime Werbung erlauben**

7. Gehen Sie in der Liste der verfügbaren Kategorien (siehe Abschnitt "Kategorieliste" auf Seite 230) wie folgt vor:

   - Aktivieren Sie das entsprechende Kontrollkästchen, um eine Kategorie zu erlauben.

     Die Spalte **Typ** ändert sich auf **Erlaubnis**.

   - Deaktivieren Sie das entsprechende Kontrollkästchen, um eine Kategorie zu sperren.

     Die Spalte **Typ** ändert sich auf **Verbot**.

   Die Kategorieliste ist vordefiniert und kann nicht geändert werden (Sie können keine Kategorien hinzufügen oder entfernen).

8. Klicken Sie auf **OK**.

Die Regelkonfiguration wird gespeichert.

Verwenden der Not-a-virus-Maske

► *Um die `not-a-virus`-Maske zur Analyse von Kategorien zu verwenden, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Verwaltungskonsole von Kaspersky Security Center die Aufgabeneinstellungen für die Verwendung von KSN (siehe Abschnitt "Konfiguration der Aufgabe Verwendung von KSN"

auf Seite 194).

2. Wählen Sie das Kontrollkästchen **Daten über angeforderte URLs senden**.
3. Starten Sie die Aufgabe "Verwendung von KSN".
4. Aktivieren Sie im Fenster Einstellungen zur Sicherheit des Datenverkehrs (siehe Abschnitt "Anpassen der Aufgabe zum Schutz des Datenverkehrs" auf Seite 211) das Kontrollkästchen **KSN zum Schutz verwenden**.
5. Aktivieren Sie im Fenster **Regeln für die Web-Kontrolle** auf der Registerkarte **Kategorisierung** das Kontrollkästchen **Regeln zur Überwachung von Web-Datenverkehr-Kategorien anwenden**.
6. Wählen Sie in der Kategorieliste die Kategorien aus, für die Sie die `not-a-virus`-Maske übernehmen möchten.

   Objekte aus den ausgewählten Kategorien, die mit der Maske zusammenhängen, werden von der Aufgabe zum Schutz des Datenverkehrs nicht gefunden.

Die `not-a-virus`-Maske wird in den Einstellungen für die **Vertrauenswürdige Zone** angepasst (s. Abschnitt "Anwenden der Not-a-virus-Maske" auf S. 163).

Kategorieliste

Webressourcen werden anhand der Tags analysiert und kategorisiert. Tags können auf eine Reihe von Kategorien angewendet werden (siehe Tabelle unten).

Tabelle 39. Tags für Kategorien von Webressourcen

Tag	Beschreibung	Kategorieliste
18+ (Erwachsene)	Diese Kategorien können Webressourcen beinhalten, die möglicherweise Inhalte für Erwachsene (18+) enthalten, z. B. Beschreibung von Gewalt, Pornografie oder obszöne Sprache.	Schwangerschaftsabbruch, Partnerbörsen für Erwachsene, Anorexie, Unmut, Diskriminierung, Erotik, Illegale Drogen, Illegale Software, LGBT, Dessous, Jugendfreie Partnerbörsen, Nudismus, Richtlinienentscheidung, Pornografie, Unterliegt Einschränkungen durch globale Gesetzgebung, Unterliegt Einschränkungen durch russische Gesetzgebung, Unterliegt Einschränkungen durch Roskomnadzor (Russland), Sexualaufklärung, Sex-Shops, Soziale Netzwerke, Suizid, Obszönes Vokabular, Gewalt, Waffen.

Tag	Beschreibung	Kategorieliste
Kinder	Diese Kategorien können Webressourcen beinhalten, die möglicherweise Inhalte für Kinder enthalten. Zum Beispiel Bildungs-Websites, Unterhaltungs-Websites für Kinder, Forums und Blogs über Kindererziehung.	Für Kinder, Unterliegt Einschränkungen durch das föderale Gesetz 436 (Russland), Seiten von Schulen und Universitäten.
Drogen	Diese Kategorien können Webressourcen beinhalten, die möglicherweise Informationen über Drogen und andere legale und illegale Substanzen enthalten. Zum Beispiel Informationen über den Vertrieb von verbotenen Drogen oder Alkohol, oder die Websites von registrierten Pharmaunternehmen.	Schwangerschaftsabbruch, Alkohol, Anorexie, Drogen, Gesundheit und Schönheit, Illegale Drogen, Medizin, Pharmazie, Tabak.
Bildung	Diese Kategorien können Webressourcen beinhalten, die möglicherweise Unterrichtsmaterial oder Materialien für Lehrer enthalten. Zum Beispiel Online-Enzyklopädien, Wissensdatenbanken, Wikis und die Webseiten von Bildungsinstituten oder Webseiten über Sexualaufklärung.	Bücher und Literatur, Bildung, Für Kinder, Informationstechnologie, Online-Enzyklopädien, Seiten von Schulen und Universitäten, Suchmaschinen, Sexualaufklärung.
Hobby und Unterhaltung	Diese Kategorien können Webressourcen beinhalten, die möglicherweise einen Bezug zu Unterhaltung, Hobbys und Freizeitaktivitäten haben. Zum Beispiel verschiedene Arten von Online-Spielen einschließlich Glücksspiele und soziale Netzwerke, Webseiten über Bücher oder die Jagd, Blogs über Gesundheit und Schönheit und News-Feeds.	Partnerbörsen für Erwachsene, Hobby und Unterhaltung, Alle Kommunikationsmittel, Astrologie und Esoterik, Audio, Video und Software, Wetten, Bloggen, Casinos, Kartenspiele, Gelegenheitsspiele, Chats und Foren, Computerspiele, Kultur und Gesellschaft, Erotik, Mode, Datentausch, Jagd und Fischerei, Für Kinder, Glücksspiele, Gesundheit und Schönheit, Hobby und Unterhaltung, Familie und Zuhause, Humor, LGBT, Dessous, Lotterien, Medien-Hosting und Streaming, Medizin, Musik, News, Jugendfreie Partnerbörsen, Nudismus, Online-Shopping, Online-Shopping (eigenfinanziert), Tiere und Haustiere, Pornografie, Restaurants, Cafés und Essen, Sex-Shops, Soziale Netzwerke, Sport, Torrents, Reisen, TV und Radio, Kriegsspiele.

Tag	Beschreibung	Kategorieliste
Spiele	Diese Kategorien können Webressourcen beinhalten, die möglicherweise einen Bezug zu verschiedenen Arten von Spielen haben. Zum Beispiel Hasardspiele und Wetten, Lotterien, Online- oder Gelegenheitsspiele sowie Website und Foren zum Thema Spiele	Gelegenheitsspiele, Computerspiele, Sport, Kriegsspiele.
Risiko	Diese Kategorie umfasst Webseiten, die Folgendes enthalten: • Glücksspiele mit "Pay to Play" (bezahlen, um zu spielen) • Wettbüros • Lotterien, bei denen Lose/Lottozahlen gekauft werden	Wetten, Casinos, Kartenspiele, Glücksspiele, Glücksspiele (erweitert), Lotterien.
Gesundheit und Medizin	Webseiten zum Thema "gesunder Lebensstil". Können Websites zu Fitness, gesunder Ernährung, alternativen Verfahren und Behandlungsmethoden, Medizin, Pharmazie, Pharmaunternehmen sowie Medikamenten und Nahrungsergänzungsmitteln umfassen.	Schwangerschaftsabbruch, Anorexie, Drogen (legale und illegale), Gesundheit und Schönheit, Medizin, Pharmazie, Sport.
Illegal	Diese Kategorien können möglicherweise illegale Webressourcen beinhalten. Zum Beispiel illegales Teilen von Mediendateien oder Installationspaketen sowie Webseiten, die durch die Gesetze verschiedener Länder verboten sind.	Alkohol, Audio, Video und Software, Drogen, Datentausch, Illegale Drogen, Illegale Software, Lotterien, Unterliegt Einschränkungen durch globale Gesetzgebung, Unterliegt Einschränkungen durch russische Gesetzgebung, Unterliegt Einschränkungen durch Roskomnadzor (Russland), Tabak.
IT	Generell sind Websites, die den Benutzern erlauben, mit oder ohne Anmeldung persönliche Nachrichten an andere Benutzer zu senden (darunter E-Mail-Dienste, soziale Netzwerke, Blogs usw.).	Anonyme Proxyserver, Hosting und Domänendienste, Illegale Software, Informationstechnologie, Suchmaschinen, Webmail.

Tag	Beschreibung	Kategorieliste
gesetzlich verboten	Diese Kategorien können Webressourcen beinhalten, die möglicherweise durch Bundesgesetze kontrolliert werden oder einen Bezug zur Regierung oder Politik haben.	Recht und Politik, Aufgenommen in die Föderale Liste der Extremisten (Russland), Unterliegt Einschränkungen durch das föderale Gesetz 436 (Russland), Unterliegt Einschränkungen durch globale Gesetzgebung, Unterliegt Einschränkungen durch russische Gesetzgebung, Unterliegt Einschränkungen durch Roskomnadzor (Russland).
Legal	Diese Kategorien können möglicherweise legale Webressourcen beinhalten.	Alkohol, Audio, Video und Software, Drogen, Datentausch, Legale Werbung, Lotterien, Militär, Pharmazie, Religion, Sexualaufklärung, Teaser und Werbedienste, Tabak, Kriegsspiele.
Medienaustausch	Diese Kategorien können Webressource beinhalten, die zum Datentausch dienen. Zum Beispiel Torrents, Datentausch-Websites, Musik- und Video-Hosting, sowohl legal als auch illegal.	Audio, Video und Software, Bücher und Literatur, Datentausch**,**Für Kinder, Internetdienste, Medien-Hosting und Streaming, Musik, Suchmaschinen, Torrents, TV und Radio.
Geld und Bezahlsysteme	Diese Kategorien können Webressourcen beinhalten, die möglicherweise einen Bezug zur Finanzwelt und finanziellen Transaktionen haben. Zum Beispiel die offiziellen Websites von Banken, Online-Banken, Online-Shops und Webseiten für die Durchführung von Geldtransfers.	Bankwesen, Bücher und Literatur, Gelegenheitsspiele, E-Commerce, Online-Shopping (eigenfinanziert), Zahlung mit Kreditkarten, Zahlungssysteme, Restaurants, Cafés und Essen, Reisen.
Online-Zusammenarbeit	Diese Kategorien können Webressourcen beinhalten, die möglicherweise einen Bezug zur Online-Kommunikation haben. Zum Beispiel spezielle Blogs und Foren, private Chat-Rooms, soziale Netzwerke und Partnerbörsen.	Partnerbörsen für Erwachsene, Bloggen, Chats und Foren, Für Kinder, Gesundheit und Schönheit, Karriere-Netzwerk, Medizin, Jugendfreie Partnerbörsen, Soziale Netzwerke, Reisen.
Psychotrope Substanzen und Drogen	Diese Kategorien können Webressourcen beinhalten, die einen Bezug zu Drogen, psychotropen Medikamenten oder Tabak haben.	Drogen (legal und illegal), Gesundheit und Schönheit, Illegale Drogen, Medizin, Pharmazie, Tabak.

Tag	Beschreibung	Kategorieliste
Sex&Für Erwachsene	Diese Kategorien können Webressourcen beinhalten, die möglicherweise sexuelles und erotisches Material enthalten. Zum Beispiel Hosting von Pornografie, Webseiten über Sexualaufklärung und Webseiten über sexuelle Minderheiten.	Partnerbörsen für Erwachsene, Erotik, LGBT, Dessous, Nudismus, Pornografie, Sexualaufklärung, Sex-Shops.
Gesellschaft und Gesetz	Diese Kategorie schließt viele Aspekte der Gesellschaft und des menschlichen Lebens ein, darunter Religion, religiöse Vereinigungen, Regierung, Politik, Gesetze, Familie und Zuhause, Nachrichtenmedien, Militär und Waffen.	Kultur und Gesellschaft, Recht und Politik, Militär, Religion, Waffen.
Shopping	Diese Kategorien können Webressourcen beinhalten, die möglicherweise einen Bezug zum Online-Shopping haben.	Bücher und Literatur, Dessous, Online-Shopping, Online-Shopping (eigenfinanziert), Zahlung mit Kreditkarten, Restaurants, Cafés und Essen, Sex-Shops, Reisen.
Gewalt	Diese Kategorien können Webressourcen beinhalten, die möglicherweise explizite Darstellungen von Aggression, Beschreibung von Grausamkeit, extremistische Propaganda oder Beschreibungen von Suizid enthalten.	Unmut, Diskriminierung, Extremismus uns Rassismus, Jagd und Fischerei, Hass und Diskriminierung, Aufgenommen in die Föderale Liste der Extremisten (Russland), Militär, Polizeibeschlüsse (JP), Unterliegt Einschränkungen durch globale Gesetzgebung, Unterliegt Einschränkungen durch russische Gesetzgebung, Unterliegt Einschränkungen durch Roskomnadzor (Russland), Suizid, Gewalt, Kriegsspiele, Waffen.
Webdienste	Diese Kategorien können Webressourcen beinhalten, die möglicherweise verschiedene Webdienste anbieten. Zum Beispiel Anonymisierung, Web-Hosting oder E-Mail-Dienste.	Anonyme Proxyserver, Hosting und Domänendienste, Internetdienste, Suchmaschinen, Teaser und Werbedienste, Webmail.

Überwachung der Server-Aktivitäten

Dieser Abschnitt enthält Informationen über die Funktionen von Kaspersky Security 10.1 für Windows Server zur Kontrolle der Starts und Verbindungen von Apps durch externe Geräte über USB.

In diesem Kapitel

Verwaltung des Programmstarts aus Kaspersky Security Center

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

In diesem Abschnitt

Aufgabe Kontrolle des Programmstarts konfigurieren

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

Tabelle 40. Standardeinstellungen der Aufgabe zur Kontrolle des Programmstarts

Einstellung	Standardwert	Beschreibung
Aufgabenmodus	**Nur Statistik**. Die Aufgabe trägt Ereignisse, die auf Verbot und Start von Programmen basieren, gemäß den festgelegten Regeln in den Bericht über Aufgabenausführung ein. Der Programmstart wird nicht explizit verboten.	Sie können den Modus **Aktiv** für den Schutz des Servers auswählen, nachdem die endgültige Liste der Regeln erstellt wurde.
Regeln verwalten	**Lokale Regeln durch Richtlinienregeln ersetzen.**	Sie können den Modus der gemeinsamen Anwendung der in der Richtlinie festgelegten Regeln und der Regeln auf dem lokalen Computer auswählen.
Gültigkeitsbereich der Regeln	Die Aufgabe kontrolliert den Start von ausführbaren Dateien, Skripten und MSI-Paketen.	Sie können Dateitypen angeben, deren Start durch die Regeln kontrolliert werden soll.
Verwendung von KSN	Die Daten von KSN bezüglich der Reputation von Programmen werden nicht verwendet.	Sie können die Daten über die Reputation von Programmen in KSN bei der Ausführung der Aufgabe zur Kontrolle des Programmstarts verwenden.
Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben	Wird nicht verwendet.	Sie können die Softwareverteilung mithilfe der in den Einstellungen angegebenen Installationspakete und Programme erlauben. Standardmäßig ist die Verteilung der Programme nur mithilfe des Dienstes Windows Installer erlaubt.
Verteilung von Programmen mithilfe von Windows Installer immer erlauben	Wird verwendet	Sie können die Installation oder das Update einer beliebigen Software erlauben, wenn der entsprechende Vorgang über Windows Installer ausgeführt wird.
Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten	Wird nicht verwendet.	Sie können den Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten.

Einstellung	Standardwert	Beschreibung
Aufgabenstart	Der erste Start ist nicht festgelegt.	Die Aufgabe zur Kontrolle des Programmstarts wird beim Start von Kaspersky Security 10.1 für Windows Server nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

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

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

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

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

     - **Aktiv**. Kaspersky Security 10.1 für Windows Server kontrolliert alle Programmstarts mithilfe vorgegebener Regeln.
     - **Nur Statistik**. Kaspersky Security 10.1 für Windows Server kontrolliert den Programmstart nicht mithilfe vorgegebener Regeln, sondern hält lediglich Informationen über den Start von Programmen im Bericht über Aufgabenausführung fest. Der Start aller Programme ist erlaubt. Sie können diesen Modus für die Erstellung einer Liste der Regeln für die Kontrolle des Programmstarts auf Grundlage der im Bericht über Aufgabenausführung enthaltenen Informationen verwenden.

     Standardmäßig wird die Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik** gestartet.
   - Deaktivieren oder aktivieren Sie das Kontrollkästchen **Weitere Starts der überwachten Programme**

nach gleichem Schema wie beim ersten Start verarbeiten.

Das Kontrollkästchen aktiviert oder deaktiviert die Kontrolle wiederholter Programmstarts auf Basis von Einträgen des Caches für Präzedenzfälle.

Ist das Kontrollkästchen aktiviert, so verbietet oder erlaubt Kaspersky Security 10.1 für Windows Server die Ausführung eines wiederholt gestarteten Programms auf Grundlage der Entscheidung, die durch die Aufgabe zur Kontrolle des Programmstarts beim ersten Programmstart getroffen wurde. Wenn beispielsweise der erste Programmstart durch die Regeln für die Kontrolle des Programmstarts erlaubt wurde, so verbleibt der Eintrag über dieses Ereignis im Cache und der wiederholte Start dieses Programms wird erlaubt, ohne erneut zu überprüfen, ob Erlaubnisregeln vorliegen.

Ist das Kontrollkästchen deaktiviert, so untersucht Kaspersky Security 10.1 für Windows Server das Programm bei jedem Programmstart von neuem.

Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

- Deaktivieren oder aktivieren Sie das Kontrollkästchen **Start von Kommandozeileninterpretern ohne auszuführenden Befehl verbieten**.

  Wenn das Kontrollkästchen aktiviert ist, verbietet Kaspersky Security 10.1 für Windows Server den Start des Kommandozeileninterpreters auch dann, wenn der Start des Interpreters erlaubt ist. Die Befehlszeile ohne Befehle kann nur dann gestartet werden, wenn beide Bedingungen erfüllt sind:

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

  Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Security 10.1 für Windows Server für den Start der Befehlszeile nur die Erlaubnisregeln. Der Start wird verboten, wenn keine Erlaubnisregel übernommen wurde oder der ausführbare Prozess keinen vertrauenswürdigen KSN-Status hat. Wenn die Erlaubnisregel übernommen wird oder der Prozess einen vertrauenswürdigen KSN-Status hat, kann die Befehlszeile mit oder ohne Befehl zur Ausführung gestartet werden.

  Kaspersky Security 10.1 für Windows Server erkennt die folgenden Kommandozeileninterpreter:

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

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

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

   Kaspersky Security 10.1 für Windows Server erkennt keine Pfade, die einen Schrägstrich "/" enthalten. Verwenden Sie den Backslash "\", um den Pfad korrekt einzutragen.

   b. Wählen Sie den Modus für die Anwendung der Regeln aus:

   - **Lokale Regeln durch Richtlinienregeln ersetzen**.

     Das Programm wendet die in der Richtlinie festgelegte Regelliste für die zentralisierte Kontrolle des Programmstarts auf der Computergruppe an. Das Erstellen, Bearbeiten und Anwenden der lokalen Regellisten ist nicht verfügbar.

- **Richtlinienregeln zu lokalen Regeln hinzufügen**.

  Das Programm wendet die in der Richtlinie festgelegte Regelliste zusammen mit den lokalen Regellisten an. Sie können die lokalen Regellisten mithilfe der Aufgabe "Automatisches Erstellen von Erlaubnisregeln" bearbeiten.

Standardmäßig wendet Kaspersky Security 10.1 für Windows Server zwei vordefinierte Regeln an, die den Start von Skripts, MSI-Paketen und Startdateien gemäß Zertifikat erlauben.

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

- **Regeln für ausführbare Dateien verwenden**.

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

  Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Security 10.1 für Windows Server den Start ausführbarer Programmdateien mithilfe vorgegebener Regeln, in deren Einstellungen "Ausführbare Dateien" als Geltungsbereich angegeben ist.

  Ist das Kontrollkästchen deaktiviert, so erfolgt durch Kaspersky Security 10.1 für Windows Server keine Kontrolle des Starts ausführbarer Programmdateien mithilfe vorgegebener Regeln. Der Start ausführbarer Programmdateien ist erlaubt.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

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

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

  Ist das Kontrollkästchen aktiviert, erlaubt oder verbietet Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server keine Kontrolle des Ladens von DLL-Modulen mithilfe vorgegebener Regeln. Das Laden von DLL-Modulen ist erlaubt.

  Das Kontrollkästchen ist aktiv, wenn das Kontrollkästchen "Regeln für ausführbare Dateien verwenden" aktiviert ist.

  Das Kontrollkästchen ist standardmäßig deaktiviert.

Die Kontrolle des Ladens von DLL-Modulen kann sich auf die Leistung des Betriebssystems auswirken.

- **Regeln für Skripte und MSI-Pakete verwenden**

  Dieses Kontrollkästchen aktiviert oder deaktiviert die Kontrolle des Starts von Skripten und MSI-Paketen.

  Wenn dieses Kontrollkästchen aktiviert ist, erlaubt oder verbietet Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server keine Kontrolle des Starts von Skripten und MSI-Paketen mithilfe vorgegebener Regeln. Der Start von Skripten und MSI-Paketen ist erlaubt.

  Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

7. Passen Sie im Block **Verwendung von KSN** die folgenden Einstellungen des Programmstarts an:

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

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

     Ist das Kontrollkästchen aktiviert, verbietet Kaspersky Security 10.1 für Windows Server den Start von Programmen, die laut KSN nicht vertrauenswürdig sind. Hierbei greifen die Erlaubnisregeln für die Kontrolle des Programmstarts, welche laut KSN zu den nicht vertrauenswürdigen Programmen gehören, nicht. Die Aktivierung des Kontrollkästchens gewährleistet zusätzlichen Schutz vor Schadsoftware.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Security 10.1 für Windows Server die Reputation von Programmen, die laut KSN nicht vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die sich auf diese Programme erstrecken.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

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

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

     Ist das Kontrollkästchen aktiviert, erlaubt Kaspersky Security 10.1 für Windows Server den Start von Programmen, die laut KSN vertrauenswürdig sind. Dabei haben die Verbotsregeln für die Kontrolle des Programmstarts, die für die im KSN vertrauenswürdigen Programme gelten, eine höhere Priorität: wenn das Programm von den KSN-Diensten als vertrauenswürdig eingestuft ist, aber von den Regeln für die Kontrolle des Programmstarts verboten ist, wird der Start eines solchen Programms blockiert.

     Ist das Kontrollkästchen deaktiviert, berücksichtigt Kaspersky Security 10.1 für Windows Server die Reputation von Programmen, die laut KSN vertrauenswürdig sind, nicht und erlaubt oder verbietet deren Start in Übereinstimmung mit den Regeln, die sich auf diese Programme erstrecken.

     Das Kontrollkästchen ist standardmäßig deaktiviert.

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

8. Passen Sie auf der Registerkarte **Kontrolle für Installationspakete** die Einstellungen für die Kontrolle für Installationspakete an (siehe Abschnitt "Kontrolle für Installationspakete anpassen" auf Seite 240).
9. Passen Sie auf der Registerkarte **Aufgabenverwaltung** die geplanten Einstellungen für den Aufgabenstart an (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite 148).
10. Klicken Sie im Fenster **Aufgabeneinstellungen** auf **OK**.

Kaspersky Security 10.1 für Windows Server 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 Bericht über Aufgabenausführung gespeichert.

Konfiguration der Kontrolle für Installationspakete

Sie können den Installationsvorgang oder das Software-Update mithilfe der Funktion der Kontrolle für Installationspakete vereinfachen. Die Kontrolle für Installationspakete erlaubt es, den Programmstart

automatisch zu erlauben, wenn dieser über ein vertrauenswürdiges Programm oder ein vertrauenswürdiges Installationspaket erfolgt. Nach dem Start eines vertrauenswürdigen Installationspakets berechnet Kaspersky Security 10.1 für Windows Server automatisch eine Prüfsumme für jede untergeordnete Datei und übernimmt für solche Dateien nicht länger die Richtlinien für "standardmäßig verboten". Kaspersky Security 10.1 für Windows Server ermöglicht vertrauenswürdige Installationspakete zu entpacken und alle untergeordneten Dateien auszuführen, wenn ihr Start nicht von den Regeln der Aufgabe zur Gerätekontrolle verboten ist und wenn sie von KSN nicht den Status "nicht vertrauenswürdig" erhalten haben.

Eine Änderung oder Verschiebung der untergeordneten Datei kann dazu führen, dass der Start dieser Datei verboten wird.

► *Um ein vertrauenswürdiges Installationspaket hinzuzufügen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Kontrolle des Programmstarts** wird geöffnet.
4. Aktivieren Sie auf der ausgewählten Registerkarte das Kontrollkästchen **Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben**.

   Dieses Kontrollkästchen aktiviert/deaktiviert die Möglichkeit, automatisch Ausnahmen für alle Dateien zu erstellen, die mithilfe der in der Liste angegebenen Programme und Installationspakete gestartet werden.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt das Programm automatisch den Start von Dateien, die von vertrauenswürdigen Installationspaketen gestartet wurden. Die Liste der für den Start freigegebenen Programme und Installationspakete kann bearbeitet werden.

   Wenn das Kontrollkästchen deaktiviert ist, verwendet das Programm die in der Liste angegebenen Ausnahmen nicht.

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Sie können das Kontrollkästchen **Verteilung mithilfe der festgelegten Programme und Installationspakete automatisch erlauben** aktivieren, wenn das Kontrollkästchen **Regeln für ausführbare Dateien verwenden** in den Einstellungen der Aufgabe zur **Kontrolle des Programmstarts** aktiviert ist.

5. Deaktivieren Sie bei Bedarf das Kontrollkästchen **Verteilung von Programmen mithilfe von Windows Installer immer erlauben**.

   Dieses Kontrollkästchen aktiviert/deaktiviert die Möglichkeit, Ausnahmen für alle Dateien, die mithilfe des Subsystems Windows Installer gestartet werden, automatisch zu erstellen.

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

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

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Dieses Kontrollkästchen kann nicht bearbeitet werden, wenn das Kontrollkästchen **Verteilung von Programmen mithilfe der angegebenen Installationspakete automatisch erlauben** deaktiviert ist.

Das Kontrollkästchen **Verteilung von Programmen mithilfe von Windows Installer immer erlauben** sollte nur deaktiviert werden, wenn dies absolut notwendig ist. Das Deaktivieren dieses Kontrollkästchens kann zu Problemen beim Update der Dateien des Betriebssystems sowie zum Verbot des Starts von untergeordneten Dateien vertrauenswürdiger Installationspakete führen.

6. Aktivieren Sie bei Bedarf das Kontrollkästchen **Verteilung von Programmen über SCCM mithilfe des Background Intelligent Transfer Service (BITS) immer erlauben**.

   Dieses Kontrollkästchen aktiviert oder deaktiviert das automatische Erlauben der Verteilung von Software mithilfe der Softwarelösung System Center Configuration Manager.

   Wenn das Kontrollkästchen aktiviert ist, erlaubt Kaspersky Security 10.1 für Windows Server automatisch die Verteilung von Microsoft Windows mithilfe von System Center Configuration Manager. Das Programm erlaubt die Verteilung von Software nur mithilfe des intelligenten Hintergrundübertragungsdienstes (Background Intelligent Transfer Service).

   Das System überwacht den Start von Objekten mit folgenden Erweiterungen:

   - .exe
   - .msi

   Das Kontrollkästchen ist standardmäßig deaktiviert.

Das Programm überwacht den Verteilungszyklus der Software von der Zustellung des Pakets an den Server 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 Server ausgeführt wurde.

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

   - **Ein Installationspaket hinzufügen**.

     a. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie die Startdatei des Programms oder das Installationspaket aus.

        Im Block **Kriterien für Vertrauenswürdigkeit** werden die Daten zur ausgewählten Datei automatisch angezeigt.

     b. Wählen Sie eine der beiden verfügbaren Varianten der Kriterien für die Vertrauenswürdigkeit aus, auf deren Grundlage die Datei oder das Installationspaket als vertrauenswürdig gelten:

        - **Digitales Zertifikat verwenden**

          Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts das Vorhandensein eines digitalen Zertifikats als Auslösekriterium für die Regel angegeben. Anschließend erlaubt das Programm den Start von Programmen mithilfe von Dateien, die über ein digitales Zertifikat verfügen. Diese Option empfiehlt sich, wenn Sie den Start beliebiger Programme erlauben möchten, die im Betriebssystem als vertrauenswürdig eingestuft sind.

        - **SHA256-Hash verwenden**

          Wenn diese Option ausgewählt ist, wird in den Parametern der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts die Prüfsumme der Datei, auf deren Grundlage die Regel erstellt wird, als Auslösekriterium für die Regel angegeben. Anschließend erlaubt das Programm den Start von Programmen durch Dateien mit den angegebenen Werten der Prüfsumme.

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

          Diese Variante gilt als Standard.

   - **Mehrere Pakete anhand von Hash hinzufügen**.

     Sie können eine unbegrenzte Anzahl an Startdateien und Installationspaketen auswählen und gleichzeitig zur Liste hinzufügen. Kaspersky Security 10.1 für Windows Server untersucht den Hash und erlaubt dem Betriebssystems den Start der angegebenen Dateien.

   - **Ausgewähltes Paket bearbeiten**.

     Verwenden Sie diese Variante, um eine andere Startdatei oder ein anderes Installationspaket auszuwählen sowie die Kriterien für die Vertrauenswürdigkeit zu ändern.

   - **Liste mit Paketen aus Datei importieren**.

     Sie können die Liste der vertrauenswürdigen Installationspakete aus einer gespeicherten Konfigurationsdatei importieren. Die von Kaspersky Security 10.1 für Windows Server erkannte Datei muss folgende Voraussetzungen erfüllen:

     - Sie muss eine Texterweiterung besitzen
     - Sie muss Informationen in Form einer Liste mit Zeilen enthalten, von denen jede die Daten einer einzigen vertrauenswürdigen Datei enthält
     - Sie muss eine Liste enthalten, die einem von zwei Formaten entspricht:
       - <Dateiname>:<Hash SHA256>
       - <Hash SHA256>*<Dateiname>

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

Installationspakete an.

8. Wenn Sie ein früher hinzugefügtes Programm oder Installationspaket aus der Liste der vertrauenswürdigen Installationspakete löschen möchten, klicken Sie auf die Schaltfläche **Installationspakete löschen**.
   Der Start untergeordneter Dateien wird erlaubt.

   > Um den Start untergeordneter Dateien zu verbieten, deinstallieren Sie das Programm vollständig vom geschützten Server oder erstellen Sie eine Verbotsregel in den Einstellungen der Aufgabe zur Kontrolle des Programmstarts.

9. Klicken Sie auf **OK**.

Die vorgenommenen Einstellungen für die Aufgabe werden gespeichert.

Aktivierung des Standarderlaubnismodus

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

► *Um eine Standarderlaubnisregel hinzuzufügen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

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

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

   Es öffnet sich das Fenster **Einstellungen der Regel**.
6. Geben Sie im Feld **Name** den Namen der Regel an.

7. Wählen Sie in der Dropdown-Liste **Typ** den Typ **Erlaubnisregel**.
8. Wählen Sie in der Dropdown-Liste **Gültigkeitsbereich** den Dateityp aus, dessen Start durch die Regel kontrolliert werden soll:
   - **Ausführbare Dateien**, wenn Sie möchten, dass die Regel den Start ausführbarer Programmdateien kontrolliert.
   - **Skripte und MSI-Pakete**, wenn Sie möchten, dass die Regel den Start von Skripten und MSI-Paketen kontrolliert.
9. Wählen Sie im Block **Auslösekriterium für die Regel** eine Option für den **Dateipfad**.
10. Geben Sie die folgende Maske ein: **?:**
11. Klicken Sie im Fenster **Einstellungen der Regel** auf **OK**.

Kaspersky Security 10.1 für Windows Server übernimmt den Standarderlaubnismodus.

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

Sie können mithilfe der Aufgaben und Richtlinien von Kaspersky Security Center für alle Server und Servergruppen im Netzwerk des Unternehmens gleichzeitig Listen mit Regeln für die Kontrolle des Programmstarts erstellen. Dieses Szenario empfiehlt sich, wenn sich im Unternehmensnetzwerk keine Referenzcomputer befinden und Sie keine Möglichkeit haben, mithilfe der Aufgabe zur automatischen Generierung von Erlaubnisregeln anhand der auf einem solchen Referenzcomputer installierten Programme eine allgemeine Regelliste zu erstellen.

Sie können Listen mit Regeln für die Kontrolle des Programmstarts in der Konsole von Kaspersky Security Center auf zwei Arten erstellen:

- Mithilfe der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" für die Kontrolle des Programmstarts.

  Bei Verwendung dieser Option erstellt die Gruppenaufgabe für jeden Server im Netzwerk eine eigene Liste der Regeln für die Kontrolle des Programmstarts und speichert diese Listen in der angegebenen Netzwerkfreigabe in Form einer XML-Datei. Danach können Sie die erstellten Listen mit Regeln manuell in die Aufgabe Kontrolle des Programmstarts in der Richtlinie von Kaspersky Security Center importieren. Sie können eine Richtlinie von Kaspersky Security Center so konfigurieren, dass die erstellten Regeln nach Abschluss der Gruppenaufgabe zum automatischen Erstellen von Erlaubnisregeln automatisch zur Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt werden.

  Es wird empfohlen, diese Option zu verwenden, wenn die kurzfristige Erstellung von Listen mit Regeln für die Kontrolle des Programmstarts erforderlich ist. Es wird empfohlen, den Start der Aufgabe "Automatisches Erstellen von Erlaubnisregeln" nur dann einzurichten, wenn der Gültigkeitsbereich der Erlaubnisregeln Ordner mit zweifelsfrei sicheren Dateien enthält.

  Stellen Sie bei der Übernahme der Richtlinie für die Kontrolle des Programmstarts im Netzwerk sicher, dass für alle geschützten Server der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Anwendung der Netzwerkfreigabe in der Arbeit der Server im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Server-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

- Auf Grundlage des Ereignisberichts für die Aufgabe, der in Kaspersky Security Center anhand der Ausführung der Aufgabe Kontrolle des Programmstarts im Modus **Nur Statistik** erstellt wird.

  Bei Verwendung dieses Szenarios verbietet Kaspersky Security 10.1 für Windows Server Programmstarts nicht, registriert jedoch im Abschnitt **Ereignisse** von Kaspersky Security Center alle erlaubten und verbotenen Programmstarts auf allen Servern des Netzwerks während der Ausführung der Aufgabe zur Kontrolle des Programmstarts im Modus **Nur Statistik**. Kaspersky Security Center erstellt auf der Grundlage des Berichts über Aufgabenausführung eine einheitliche Liste der Ereignisse aufgrund von verbotenen Programmstarts.

  Sie müssen den Zeitraum für die Ausführung der Aufgabe so konfigurieren, dass während des Zeitraums alle möglichen Betriebsszenarien und mindestens ein Neustart der geschützten Server und Servergruppen ausgeführt werden. Danach können Sie beim Hinzufügen von Regeln zur Aufgabe zur Kontrolle des Programmstarts Daten über Programmstarts aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (im Format TXT) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle des Starts der betreffenden Programme erstellen.

  Dieses Szenario wird empfohlen, wenn das Netzwerk des Unternehmens eine große Anzahl an Servern verschiedener Typen (siehe Abschnitt "Über die Verwendung von Profilen bei der Konfiguration der Aufgabe zur Kontrolle des Programmstarts in der Richtlinie von Kaspersky Security Center" auf S. 235) (mit unterschiedlichen Zusammenstellungen installierter Programme) enthält.

- Auf Grundlage der Ereignisse über den verbotenen Start von Programmen, die über Kaspersky Security Center erhalten wurden, ohne Erstellen und Importieren der Konfigurationsdatei.

  Um die vorliegende Möglichkeit zu nutzen, muss sich die Aufgabe zur Kontrolle des Programmstarts auf dem lokalen Computer unter der Verwaltung der aktiven Richtlinie für Kaspersky Security Center befinden. Alle Ereignisse auf dem lokalen Computer werden dabei an den Administrationsserver übergeben.

Es wird empfohlen, die Regelliste bei Änderungen an der Zusammensetzung der auf den Servern des Netzwerks installierten Programme zu aktualisieren (beispielsweise bei der Installation von Updates oder nach einer Neuinstallation des Betriebssystems). Es wird empfohlen, die Aufgabe "Automatisches Erstellen von Erlaubnisregeln" oder die Richtlinie zur Kontrolle des Programmstarts im Modus **Nur Statistik** zu verwenden, die auf Servern der Test-Administrationsgruppe ausgeführt werden, um eine aktualisierte Regelliste zu erstellen. Die Test-Administrationsgruppe beinhaltet Server, die für den probeweisen Start der neuen Programme vor deren Installation auf den Servern des Netzwerks erforderlich sind.

Bevor Sie die Erlaubnisregeln hinzufügen, wählen Sie einen der verfügbaren Modi zur Anwendung der Regeln aus (siehe Abschnitt "Aufgabe Kontrolle des Programmstarts konfigurieren" auf Seite 236). In der Regelliste der Richtlinie für Kaspersky Security Center werden nur jene Regeln angezeigt, die in dieser Richtlinie festgelegt sind, unabhängig vom Modus der Regelanwendung. In der Regelliste des lokalen Computers werden alle angewendeten Regeln angezeigt – sowohl lokale als auch durch die Richtlinie hinzugefügte.

In diesem Abschnitt

Erlaubnisregeln aus Ereignissen in Kaspersky Security Center erstellen

► *Um Erlaubnisregeln mithilfe der Option "Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center erstellen" zu erstellen, gehen Sie in den Einstellungen der Richtlinie zur Kontrolle des Programmstarts wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Öffnen Sie die Administrationsgruppe, deren Richtlinieneinstellungen Sie anpassen möchten, und wählen Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.
3. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.

   Das Fenster **Eigenschaften: <Richtlinienname>** wird geöffnet.
4. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Kontrolle des Programmstarts**.
5. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.
6. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Erlaubnisregeln für Programme aus Ereignissen von Kaspersky Security Center erstellen**.
7. Wählen Sie das Prinzip aus, nach dem Regeln zur Liste der bereits festgelegten Regeln für die Kontrolle des Programmstarts hinzugefügt werden sollen.
   - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
   - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
   - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   Das Fenster **Erstellen von Regeln für die Kontrolle des Programmstarts** wird geöffnet.
8. Passen Sie die folgenden Einstellungen für Anfragen an:
   - **Adresse des Administrationsservers**
   - **Port**
   - **Benutzer**
   - **Kennwort**
9. Wählen Sie die Ereignistypen aus, auf deren Grundlage Sie die Aufgabe erstellen möchten:
   - **Nur Statistik: Programmstart verboten**
   - **Programmstart verboten**
10. Wählen Sie den Zeitraum aus der Dropdown-Liste **In diesem Zeitraum erstellte Ereignisse anfordern**.
11. Klicken Sie auf die Schaltfläche **Regeln erstellen**.
12. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Regeln für die Kontrolle des Programmstarts**.

    Die Liste der Regeln in der Richtlinie zur Kontrolle des Programmstarts wird durch die neuen Regeln

ergänzt, die aufgrund der Systemdaten des Servers mit der installierten Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Wenn die Liste der Regeln für die Kontrolle des Programmstarts bereits in der Richtlinie festgelegt ist, fügt Kaspersky Security 10.1 für Windows Server die ausgewählten Regeln aus den Blockierungsereignissen zu den schon angegebenen Regeln hinzu. Regeln mit demselben Hash werden nicht hinzugefügt, da alle Regeln einer Liste eindeutig sein müssen.

Regeln für die Kontrolle des Programmstarts aus einer XML-Datei importieren

Sie können Berichte, die bei der Ausführung der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" erstellt wurden, importieren und als Liste mit Erlaubnisregeln in der konfigurierten Richtlinie verwenden.

Nach Abschluss der Gruppenaufgabe für die automatische Erstellung von Erlaubnisregeln exportiert das Programm die erstellten Erlaubnisregeln in Form von XML-Dateien in die Netzwerkfreigabe. Jede Datei mit einer Regelliste wird auf Grundlage einer Analyse des Starts der Dateien und Programme auf jedem einzelnen Server des Unternehmensnetzwerks erstellt. Die Listen enthalten Erlaubnisregeln für den Start von Dateien und Programmen, deren Typ den in den Einstellungen der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" gemachten Angaben entspricht.

Die Vorgehensweise beim Anpassen der Einstellungen der Funktionskomponenten von Kaspersky Security 10.1 für Windows Server in Kaspersky Security Center unterscheidet sich nicht wesentlich von der lokalen Konfiguration der Einstellungen dieser Komponenten in der Konsole für Kaspersky Security 10.1 für Windows Server. Eine detaillierte Anleitung zum Anpassen der Aufgabeneinstellungen und Programmfunktionen finden Sie in den entsprechenden Abschnitten des *Benutzerhandbuchs für Kaspersky Security 10.1 für Windows Server*.

► *Gehen Sie wie folgt vor, um Erlaubnisregeln zur Kontrolle des Programmstarts für Servergruppen auf Grundlage einer automatisch erstellten Liste von Erlaubnisregeln festzulegen.*

1. Erstellen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Servergruppe die Gruppenaufgabe Automatisches Erstellen von Erlaubnisregeln oder wählen Sie eine bereits erstellte Aufgabe aus.
2. Konfigurieren Sie in den Eigenschaften der erstellten Gruppenaufgabe für die automatische Erstellung von Erlaubnisregeln oder im Assistenten für neue Aufgaben die folgenden Einstellungen:
   - Konfigurieren Sie im Abschnitt **Benachrichtigung** die Einstellungen für die Speicherung des Berichts über die Aufgabenausführung.

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

   - Legen Sie im Abschnitt **Einstellungen** die Programmtypen fest, deren Start durch die erstellten Regeln erlaubt werden soll. Sie können auch den Bestand der Ordner ändern, aus denen ein Programmstart erlaubt ist: Standard-Ordner aus dem Gültigkeitsbereich der Aufgabe ausschließen und neue Ordner manuell hinzufügen.
   - Legen Sie im Abschnitt **Einstellungen** die Aktionen der Aufgabe während ihrer Ausführung und nach

ihrem Abschluss fest. Geben Sie die Kriterien an, auf deren Grundlage die Regeln erstellt werden sollen, sowie den Namen der Datei, in welche die Regeln exportiert werden.

- Passen Sie im Abschnitt **Zeitplan** die Zeitplan-Einstellungen für den Aufgabenstart.
- Geben Sie im Abschnitt **Benutzerkonto** das Benutzerkonto an, mit dessen Rechten die Aufgabe ausgeführt werden soll.
- Geben Sie im Abschnitt **Ausnahmen vom Gültigkeitsbereich der Aufgabe** diejenigen Servergruppen an, die aus dem Gültigkeitsbereich der Aufgabe ausgeschlossen werden sollen.

> Kaspersky Security 10.1 für Windows Server erstellt keine Erlaubnisregeln für Programme, die auf ausgeschlossenen Servern gestartet werden.

3. Wählen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Servergruppe in der Liste der Gruppenaufgaben die erstellte Aufgabe zur automatischen Erstellung von Erlaubnisregeln aus und klicken Sie auf **Starten**, um die Aufgabe zu starten.

   Nach Abschluss der Aufgabe werden die automatisch erstellten Listen mit Erlaubnisregeln in Form von XML-Dateien in der Netzwerkfreigabe gespeichert.

> Stellen Sie bei der Übernahme der Richtlinie für die Kontrolle des Programmstarts im Netzwerk sicher, dass für alle geschützten Server der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Anwendung der Netzwerkfreigabe in der Arbeit der Server im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Server-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

4. Fügen Sie die erstellten Listen mit Erlaubnisregeln der Aufgabe zur Kontrolle des Programmstarts hinzu. Gehen Sie dazu in den Eigenschaften der zu konfigurierenden Richtlinie in den Einstellungen der Aufgabe Kontrolle des Programmstarts wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie in der folgenden Liste den Punkt **Regeln aus XML-Datei importieren** aus.

   c. Wählen Sie das Prinzip aus, nach dem automatisch erstellte Erlaubnisregeln der Liste der bereits festgelegten Regeln für die Kontrolle des Programmstarts hinzugefügt werden sollen:

      - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
      - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
      - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   d. Wählen Sie im erscheinenden Standardfenster von Windows die XML-Dateien aus, die nach Abschluss der Gruppenaufgabe Automatisches Erstellen von Erlaubnisregeln erstellt wurden.

   e. Klicken Sie auf die Schaltfläche **OK** im Fenster **Regeln für die Kontrolle des Programmstarts** und im Fenster **Aufgabeneinstellungen**.

5. Wenn Sie die erstellten Kontrollregeln für den Start von Programmen übernehmen möchten, wählen Sie

in den Eigenschaften der Aufgabe "Kontrolle des Programmstarts" in der Richtlinie den Modus für die Aufgabenausführung **Aktiv** aus.

Automatisch auf Grundlage der Aufgabenstarts auf jedem einzelnen Server erstellte Erlaubnisregeln werden für alle Server im Netzwerk, auf denen die konfigurierte Richtlinie übernommen wird, übernommen. Für diese Server erlaubt das Programm nur den Start derjenigen Programme, für die Erlaubnisregeln erstellt wurden.

Import von Regeln aus einer Berichtsdatei von Kaspersky Security Center über blockierte Programme

Sie können Daten über blockierte Programmstarts aus dem in Kaspersky Security Center anhand der Ausführung der Aufgabe Kontrolle des Programmstarts im Modus **Nur Statistik** erstellten Bericht importieren und diese Daten für die Erstellung einer Liste von Erlaubnisregeln für den Programmstart in der konfigurierten Richtlinie verwenden.

Bei der Berichterstellung über Ereignisse, die während der Ausführung der Aufgabe zur Kontrolle des Programmstarts eintreten, können Sie verfolgen, für welche Programme der Start blockiert wird.

Vergewissern Sie sich beim Import von Daten über blockierte Programme aus einem Bericht in die Richtlinieneinstellungen davon, dass die verwendete Liste nur diejenigen Programme beinhaltet, deren Start Sie erlauben möchten.

► *Gehen Sie wie folgt vor, um Erlaubnisregeln zur Kontrolle des Programmstarts für Servergruppen auf Grundlage eines Berichts aus Kaspersky Security Center über die gesperrten Programme festzulegen:*

1. Wählen Sie in den Richtlinieneigenschaften in den Parametern für die Aufgabe Kontrolle des Programmstarts den Modus **Nur Statistik** aus.
2. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisse**, dass:
   - auf der Registerkarte **Kritische Ereignisse** für das Ereignis Programmstart verboten eine Dauer für die Speicherung des Ereignisses eingestellt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage).
   - auf der Registerkarte **Warnung** für das Ereignis *Nur Statistik: Programmstart verboten* eine Dauer für die Speicherung des Ereignisses eingestellt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage).

   Nach Ablauf des unter **Speicherdauer** angegebenen Zeitraums werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in die Berichtsdatei aufgenommen. Vergewissern Sie sich vor dem Start der Aufgabe Kontrolle des Programmstarts im Modus **Nur Statistik**, dass die Ausführungsdauer der Aufgabe die eingestellte Speicherzeit für die angegebenen Ereignisse nicht überschreitet.
3. Exportieren Sie nach Abschluss der Aufgabe die protokollierten Ereignisse in eine TXT-Datei:
   a. Erweitern Sie dazu in den Eigenschaften der Aufgabe zur Kontrolle des Programmstarts den Knoten **Berichte und Benachrichtigungen**.
   b. Erstellen Sie im untergeordneten Knoten **Ereignisse** eine Auswahl von Ereignissen anhand der Eigenschaft *Blockiert*, um zu sehen, welche Programmstarts durch die Aufgabe zur Kontrolle des Programmstarts blockiert werden.

c. Klicken Sie im Ergebnisbereich der erstellten Auswahl auf den Link **Ereignisse exportieren**, um einen Bericht über die blockierten Geräte in einer txt-Datei zu speichern.

Vergewissern Sie sich vor dem Import und der Verwendung des erstellten Berichts in der Richtlinie, dass der Bericht nur Daten derjenigen Programme enthält, deren Start Sie erlauben möchten.

4. Importieren Sie die Daten über blockierte Programmstarts in die Aufgabe zur Kontrolle des Programmstarts. Gehen Sie dazu in den Eigenschaften der Richtlinie in den Einstellungen der Aufgabe Kontrolle des Programmstarts wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Kontrolle des Programmstarts** wird geöffnet.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Importieren der Daten über blockierte Programme aus dem Bericht von Kaspersky Security Center**.

   c. Wählen Sie das Prinzip aus, nach dem die Regeln aus der auf Grundlage des Berichts von Kaspersky Security Center erstellten Liste zur Liste der bereits bestehenden Regeln für die Kontrolle des Programmstarts hinzugefügt werden:

      - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
      - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
      - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   d. Wählen Sie folgenden Windows-Standardfenster die txt-Datei aus, in welche die Ereignisse aus dem Bericht über die gesperrten Programmstarts exportiert wurden.

   e. Klicken Sie auf die Schaltfläche **OK** im Fenster Regeln für die Kontrolle des Programmstarts und im Fenster **Aufgabeneinstellungen**.

Die auf Grundlage des Berichts von Kaspersky Security Center über die blockierten Programme erstellten Regeln werden zur Liste der Regeln für die Kontrolle des Programmstarts hinzugefügt.

Verwaltung von Geräteverbindungen über Kaspersky Security Center

Sie können die Verbindung von Flash-Laufwerken und anderen Massenspeichern zu allen Servern im Netzwerk erlauben oder verbieten, indem Sie einheitliche Listen mit den Regeln für die Server-Kontrolle auf Seiten Kaspersky Security Center für Servergruppen erstellen.

In diesem Abschnitt

Über die Aufgabe Gerätekontrolle

Kaspersky Security 10.1 für Windows Server kontrolliert die Registrierung und die Verwendung von Massenspeichern und CD-/DVD-Geräten, um den Server vor Gefahren zu schützen, die während des Dateiaustausches mit angeschlossen USB-Flash-Laufwerken oder anderen Arten von externen Geräten entstehen können. Ein Massenspeicher ist ein externes Gerät, das zum Zweck des Kopieren und Speicherns von Daten mit einem Server verbunden werden kann.

Kaspersky Security 10.1 für Windows Server kontrolliert die folgenden Verbindungen zu externen USB-Geräten:

- USB-Flash-Laufwerke
- CD-ROM-Laufwerke
- USB-Diskettenlaufwerke
- über USB angeschlossene mobile MTP-Geräte

Kaspersky Security 10.1 für Windows Server informiert Sie mithilfe eines entsprechenden Ereignisses in den Aufgabenberichten und Ereignisberichten über alle Geräte, die über USB angeschlossen werden. Das Ereignis enthält den Gerätetyp und den Verbindungspfad. Wenn die Aufgabe "Gerätekontrolle" gestartet wurde, prüft Kaspersky Security 10.1 für Windows Server 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 Server über USB und blockiert die Verbindung, wenn für diese Geräte keine Erlaubnisregeln gefunden werden. Wenn die Verbindung blockiert wird, ist das Gerät nicht verfügbar.

Das Programm weist jedem angeschlossenen Massenspeicher einen der folgenden Status zu:

- *Vertrauenswürdig*. Gerät, mit dem der Datenaustausch erlaubt ist. Der Geräteinstanzpfad eines solchen Geräts fällt unter den Anwendungsbereich zumindest einer Erlaubnisregel.
- *Nicht vertrauenswürdig*. Gerät, mit dem der Datenaustausch verboten ist. Der Geräteinstanzpfad eines solchen Geräts fällt nicht unter den Anwendungsbereich von Erlaubnisregeln.

Sie können mithilfe der Aufgabe Erstellen von Regeln für die Gerätekontrolle Erlaubnisregeln für externe Geräte erstellen, mit denen Sie einen Datenaustausch erlauben wollen. Sie können den Gültigkeitsbereich von bereits erstellten Erlaubnisregeln auch erweitern. Sie können keine Erlaubnisregeln manuell erstellen.

Kaspersky Security 10.1 für Windows Server identifiziert im System registrierte Massenspeicher anhand des Wertes

des *Geräteinstanzpfads*. Der Geräteinstanzpfad ist ein eindeutiges Merkmal für jedes externe Gerät. Die Informationen zum Geräteinstanzpfad sind in den Eigenschaften des externen Geräts im Windows-System enthalten und werden von Kaspersky Security 10.1 für Windows Server während der Erstellung von Regeln automatisch bestimmt.

Die Aufgabe Gerätekontrolle kann in einem der folgenden beiden Modi ausgeführt werden:

- **Aktiv**. Kaspersky Security 10.1 für Windows Server kontrolliert mithilfe der Regeln den Anschluss von Flash-Laufwerken und anderen externen Geräten und verbietet oder erlaubt die Verwendung aller Geräte gemäß dem Prinzip "standardmäßig verboten" (Default Deny) und den festgelegten Erlaubnisregeln. Die Verwendung von vertrauenswürdigen externen Geräten wird erlaubt. Die Verwendung von nicht vertrauenswürdigen externen Geräten wird standardmäßig verboten.

  Wenn das externe Gerät, das Sie für nicht vertrauenswürdig halten, zum Zeitpunkt des Starts der Aufgabe zur Gerätekontrolle im Modus **Aktiv** an den geschützten Server angeschlossen war, wird es vom Programm nicht verboten. Wir empfehlen, das nicht vertrauenswürdige Gerät manuell zu trennen oder den Server neu zu starten. Anderenfalls wird das Prinzip "Standardmäßig verboten" für das Gerät nicht übernommen.

- **Nur Statistik**. Kaspersky Security 10.1 für Windows Server 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 Server sowie zu den Erlaubnisregeln zur Gerätekontrolle, denen die angeschlossenen Geräte unterliegen, im Bericht über 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, die während der Aufgabenausführung aufgezeichnet wurden, verwenden.

Über die Erstellung von Regeln zur Gerätekontrolle für das gesamte Netzwerk über Kaspersky Security Center

Sie können mithilfe der Aufgaben von Kaspersky Security Center für alle Server und Servergruppen im Netzwerk des Unternehmens gleichzeitig Listen mit Regeln für die Gerätekontrolle erstellen.

Sie können Listen mit Regeln zur Gerätekontrolle auf der Seite von Kaspersky Security Center auf zwei Arten erstellen:

- Mithilfe der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle".

  Bei Verwendung dieses Szenarios erstellt die Gruppenaufgabe die Regellisten aufgrund der Systemdaten jedes Servers über alle irgendwann angeschlossenen Flash-Laufwerke und anderen Massenspeichergeräten. Die Aufgabe berücksichtigt auch alle Massenspeichergeräte, die während der Ausführung der Gruppenaufgabe angeschlossen wurden. Nach der Ausführung der Gruppenaufgabe erstellt Kaspersky Security 10.1 für Windows Server Listen mit Erlaubnisregeln für alle registrierten Massenspeichergeräte des Netzwerks und speichert diese Listen in einer xml-Datei im angegebenen allgemeinen Ordner. Im Weiteren können Sie die erstellten Listen mit Regeln in die Eigenschaften der Richtlinie Gerätekontrolle manuell importieren. Im Gegensatz zur Aufgabe auf einem lokalen Computer können Sie in der Richtlinie auf Seiten von Kaspersky Security Center kein automatisches Hinzufügen erstellter Regeln in die Liste der Regeln zur Gerätekontrolle nach Abschluss der Gruppenaufgabe "Automatisches Erstellen von Erlaubnisregeln" einrichten.

  Es wird empfohlen, diese Option für die Erstellung einer Liste mit Erlaubnisregeln vor dem ersten Start

der Richtlinie Gerätekontrolle im Modus der aktiven Regelanwendung zu verwenden.

> Stellen Sie bei der Übernahme der Richtlinie für Gerätekontrolle im Netzwerk sicher, dass für alle geschützten Server der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Anwendung der Netzwerkfreigabe in der Arbeit der Server im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Server-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

- Auf Grundlage des in Kaspersky Security Center erstellten Berichts über Ereignisse bei der Ausführung der Aufgabe Gerätekontrolle im Modus **Nur Statistik**.

  Bei Verwendung dieses Szenarios blockiert Kaspersky Security 10.1 für Windows Server den Anschluss der Massenspeichergeräte nicht, protokolliert aber im Abschnitt **Ereignisse** von Kaspersky Security Center alle Verbindungs- und Registrierungsversuche von Massenspeichergeräten auf allen Netzwerkcomputern während der Ausführung der Aufgabe zur Gerätekontrolle im Modus **Nur Statistik**. Daraufhin erstellt Kaspersky Security Center auf Grundlage des Berichts über Aufgabenausführung eine einheitliche Liste der aufgrund von Blockierungen und Geräteverbindungen eingetretenen Ereignisse.

  Sie müssen den Zeitraum der Aufgabenausführung so anpassen, dass für den angegebenen Zeitraum alle Verbindungen von Massenspeichergeräten ausgeführt werden. Danach können Sie beim Hinzufügen von Regeln zur Aufgabe zur Gerätekontrolle Daten über Geräteverbindungen aus der gespeicherten Berichtsdatei über Ereignisse von Kaspersky Security Center (im Format TXT) importieren und auf Grundlage dieser Daten Erlaubnisregeln für die Kontrolle der betreffenden Geräte erstellen. Beim Import eines erstellten Berichtes anhand von Ereignissen jedes beliebigen Typs werden nur Erlaubnisregeln erstellt.

  Es wird empfohlen, dieses Szenario zu verwenden, wenn Erlaubnisregeln für eine große Menge neuer Massenspeicher erstellt werden sollen, sowie für das Erstellen von Erlaubnisregeln für über das MTP-Protokoll angeschlossene mobile Geräte.

- Auf Grundlage der Daten der System-Registry über die angeschlossenen Massenspeichergeräte (mithilfe der Option "Regel auf Grundlage der folgenden Systemdaten erstellen" in den Einstellungen der Richtlinie zur Gerätekontrolle)

  Bei Verwendung dieses Szenarios erstellt Kaspersky Security 10.1 für Windows Server Erlaubnisregeln für Massenspeicher, die in diesem Moment oder zuvor an den Computer angeschlossen wurden, auf dem Kaspersky Security Center installiert ist.

  Es wird empfohlen, dieses Szenario zu verwenden, wenn Regeln für eine geringe Anzahl neuer Massenspeichergeräte erstellt werden sollen, deren Verwendung Sie auf allen Computern im Netzwerk erlauben möchten.

- Auf Grundlage der Daten über die Geräte, die momentan angeschlossen sind (mithilfe der Option "**Regeln für momentan angeschlossene Geräte berücksichtigen**")

  Bei Verwendung dieses Szenarios erstellt Kaspersky Security 10.1 für Windows Server die Erlaubnisregeln nur für Geräte, die momentan angeschlossen sind. Sie können ein oder mehrere Geräte auswählen, für die Sie die Erlaubnisregeln erstellen möchten.

> Kaspersky Security 10.1 für Windows Server erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Sie können Erlaubnisregeln für vertrauenswürdige mobile Geräte, die über das MTP-Protokoll angeschlossen werden nicht mithilfe von Szenarien zur Ergänzung von Regellisten zur Gerätekontrolle erstellen, die auf der Anwendung der Systemdaten über alle Geräte basieren.

Erstellen von Regeln aufgrund der Systemdaten der externen Geräte, die an die Netzwerkcomputer angeschlossen sind

Sie können auf der Grundlage von Windows-Daten über alle Massenspeichergeräte, die jemals verbunden waren oder derzeit verbunden sind Regeln erstellen (siehe Abschnitt "Über die Erstellung von Regeln zur Gerätekontrolle für das gesamte Netzwerk über Kaspersky Security Center" auf Seite 253). Dazu gibt es drei Szenarien:

- Mithilfe der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle". Verwenden Sie diese Methode, wenn Sie möchten, dass beim Erstellen der Erlaubnisregeln die Daten über die jemals angeschlossenen Massenspeicher, die in den Systemen aller Computer im Netzwerk registriert wurden, berücksichtigt werden.
- Mithilfe der Option **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Richtlinie Gerätekontrolle. Verwenden Sie diese Methode, wenn Sie möchten, dass beim Erstellen der Erlaubnisregeln die Daten über alle jemals angeschlossenen Massenspeicher, die im System des Computers mit der installierten Verwaltungskonsole von Kaspersky Security Center registriert wurden, berücksichtigt werden.
- Mithilfe der Option **Regeln für momentan angeschlossene Geräte berücksichtigen** in den Einstellungen der Richtlinie zur Gerätekontrolle und der Aufgabe "Erstellen von Regeln für die Gerätekontrolle". Verwenden Sie diese Methode, wenn Sie möchten, dass nur Daten über Geräte berücksichtigt werden, die momentan an den geschützten Computer angeschlossen sind, wenn Sie Erlaubnisregeln erstellen.

Kaspersky Security 10.1 für Windows Server erhält keinen Zugriff auf Systemdaten über mobile Geräte, die über das MTP-Protokoll angeschlossen werden. Sie können Erlaubnisregeln für vertrauenswürdige mobile Geräte, die über das MTP-Protokoll angeschlossen werden nicht mithilfe von Szenarien zur Ergänzung von Regellisten zur Gerätekontrolle erstellen, die auf der Anwendung der Systemdaten über alle Geräte basieren.

In diesem Abschnitt

Regeln mithilfe der Aufgabe „Erstellen von Regeln für die Gerätekontrolle" erstellen

► *Um Erlaubnisregeln für die Gerätekontrolle mithilfe der Aufgabe zum Erstellen von Regeln für die Gerätekontrolle festzulegen, gehen Sie wie folgt vor.*

1. Erstellen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Computergruppe die Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" oder wählen Sie eine bereits erstellte Aufgabe aus.
2. Konfigurieren Sie in den Eigenschaften der erstellten Gruppenaufgabe für die automatische Erstellung von Erlaubnisregeln oder im Assistenten für neue Aufgaben die folgenden Einstellungen:
   - Konfigurieren Sie im Abschnitt **Benachrichtigungen** die Einstellungen für die Speicherung des Berichts über die Aufgabenausführung.
   - Legen Sie im Abschnitt **Einstellungen** die Aktionen der Aufgabe nach ihrem Abschluss fest. Geben Sie

den Namen der Datei an, in die die erstellten Regeln exportiert werden.

- Konfigurieren Sie im Abschnitt **Zeitplan** die Einstellungen für den Aufgabenstart nach Zeitplan.

3. Wählen Sie auf der Registerkarte **Aufgaben** in der Steuerleiste der konfigurierten Servergruppe in der Liste der Gruppenaufgaben die erstellte Aufgabe zum Erstellen von Regeln für die Gerätekontrolle und klicken Sie auf **Starten**, um die Aufgabe zu starten.

   Nach Abschluss der Aufgabe werden die automatisch erstellten Listen mit Erlaubnisregeln in Form von XML-Dateien in der Netzwerkfreigabe gespeichert.

   Stellen Sie bei der Übernahme der Richtlinie für Gerätekontrolle im Netzwerk sicher, dass für alle geschützten Server der Zugriff auf die Netzwerkfreigabe angepasst ist. Falls die Anwendung der Netzwerkfreigabe in der Arbeit der Server im Netzwerk durch die Richtlinie des Unternehmens nicht vorgesehen ist, wird empfohlen, die Aufgaben zur automatischen Erstellung von Erlaubnisregeln der Server-Kontrolle auf einem Test- oder Referenzcomputer zu starten.

4. Fügen Sie die erstellten Listen mit Erlaubnisregeln der Aufgabe zur Gerätekontrolle hinzu. Gehen Sie dazu in den Eigenschaften der zu konfigurierenden Richtlinie in den Einstellungen der Aufgabe Gerätekontrolle wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie in der folgenden Liste den Punkt **Regeln aus XML-Datei importieren** aus.

   c. Wählen Sie das Prinzip aus, nach dem automatisch erstellte Erlaubnisregeln der Liste der bereits festgelegten Regeln zur Gerätekontrolle hinzugefügt werden sollen.

      - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
      - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
      - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   d. Wählen Sie im erscheinenden Standardfenster von Windows die XML-Dateien aus, die nach Abschluss der Gruppenaufgabe "Erstellen von Regeln für die Gerätekontrolle" erstellt wurden.

   e. Klicken Sie auf die Schaltfläche **OK** im Fenster "Regeln für die Gerätekontrolle" und im Fenster **Aufgabeneinstellungen**.

5. Wenn Sie die erstellten Regeln zur Gerätekontrolle verwenden möchten, wählen Sie in den Eigenschaften der Richtlinie zur **Gerätekontrolle** den Aufgabenmodus **Aktiv**.

Automatisch auf Grundlage der Systemdaten auf jedem einzelnen Computer erstellte Erlaubnisregeln werden für alle Computer im Netzwerk, auf denen die konfigurierte Richtlinie übernommen wird, übernommen. Für diese Server erlaubt das Programm nur die Verbindung von Geräten, für die Erlaubnisregeln erstellt wurden.

Erlaubnisregeln auf Grundlage der Daten des Systems in der Richtlinie von Kaspersky Security Center erstellen

► *Um die Erlaubnisregeln mithilfe der Option **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Richtlinie "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Wenn es erforderlich ist, schließen Sie an den Computer mit dem installierten Programm Kaspersky Security Center den neuen Massenspeicher an, dessen Verwendung Sie erlauben möchten.
2. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**.
3. Öffnen Sie die Administrationsgruppe, deren Richtlinieneinstellungen Sie anpassen möchten, und wählen Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.
4. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.
5. Das Fenster **Eigenschaften: <Richtlinienname>** wird geöffnet.
6. Öffnen Sie in den Eigenschaften der Richtlinie das Fenster für die Anpassung der Einstellungen der Aufgabe Gerätekontrolle und gehen Sie wie folgt vor:
   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regel auf Grundlage der folgenden Systemdaten erstellen**.

   c. Wählen Sie das Prinzip aus, nach dem Erlaubnisregeln zur Liste der bereits festgelegten Regeln für die Gerätekontrolle hinzugefügt werden sollen.

      - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
      - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
      - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

7. Klicken Sie auf die Schaltfläche **OK** im Fenster **Regeln für die Gerätekontrolle** und im Fenster **Aufgabeneinstellungen**.

Die Liste der Regeln in der Richtlinie zur Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des Computers mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Regeln für angeschlossene Geräte erstellen

► *Um die Erlaubnisregeln mithilfe der Option **Regel auf Grundlage der folgenden Systemdaten erstellen** in den Einstellungen der Richtlinie "Gerätekontrolle" festzulegen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte**.
2. Öffnen Sie die Administrationsgruppe, deren Richtlinieneinstellungen Sie anpassen möchten, und wählen

Sie im Ergebnisbereich die Registerkarte **Richtlinien** aus.

3. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.
4. Das Fenster **Eigenschaften: <Richtlinienname>** wird geöffnet.
5. Klicken Sie im Abschnitt **Überwachung der Server-Aktivitäten** auf die Schaltfläche **Einstellungen** im Block **Gerätekontrolle**.
6. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

   Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.
7. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Kontextmenü den Punkt **Regeln für momentan angeschlossene Geräte berücksichtigen** aus.

   Das Fenster **Regel auf Grundlage der folgenden Systemdaten erstellen** wird geöffnet.
8. Wählen Sie in der Liste der gefundenen Geräte, die an den geschützten Server angeschlossen sind, die Geräte aus, für die Sie Erlaubnisregeln erstellen möchten.
9. Klicken Sie auf die Schaltfläche Regel für ausgewählte Geräte **hinzufügen**.
10. Klicken Sie auf die Schaltfläche **Speichern** im Fenster **Gerätekontrolle**.

Die Liste der Regeln in der Richtlinie zur Gerätekontrolle wird durch die neuen Regeln ergänzt, die aufgrund der Systemdaten des Computers mit der installieren Verwaltungskonsole von Kaspersky Security Center erstellt wurden.

Import von Regeln aus einer Berichtsdatei von Kaspersky Security Center über blockierte Geräte

Sie können Daten über blockierte Massenspeicher aus dem in Kaspersky Security Center anhand der Ausführung der Aufgabe Gerätekontrolle im Modus **Nur Statistik** erstellten Bericht importieren und diese Daten für die Erstellung einer Liste von Erlaubnisregeln für den Programmstart in der konfigurierten Richtlinie verwenden.

Bei der Berichterstellung über Ereignisse, die während der Ausführung der Aufgabe zur Gerätekontrolle eintreten, können Sie verfolgen, für welche Programme die Verbindung blockiert wird.

Vergewissern Sie sich beim Import von Daten über blockierte Geräte aus einem Bericht in die Richtlinieneinstellungen davon, dass die verwendete Liste nur diejenigen Geräte beinhaltet, deren Verbindung Sie erlauben möchten.

► *Gehen Sie wie folgt vor, um Erlaubnisregeln zur Gerätekontrolle für Servergruppen auf Grundlage eines Berichts aus Kaspersky Security Center über die blockierten Geräte festzulegen:*

1. Wählen Sie in den Richtlinieneigenschaften in den Parametern für die Aufgabe Gerätekontrolle den Modus **Nur Statistik** aus.
2. Vergewissern Sie sich in den Richtlinieneigenschaften im Abschnitt **Ereignisse**, dass:
   - auf der Registerkarte **Kritische Ereignisse** für das Ereignis *Massenspeicher verboten* eine Dauer für die Speicherung des Ereignisses eingestellt ist, welche die geplante Ausführungsdauer der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage).
   - auf der Registerkarte **Warnung** für das Ereignis *Nur Statistik: nicht vertrauenswürdiges Gerät gefunden* eine Dauer für die Speicherung des Ereignisses eingestellt ist, welche die geplante Ausführungsdauer

der Aufgabe im Modus **Nur Statistik** überschreitet (Standardwert: 30 Tage).

> Nach Ablauf des unter **Speicherdauer** angegebenen Zeitraums werden die Informationen über die protokollierten Ereignisse gelöscht und nicht in die Berichtsdatei aufgenommen. Vergewissern Sie sich vor dem Start der Aufgabe Gerätekontrolle im Modus **Nur Statistik**, dass die Ausführungsdauer der Aufgabe die eingestellte Speicherzeit für die angegebenen Ereignisse nicht überschreitet.

3. Exportieren Sie nach Abschluss der Aufgabe die protokollierten Ereignisse in eine TXT-Datei. Erweitern Sie hierfür den Knoten **Berichte und Benachrichtigungen** und erstellen Sie im untergeordneten Knoten **Ereignisse** eine Auswahl von Ereignissen anhand der Eigenschaft *Verboten*, um zu sehen, welche Gerätestarts durch die Aufgabe Gerätekontrolle blockiert werden. Klicken Sie im Ergebnisbereich der erstellten Auswahl auf den Link **Ereignisse exportieren**, um einen Bericht über die blockierten Geräte in einer txt-Datei zu speichern.

   > Vergewissern Sie sich vor dem Import und der Verwendung des erstellten Berichts in der Richtlinie, dass der Bericht nur Daten derjenigen Geräte enthält, deren Verbindung Sie erlauben möchten.

4. Importieren Sie die Daten über die blockierten Verbindungsversuche der Geräte in die Richtlinie zur Gerätekontrolle. Gehen Sie dazu in den Eigenschaften der Richtlinie in den Einstellungen der Aufgabe Gerätekontrolle wie folgt vor:

   a. Klicken Sie auf der Registerkarte **Allgemein** auf **Regelliste**.

      Das Fenster **Regeln für die Gerätekontrolle** wird geöffnet.

   b. Klicken Sie auf **Hinzufügen** und wählen Sie im Kontextmenü der Schaltfläche den Punkt **Regeln aus Datei des KSC-Berichts über blockierte Geräte importieren**.

   c. Wählen Sie das Prinzip aus, nach dem die Regeln aus der auf Grundlage des Berichts von Kaspersky Security Center erstellten Liste zur Liste der bereits bestehenden Regeln zur Gerätekontrolle hinzugefügt werden.

      - **Zu den bestehenden Regeln hinzufügen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden dupliziert.
      - **Bestehende Regeln ersetzen**, wenn Sie möchten, dass die importierten Regeln anstatt der bestehenden Regeln aufgenommen werden.
      - **Mit bestehenden Regeln zusammenführen**, wenn Sie möchten, dass die importierten Regeln zu der Liste der bestehenden Regeln hinzugefügt werden. Regeln mit identischen Einstellungen werden nicht hinzugefügt; ist zumindest eine Einstellung der Regel unterschiedlich, so wird sie hinzugefügt.

   d. Wählen Sie im erscheinenden Windows-Standardfenster die TXT-Datei aus, in welche die Ereignisse aus dem Bericht über die blockierten Geräte exportiert wurden.

   e. Klicken Sie auf die Schaltfläche **OK** im Fenster **Regeln für die Gerätekontrolle** und im Fenster **Aufgabeneinstellungen**.

Die auf Grundlage des Berichts von Kaspersky Security Center über die blockierten Geräte erstellten Regeln werden der Liste der Regeln in der Richtlinie zur Gerätekontrolle hinzugefügt.

Netzwerküberwachung

Dieser Abschnitt enthält Informationen über die Aufgaben zur Firewall-Verwaltung und zum Schutz vor Verschlüsselung.

In diesem Kapitel

Firewall-Verwaltung

Dieser Abschnitt informiert über die Aufgabe zur Firewall-Verwaltung und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

Über die Aufgabe zur Firewall-Verwaltung

Kaspersky Security 10.1 für Windows Server stellt eine sichere und ergonomische Lösung für den Schutz von Netzwerkverbindungen mithilfe der Aufgabe zur Firewall-Verwaltung zur Verfügung.

Die Aufgabe zur Firewall-Verwaltung führt keine selbständige Filterung des Datenverkehrs durch, sondern ermöglicht es, die Windows-Firewall über die grafische Benutzeroberfläche von Kaspersky Security 10.1 für Windows Server zu verwalten. Während der Ausführung der Aufgabe zur Firewall-Verwaltung übernimmt Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server vorgenommen werden.

Wenn die Windows-Firewall bei der Installation von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server bei der Durchführung der Abfrage feststellt, dass die Einstellungen der Windows-Firewall und der Einstellungen der Aufgabe zur Firewall-Verwaltung nicht übereinstimmen, erzwingt das Programm die Weitergabe der Einstellungen der Aufgabe an die Firewall des Betriebssystems.

Bei der minutengenauen Abfrage der Windows-Firewall prüft Kaspersky Security 10.1 für Windows Server Folgendes:

- Status der Funktion der Windows-Firewall
- Status der Regeln, die nach der Installation von Kaspersky Security 10.1 für Windows Server von anderen Programmen oder Tools hinzugefügt wurden (z. B. Hinzufügen einer neuen Regel des Programms für einen Port oder eine App mithilfe von wf.msc)

Wenn Sie die neuen Regeln für die Windows Firewall übernehmen, erstellt Kaspersky Security 10.1 für Windows Server einen Satz von Gruppenregeln für Kaspersky Security im **Windows Firewall**-Snap-in. Dieser Regelsatz vereint alle von Kaspersky Security 10.1 für Windows Server mithilfe der Aufgabe zur Firewall-Verwaltung erstellten Regeln. Die Regeln, die zur Gruppe Kaspersky Security Group gehören, werden vom Programm bei der minutenweisen Abfrage nicht überprüft und nicht automatisch mit der Liste der Regeln synchronisiert, die in den Einstellungen der Aufgabe zur Firewall-Verwaltung festgelegt wurden. Bei Bedarf können Sie das Update der Regeln von Kaspersky Security Group manuell vornehmen.

► *Um die Regelliste von Kaspersky Security Group manuell zu aktualisieren,*

starten Sie die Aufgabe zur Firewall-Verwaltung in Kaspersky Security 10.1 für Windows Server neu.

Außerdem können Sie die Regeln von Kaspersky Security Group manuell über das Snap-In **Windows Firewall** anpassen.

Der Start der Aufgabe zur Firewall-Verwaltung ist nicht möglich, wenn die Windows-Firewall von der Gruppenrichtlinie von Kaspersky Security Center verwaltet wird.

Über Firewall-Regeln

Die Aufgabe zur Firewall-Verwaltung kontrolliert die Filterung des eingehenden und ausgehenden Datenverkehrs

mithilfe von Erlaubnisregeln, deren Weitergabe an die Windows-Firewall bei der Aufgabenausführung erzwungen wird.

Beim ersten Aufgabenstart liest Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server diese Regel.
- Wenn in den Einstellungen der Windows-Firewall eine bereits vorhandene Regel gelöscht wird, stellt Kaspersky Security 10.1 für Windows Server diese Regel wieder her.
- Wenn in den Einstellungen der Windows-Firewall die Einstellungen einer vorhandenen Regel geändert werden, verwirft Kaspersky Security 10.1 für Windows Server die Änderungen.
- Wenn in den Einstellungen der Aufgabe zur Firewall-Verwaltung eine neue Regel erstellt wird, erzwingt Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server das Löschen dieser Regel aus den Einstellungen der Windows-Firewall.
- Wenn in den Einstellungen der Aufgabe zur Firewall-Verwaltung eine bereits vorhandene Regel gelöscht wird, erzwingt Kaspersky Security 10.1 für Windows Server das Löschen dieser Regel aus den Einstellungen der Windows-Firewall.

Kaspersky Security 10.1 für Windows Server funktioniert nicht mit Verbotsregeln sowie mit Regeln, die den ausgehenden Datenverkehr kontrollieren. Zum Zeitpunkt des Starts der Aufgabe zur Firewall-Verwaltung löscht Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server festgelegt werden, kontrollieren nur den eingehenden Datenverkehr.

Sie können mit Firewall-Regeln folgender Arten arbeiten:

- Regeln für Apps
- Regeln für Ports

Regeln für Apps

Regeln dieser Art erlauben Netzwerkverbindungen für ausgewählte angegebene Apps. Ein Auslösekriterium für solche Regeln ist der Pfad zur ausführbaren Datei.

Sie können die Regeln für Apps auf folgende Weise verwalten:

- Neue Regeln hinzufügen

- Vorhandene Regeln löschen
- Festgelegte Regeln aktivieren oder deaktivieren
- Einstellungen der festgelegten Regeln ändern: Regelname, Pfad der ausführbaren Datei und Gültigkeitsbereich der Regel angeben

Regeln für Ports

Regeln dieser Art erlauben Netzwerkverbindungen für angegebene Ports und Protokolle (TCP/UDP). Die Auslösekriterien solcher Regeln sind die Portnummer und der Typ des Protokolls.

Sie können Regeln für Ports auf folgende Weise verwalten:

- Neue Regeln hinzufügen
- Vorhandene Regeln löschen
- Festgelegte Regeln aktivieren oder deaktivieren
- Einstellungen der festgelegten Regeln ändern: Regelname, Portnummer, Protokolltyp und Gültigkeitsbereich der Regel festlegen

Die Regeln für Ports sind mit einem größeren Gültigkeitsbereich verbunden als die Regeln für Apps. Indem Sie Verbindungen anhand von Regeln für Ports erlauben, reduzieren Sie die Sicherheitsstufe des geschützten Servers.

Firewall-Regeln aktivieren und deaktivieren

► *Um eine bereits vorhandene Regel zur Filterung des eingehenden Datenverkehrs zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Regelliste** wird geöffnet.
5. Wählen Sie je nach Art der Regel, deren Status Sie ändern möchten, die Registerkarte **Programme** oder

Ports aus.

6. Suchen Sie in der Liste der Regeln die Regel, deren Status Sie ändern möchten, und führen Sie eine der folgenden Aktionen aus:

   - Damit eine inaktive Regel angewendet wird, aktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird aktiviert.

   - Damit eine aktive Regel nicht angewendet wird, deaktivieren Sie das Kontrollkästchen links neben dem Namen der Regel.

     Die ausgewählte Regel wird deaktiviert.

7. Klicken Sie im Fenster "Firewall-Regeln" auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln manuell hinzufügen

Sie können nur Regeln für Apps und Ports hinzufügen und bearbeiten. Sie können für Gruppen keine neuen Regeln hinzufügen oder bereits vorhandene Regeln bearbeiten.

► *Um eine neue Regel zur Filterung des eingehenden Datenverkehrs hinzuzufügen oder eine bereits vorhandene Regel zu ändern, gehen Sie wie folgt vor:*

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.

   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Firewall-Verwaltung**.
4. Klicken Sie im folgenden Fenster auf die Schaltfläche **Regelliste**.

   Das Fenster **Regelliste** wird geöffnet.

5. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus – je nachdem, welche Art

der Regel Sie hinzufügen möchten – und führen Sie eine der folgenden Aktionen aus:

- Um eine bereits vorhandene Regel zu ändern, wählen Sie in der Regelliste die Regel aus, deren Einstellungen Sie anpassen möchten, und klicken Sie auf **Ändern**.
- Um eine neue Regel zu erstellen, klicken Sie auf **Hinzufügen**.

  Je nach Art der angepassten Regel öffnet sich das Fenster **Regel für Port anpassen** oder das Fenster **Regel für Programm anpassen**.

6. Im sich öffnenden Fenster gehen Sie wie folgt vor:
   - Wenn Sie eine Regel für Apps anpassen, gehen Sie wie folgt vor:
     a. Geben Sie im Feld **Regelname** den Namen der bearbeiteten Regel an.
     b. Geben Sie im Feld **Pfad zum Programm** den Pfad zur ausführbaren Datei des Programms an, für das Sie mithilfe der bearbeiteten Regel Verbindungen erlauben möchten.

        Sie können den Pfad manuell oder über die Schaltfläche **Durchsuchen** angeben.
     c. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

        > Die Angabe von IP-Adressen ist nur im Format IPv4 zulässig.

   - Wenn Sie eine Regel für Ports anpassen, gehen Sie wie folgt vor:
     a. Geben Sie im Feld **Regelname** den Namen der bearbeiteten Regel an.
     b. Geben Sie im Feld **Portnummer** die Portnummer an, für die das Programm Verbindungen erlauben soll.
     c. Wählen Sie den Typ des Protokolls (TCP/UDP) aus, für den das Programm Verbindungen erlauben soll.
     d. Geben Sie im Feld **Gültigkeitsbereich der Regel** die Netzadressen an, in deren Rahmen die bearbeitete Regel ausgeführt wird.

        > Die Angabe von IP-Adressen ist nur im Format IPv4 zulässig.

7. Klicken Sie im Fenster **Regel für Programm anpassen** oder **Regel für Port anpassen** auf **OK**.
8. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Firewall-Regeln löschen

> Sie können nur Regeln für Apps und Ports löschen. Sie können bereits vorhandene Regeln für Gruppen nicht löschen.

► *Um eine bereits vorhandene Regel zur Filterung von eingehendem Datenverkehr zu löschen, gehen*

Sie wie folgt vor:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Regelliste** wird geöffnet.
5. Wählen Sie die Registerkarte **Programme** oder die Registerkarte **Ports** aus, je nachdem, welchen Regeltyp Sie löschen möchten.
6. Wählen Sie in der Regelliste eine oder mehrere Regeln aus, die Sie löschen möchten.
7. Klicken Sie auf die Schaltfläche **Löschen**.

   Die ausgewählte Regel wird gelöscht.
8. Klicken Sie im Fenster **Firewall-Regeln** auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen für die Firewall-Verwaltung werden gespeichert. Die neuen Regeleinstellungen werden an die Windows Firewall gesendet.

Schutz vor Verschlüsselung

Dieser Abschnitt informiert über die Aufgabe Schutz vor Verschlüsselung und erläutert die Konfiguration dieser Aufgabe.

In diesem Abschnitt

Über die Aufgabe Schutz vor Verschlüsselung

Mithilfe der Aufgabe zum Schutz vor Verschlüsselung können Sie Verschlüsselungen der freigegebenen Netzwerkordner eines geschützten Servers von Remote-Computern des Unternehmensnetzwerks aus erkennen.

Während der Ausführung der Aufgabe zum Schutz vor Verschlüsselung untersucht Kaspersky Security 10.1 für Windows Server die Anfragen von Remote-Computern auf Zugriff auf die Netzwerkfreigabe der geschützten Server. Wenn das Programm die Aktionen eines Remote-Computers in freigegebenen Netzwerkordnern als Verschlüsselung einstuft, wird der Computer zu einer Liste der nicht vertrauenswürdigen Computer hinzugefügt und der Zugriff auf die Netzwerkfreigabe blockiert.

Kaspersky Security 10.1 für Windows Server stuft eine Aktivität nicht als Verschlüsselung ein, wenn die gefundene Verschlüsselungsaktivität in Verzeichnissen stattfindet, die nicht in den Bereich der Aufgabe zum Schutz vor Verschlüsselung fallen.

Standardmäßig sperrt das Programm den Zugriff von nicht vertrauenswürdigen Computern auf freigegebene Netzwerkordner für 30 Minuten.

Die Aufgabe Schutz vor Verschlüsselung ermöglicht die Blockierung des Zugriffs eines Remote-Computers auf die freigegebenen Netzwerkordner erst dann, wenn die Aktivität des betreffenden Computers als schädlich eingestuft wurde. Dies kann einige Zeit in Anspruch nehmen – währenddessen kann das Verschlüsselungsprogramm weiterhin schädliche Aktivitäten ausführen.

Wenn die Aufgabe "Schutz vor Verschlüsselung" im Modus "Nur Statistik" ausgeführt wird, protokolliert Kaspersky Security 10.1 für Windows Server nur die Verschlüsselungsversuche von Remote-Computern im Bericht über Aufgabenausführung.

Konfiguration der Aufgabe zum Schutz vor Verschlüsselung

Die Aufgabe Schutz vor Verschlüsselung weist die folgenden Standardeinstellungen auf:

- **Aufgabenmodus**. Die Aufgabe "Schutz vor Verschlüsselung" wird im Modus **Aktiv** oder **Nur Statistik** gestartet. Der Modus **Aktiv** ist standardmäßig eingestellt.
- **Schutzbereich**. Kaspersky Security 10.1 für Windows Server übernimmt die Aufgabe zum Schutz vor Verschlüsselung standardmäßig für die gesamte Netzwerkfreigabe des geschützten Servers. Sie können den Schutzbereich ändern, indem Sie die freigegebenen Ordner angeben, für die die Aufgabe übernommen werden soll.
- **Heuristische Analyse**. Kaspersky Security 10.1 für Windows Server übernimmt die Genauigkeitsstufe der Untersuchung **Mittel**. Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren sowie die Genauigkeitsstufe der Untersuchung einstellen.
- **Zeitplan-Einstellungen**. Standardmäßig ist der erste Start der Aufgabe nicht festgelegt. Die Aufgabe zum Schutz vor Verschlüsselung wird beim Start von Kaspersky Security 10.1 für Windows Server nicht automatisch ausgeführt. Sie können die Aufgabe manuell starten oder den Aufgabenstart nach Zeitplan einrichten.

► *Gehen Sie wie folgt vor, um die Einstellungen der Aufgabe "Schutz vor Verschlüsselung" zu konfigurieren:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen

anpassen möchten.

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Schutz vor Verschlüsselung**.

   Das Fenster **Schutz vor Verschlüsselung** wird geöffnet.

4. Nehmen Sie im nächsten Fenster folgende Einstellungen vor:

   - Verwendung von Aufgabenmodus und Heuristische Analyse (s. Abschnitt "Allgemeine Aufgabeneinstellungen" auf S. 268) auf der Registerkarte **Allgemein**.
   - Schutzbereich (s. Abschnitt "Schutzbereich erstellen" auf S. 270) auf der Registerkarte **Schutzbereich**.
   - Ausnahmen(s. Abschnitt "Ausnahmen hinzufügen" auf S. 271) auf der Registerkarte **Ausnahme**.
   - Einstellungen für den Aufgabenstart nach Zeitplan (s. Abschnitt "Arbeit mit dem Aufgabenzeitplan" auf S. 148) auf der Registerkarte **Aufgabenverwaltung**.

5. Klicken Sie auf **OK**.

Kaspersky Security 10.1 für Windows Server 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 Bericht über Aufgabenausführung gespeichert.

Allgemeine Aufgabeneinstellungen

► *Um den Zeitplan einer allgemeinen Aufgabe anzupassen, gehen Sie wie folgt vor:*

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im**

Fenster Programmeinstellungen von Kaspersky Security Center anpassen" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Schutz vor Verschlüsselung**.

   Das Fenster **Schutz vor Verschlüsselung** wird geöffnet.

4. Wählen Sie im Block **Aufgabenmodus** einen von zwei verfügbaren Modi aus:

   - **Nur Statistik**.

     Wenn dieser Modus ausgewählt ist, werden alle Verschlüsselungsversuche im Ereignisbericht der Aufgabe "Schutz vor Verschlüsselung" protokolliert. Es wird keine Aktion ausgeführt. Dieser Modus gilt als Standard.

   - **Aktiv**.

     Wenn dieser Modus ausgewählt ist, blockiert Kaspersky Security 10.1 für Windows Server den Zugriff der gefährdeten Computer auf freigegebene Ordner, wenn ein Verschlüsselungsversuch erkannt wird.

5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**.

   Dieses Kontrollkästchen aktiviert bzw. deaktiviert die Verwendung der heuristischen Analyse bei der Objektuntersuchung.

   Wenn dieses Kontrollkästchen aktiviert ist, ist die heuristische Analyse aktiviert.

   Wurde dieses Kontrollkästchen deaktiviert, ist die heuristische Analyse deaktiviert.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

6. Passen Sie die Analysetiefe bei Bedarf mithilfe des Schiebereglers an.

   Mit dem Schieberegler lässt sich die Stufe die Ebene der heuristischen Analyse regulieren. Die Genauigkeitsstufe der Untersuchung regelt das Verhältnis zwischen der Ausführlichkeit der Suche nach Bedrohungen, dem Auslastungsniveau der Betriebssystemressourcen und der Untersuchungsdauer.

   Für die Untersuchung sind folgende Genauigkeitsstufen vorgesehen:

   - **Oberflächlich**. Bei der heuristischen Analyse wird eine relativ geringe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. In diesem Modus besteht eine geringere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung beansprucht weniger Systemressourcen und wird schneller ausgeführt.

- **Mittel**. Die Anzahl der Befehle, die bei der heuristischen Analyse in der ausführbaren Datei ausgeführt werden, richtet sich nach den Empfehlungen der Kaspersky-Lab-Experten.

  Diese Stufe gilt als Standard.

- **Tief**. Bei der heuristischen Analyse wird eine relativ hohe Anzahl der Aktionen ausgeführt, die in der ausführbaren Datei enthalten sind. Bei dieser Einstellung besteht eine höhere Wahrscheinlichkeit, dass eine Bedrohung gefunden wird. Die Untersuchung benötigt mehr Systemressourcen und mehr Zeit und kann eine erhöhte Anzahl an Fehlalarmen auslösen.

  Der Schieberegler ist aktiv, wenn das Kontrollkästchen **Heuristische Analyse verwenden** aktiviert ist.

7. Klicken Sie auf **OK**, um die neue Konfiguration zu übernehmen.

Schutzbereich erstellen

In der Aufgabe Schutz vor Verschlüsselung werden die folgenden Arten von Schutzbereichen übernommen:

- **Vordefiniert**. Sie können den standardmäßig festgelegten Schutzbereich verwenden, der alle Ordner der Netzwerkfreigabe des Servers in die Untersuchung einschließt. Wird übernommen, wenn die Einstellung **Alle Netzwerkfreigaben auf dem Server** ausgewählt wurde.
- **Benutzer**. Sie können den Schutzbereich selbstständig anpassen, indem Sie die Ordner manuell auswählen, die in den Verschlüsselungsschutzbereich aufgenommen werden sollen. Wird übernommen, wenn die Einstellung **Nur die angegebenen freigegebenen Ordner** ausgewählt wurde.

Zum Anpassen des Schutzbereichs der Aufgabe zum Schutz vor Verschlüsselung können nur lokale Pfade verwendet werden.

► *Gehen Sie wie folgt vor, um einen Schutzbereich für die Aufgabe zum Schutz vor Verschlüsselung zu anzupassen:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Schutz vor Verschlüsselung**.

   Das Fenster **Schutz vor Verschlüsselung** wird geöffnet.

4. Wählen Sie auf der Registerkarte **Schutzbereich** die Ordner aus, die Kaspersky Security 10.1 für Windows Server bei der Ausführung der Aufgabe "Schutz vor Verschlüsselung" untersuchen soll:

   - **Gesamte Netzwerkfreigabe des Servers**

     Wenn diese Option ausgewählt ist, untersucht Kaspersky Security 10.1 für Windows Server bei der Ausführung der Aufgabe zum Schutz vor Verschlüsselung die gesamte Netzwerkfreigabe des Servers.

     Diese Variante gilt als Standard.

   - **Nur die angegebenen freigegebenen Ordner**

     Wenn diese Option ausgewählt wurde, untersucht Kaspersky Security 10.1 für Windows Server bei der Ausführung der Aufgabe zum Schutz vor Verschlüsselung nur die von Ihnen manuell angegebenen Ordner der Netzwerkfreigabe des Servers.

5. Um die freigegebenen Ordner der Server anzugeben, die in den Bereich zum Schutz vor Verschlüsselung aufgenommen werden sollen, gehen Sie wie folgt vor:

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

      Das Fenster **Ordner zum Hinzufügen auswählen** wird geöffnet.

   b. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie einen Ordner aus bzw. geben Sie das Verzeichnis manuell ein.

   c. Klicken Sie auf **OK**.

6. Klicken Sie im Fenster Schutz vor Verschlüsselung auf **OK**.

Die vorgenommenen Einstellungen werden gespeichert.

Ausnahmen hinzufügen

► *Gehen Sie wie folgt vor, um Ausnahmen vom Schutzbereich des Schutzes vor Verschlüsselung hinzuzufügen:*

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **Netzwerküberwachung** auf die Schaltfläche **Einstellungen** im Block **Schutz vor Verschlüsselung**.

   Das Fenster **Schutz vor Verschlüsselung** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Ausnahmen** das Kontrollkästchen **Liste mit Ausnahmen übernehmen**.

   Wenn dieses Kontrollkästchen aktiviert ist, erkennt Kaspersky Security 10.1 für Windows Server keine Verschlüsselungsaktivität in den angegebenen Bereichen während der Ausführung der Aufgabe "Schutz vor Verschlüsselung".

   Wenn das Kontrollkästchen deaktiviert ist, erkennt Kaspersky Security 10.1 für Windows Server die Verschlüsselungsaktivität in allen Netzwerkfreigaben.

   Standardmäßig ist das Kontrollkästchen deaktiviert und die Ausnahmeliste leer.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Ordner zum Hinzufügen auswählen** wird geöffnet.

6. Geben Sie den Ordnernamen ein oder klicken Sie auf **Durchsuchen**, um einen Ordner auszuwählen.

7. Klicken Sie auf **OK**.

Der ausgeschlossene Bereich wird zur Liste hinzugefügt.

System-Diagnose

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

In diesem Kapitel

Überwachung der Datei-Integrität

Dieser Abschnitt enthält Informationen über den Start und das Anpassen der Aufgabe zur Überwachung der Datei-Integrität.

In diesem Abschnitt

Über die Aufgabe Überwachung der Datei-Integrität

Die Aufgabe Überwachung der Datei-Integrität überwacht Aktionen, die mit bestimmten Dateien oder Ordnern ausgeführt werden, im Rahmen von Überwachungsbereichen, die in den Einstellungen der Aufgabe festgelegt wurden. Mithilfe der Aufgabe können Sie Änderungen an Dateien erkennen, die eventuell auf eine Verletzung der Sicherheit auf dem geschützten Server hindeuten. Sie können außerdem Änderungen an Dateien in Zeiträumen nachverfolgen, in denen die Überwachung unterbrochen war.

Eine *Unterbrechung der Überwachung* tritt auf, wenn der Überwachungsbereich vorübergehend aus dem Gültigkeitsbereich der Aufgabe fällt, weil z. B. die Aufgabenausführung angehalten wird oder ein geschütztes Gerät nicht physisch auf einem geschützten Server vorhanden ist. Kaspersky Security 10.1 für Windows Server benachrichtigt Sie über gefundene Dateioperationen im Überwachungsbereich, sobald das Massenspeichergerät wieder angeschlossen ist.

Wenn das Anhalten der Aufgabenausführung im festgelegten Überwachungsbereich durch eine Neuinstallation der Komponente "Überwachung der Datei-Integrität" verursacht wurde, gilt dies nicht als Unterbrechung der Überwachung. In diesem Fall wird die Aufgabe Überwachung der Datei-Integrität nicht ausgeführt.

Umgebungsanforderungen

Für die Ausführung der Aufgabe Überwachung der Datei-Integrität müssen folgende Voraussetzungen erfüllt sein:

- Auf dem geschützten Server ist ein Speicher installiert, der die Dateisysteme ReFS und NTFS unterstützt
- Das Windows USN-Protokoll ist aktiviert. Die Komponente fragt dieses Protokoll ab, um Informationen über Dateioperationen zu erhalten.

> Wenn Sie das USN-Protokoll aktiviert haben, nachdem die Regel für das Laufwerk erstellt und die Aufgabe zur Überwachung der Datei-Integrität gestartet wurde, ist es erforderlich, die Aufgabe neu zu starten. Andernfalls wird die Regel bei der Überwachung nicht berücksichtigt.

Ausnahmen für den Überwachungsbereich

Sie können Ausnahmen vom Überwachungsbereich erstellen (siehe Abschnitt "Einstellungen der Überwachungsregeln anpassen" auf Seite 278). Die Ausnahmen werden für jede einzelne Regel angegeben und gelten nur für den angegebenen Überwachungsbereich. Sie können für jede Regel eine unbegrenzte Anzahl an Ausnahmen festlegen.

> Ausnahmen haben eine höhere Priorität als der Überwachungsbereich und werden von der Aufgabe nicht überwacht, selbst wenn ein angegebener Ordner oder eine Datei in den Überwachungsbereich fallen sollte. Wenn die Einstellungen für eine der Regeln einen Überwachungsbereich angeben, der sich auf einer niedrigeren Stufe befindet als ein in den Ausnahmen angegebener Ordner, wird der Überwachungsbereich bei der Ausführung der Aufgabe nicht berücksichtigt.

Zur Angabe von Ausnahmen können Sie die gleichen Masken verwenden wie für die Angabe des Überwachungsbereichs.

Über die Regeln zur Überwachung von Datei-Operationen

Die Aufgabe Überwachung der Datei-Integrität wird auf der Grundlage der Regeln zur Überwachung von Datei-Operationen ausgeführt. Sie können mithilfe von Auslösekriterien für Regeln die Bedingungen zum Auslösen der Aufgabe anpassen und die Ereigniskategorie für gefundene Dateioperationen bestimmen, die im Bericht über Aufgabenausführung gespeichert werden.

Die Regel zur Überwachung von Datei-Operationen wird für jeden festgelegten Überwachungsbereich angegeben.

Sie können folgende Auslösekriterien für Regeln anpassen:

- Vertrauenswürdige Benutzer
- Datei-Operations-Marker

Vertrauenswürdige Benutzer

Standardmäßig stuft das Programm die Aktionen aller Benutzer als potenzielle Verletzungen der Sicherheit ein. Die Liste mit vertrauenswürdigen Benutzern ist leer. Sie können die Ereigniskategorien des Ereignisses anpassen, indem Sie eine Liste mit vertrauenswürdigen Benutzern in den Einstellungen der Regel zur Überwachung von Datei-Operationen erstellen.

Ein *nicht vertrauenswürdiger Benutzer* ist ein beliebiger Benutzer, der nicht zur Liste vertrauenswürdiger Benutzer in den Einstellungen des Überwachungsbereichs hinzugefügt wurde. Wenn Kaspersky Security 10.1 für Windows

Server 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 Bericht über Aufgabenausführung.

Ein vertrauenswürdiger Benutzer ist ein Benutzer oder eine Benutzergruppe, dem/der das Ausführen von Dateioperationen im angegebenen Überwachungsbereich erlaubt ist. Wenn Kaspersky Security 10.1 für Windows Server Dateioperationen findet, die von einem vertrauenswürdigen Benutzer ausgeführt wurden, protokolliert die Aufgabe zur Überwachung der Datei-Integrität ein Informatives Ereignis im Bericht über Aufgabenausführung.

Kaspersky Security 10.1 für Windows Server kann Benutzer nicht bestimmen, die Operationen in einem Zeitraum, in dem die Überwachung unterbrochen war, ausführen. In diesem Fall wird der Status des Benutzers als Unbekannt angegeben.

Unbekannter Benutzer – dieser Status wird einem Benutzer zugewiesen, wenn Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server 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 Bericht über Aufgabenausführung.

Datei-Operations-Marker

Während der Ausführung der Aufgabe zur Überwachung der Datei-Integrität ermittelt Kaspersky Security 10.1 für Windows Server mithilfe von Datei-Operations-Markern, ob eine Aktion mit einer Datei ausgeführt wurde.

Der Datei-Operations-Marker ist ein eindeutiges Merkmal, mit dem eine Dateioperation charakterisiert werden kann.

Jede Dateioperation kann eine einzelne Aktion oder eine Kette von Aktionen mit Dateien darstellen. Jede solche Aktion wird einem Datei-Operations-Marker gleichgestellt. Wenn in der Kette der Dateioperationen ein Marker gefunden wird, der von Ihnen als Auslösekriterium für eine Überwachungsregel festgelegt wurde, protokolliert das Programm das Ereignis nach der Durchführung einer solchen Dateioperation.

Die Ereigniskategorie der protokollierten Ereignisse hängt nicht von den ausgewählten Datei-Operations-Markern oder ihrer Anzahl ab.

Standardmäßig werden von Kaspersky Security 10.1 für Windows Server alle verfügbaren Datei-Operations-Marker berücksichtigt. Sie können Datei-Operations-Marker manuell in den Einstellungen der Aufgabenregeln auswählen (s. Tabelle unten).

Tabelle 41. 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

ID der Dateioperation	Datei-Operations-Marker	Unterstützte Dateisysteme
DATA_TRUNCATION	Die Datei bzw. der Ordner wurde gekürzt	NTFS, ReFS
EA_CHANGE	Erweiterte Attribute von Datei oder Ordner wurden verändert	Nur NTFS
ENCRYPTION_CHANGE	Der Verschlüsselungsstatus der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
FILE_CREATE	Die Datei bzw. der Ordner wurde zum ersten Mal erstellt	NTFS, ReFS
FILE_DELETE	Eine Datei oder ein Ordner wurde mit der Tastenkombination UMSCHALT+ENTF permanent gelöscht.	NTFS, ReFS
HARD_LINK_CHANGE	Für die Datei bzw. den Ordner wurde ein harter Link erstellt oder gelöscht	Nur NTFS
INDEXABLE_CHANGE	Der Indizierungsstatus der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
INTEGRITY_CHANGE	Das Integritätsattribut für den benannten Dateidatenstrom wurde verändert	Nur ReFS
NAMED_DATA_EXTEND	Die Größe des benannten Dateidatenstroms hat sich erhöht	NTFS, ReFS
NAMED_DATA_OVERWRITE	Ein benannter Dateidatenstrom wurde überschrieben	NTFS, ReFS
NAMED_DATA_TRUNCATION	Ein benannter Dateidatenstrom wurde gekürzt	NTFS, ReFS
OBJECT_ID_CHANGE	Die ID der Datei bzw. des Ordners wurde verändert	NTFS, ReFS
RENAME_NEW_NAME	Der Datei bzw. dem Ordner wurde ein neuer Name zugewiesen	NTFS, ReFS
REPARSE_POINT_CHANGE	Für die Datei bzw. den Ordner wurde ein neuer Analysepunkt erstellt oder ein vorhandener Punkt verändert	NTFS, ReFS
SECURITY_CHANGE	Die Zugriffsrechte zur Datei bzw. zum Ordner wurden verändert	NTFS, ReFS
STREAM_CHANGE	Ein neuer benannter Dateidatenstrom wurde erstellt oder ein vorhandener verändert	NTFS, ReFS
TRANSACTED_CHANGE	Ein benannter Dateidatenstrom wurde durch die TxF-Transaktion verändert	Nur ReFS

Aufgabe „Überwachung der Datei-Integrität" anpassen

Sie können die Standard-Einstellungen der Aufgabe Überwachung der Datei-Integrität anpassen (s. Tabelle unten).

Tabelle 42. Standardeinstellungen der Aufgabe Überwachung der Datei-Integrität

Einstellung	Bedeutung	Einstellungsmöglichkeiten
Überwachungsbereiche	Nicht festgelegt.	Sie können Ordner und Dateien angeben, deren Aktionen überwacht werden sollen. Für die Ordner und Dateien des angegebenen Überwachungsbereichs werden Überwachungsereignisse erstellt.
Liste mit vertrauenswürdigen Benutzern	Nicht festgelegt.	Sie können Benutzer und\oder Benutzergruppen festlegen, deren Aktionen in den angegebenen Verzeichnissen von der Komponente als sicher bewertet werden sollen.
Dateioperationen in Leerlaufperioden der Aufgabe kontrollieren	Wird verwendet	Sie können die Protokollierung von Dateioperationen aktivieren oder deaktivieren, die in den angegebenen Überwachungsbereichen in Leerlaufperioden der Aufgabe ausgeführt wurden.
Ausgeschlossene Überwachungsbereiche berücksichtigen	Wird nicht verwendet	Sie können die Anwendung von Ausnahmen für Ordner regeln, in denen keine Dateioperationen überwacht werden müssen. Bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität überspringt Kaspersky Security 10.1 für Windows Server Überwachungsbereiche, die als Ausnahmen festgelegt wurden.
Datei-Operations-Marker berücksichtigen	Es werden alle verfügbaren Datei-Operations-Marker berücksichtigt.	Sie können eine Reihe von Markern angeben, die Dateioperationen kennzeichnen. Wenn eine im Überwachungsbereich ausgeführte Dateioperation mit einem der angegebenen Marker gekennzeichnet ist, erstellt Kaspersky Security 10.1 für Windows Server ein Überwachungsereignis.
Berechnung der Prüfsumme	Wird nicht verwendet	Sie können festlegen, dass die Berechnung der Prüfsumme der Datei nach deren Bearbeitung durchgeführt wird.
Datei-Operations-Marker berücksichtigen	Es werden alle verfügbaren Datei-Operations-Marker berücksichtigt.	Sie können eine Reihe von Markern angeben, die Dateioperationen kennzeichnen. Wenn eine im Überwachungsbereich ausgeführte Dateioperation mit einem oder mehreren angegebenen Marker gekennzeichnet ist, erstellt Kaspersky Security 10.1 für Windows Server ein Systemaudit-Ereignis.
Zeitplan für den Aufgabenstart	Der erste Start ist nicht festgelegt	Sie können die Standardeinstellungen einer geplanten Aufgabe anpassen.

Gehen Sie wie folgt vor, um die Einstellungen der Aufgabe zur Überwachung der Datei-Integrität anzupassen:

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen

anpassen möchten.

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **System-Diagnose** im Block **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Überwachung der Datei-Integrität** wird geöffnet.

4. Passen Sie im folgenden Fenster auf der Registerkarte **Einstellungen zur Überwachung von Dateioperationen** die Einstellungen des Überwachungsbereichs an:

   a. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Ereignisse zu Dateioperationen protokollieren, die im Zeitraum, in dem die Überwachung unterbrochen war, ausgeführt wurden**.

      Das Kontrollkästchen aktiviert oder deaktiviert die Überwachung der Dateioperationen, die in den Einstellungen der Aufgabe Überwachung der Datei-Integrität ausgewählt sind, auch in Zeiträumen, in denen die Aufgabenausführung aus irgendeinem Grund unterbrochen ist (Entfernung der Festplatte, Beenden der Aufgabe durch Benutzer, Funktionsstörung der Software).

      Wenn das Kontrollkästchen aktiviert ist, protokolliert Kaspersky Security 10.1 für Windows Server die Ereignisse in allen Überwachungsbereichen während der Unterbrechung der Aufgabe zur Überwachung der Datei-Integrität.

      Wenn das Kontrollkästchen deaktiviert ist, werden die Dateioperationen in den Überwachungsbereichen bei einer Unterbrechung der Aufgabe nicht vom Programm protokolliert.

      Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   b. Fügen Sie die Überwachungsbereiche (siehe Abschnitt "Einstellungen der Überwachungsregeln anpassen" auf Seite 278) hinzu, die von der Aufgabe überwacht werden sollen.

5. Starten Sie auf der Registerkarte **Aufgabenverwaltung** die Aufgabe auf der Grundlage eines Zeitplans (siehe Abschnitt "Arbeit mit dem Aufgabenzeitplan" auf Seite 148).

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Einstellungen der Überwachungsregeln anpassen

Standardmäßig ist kein Überwachungsbereich angegeben: Die Aufgabe überwacht in keinem einzigen Verzeichnis die Ausführung von Dateioperationen.

► *Um einen Überwachungsbereich hinzuzufügen, gehen Sie wie folgt vor:*

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

Verwaltete Geräte und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.

2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **System-Diagnose** im Block **Überwachung der Datei-Integrität** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Eigenschaften: Überwachung der Datei-Integrität** wird geöffnet.

4. Klicken Sie im Block **Überwachungsbereich** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Überwachungsbereich** wird geöffnet.

5. Fügen Sie den Überwachungsbereich auf eine der folgenden Arten hinzu:
   - Wenn Sie im Standarddialog von Microsoft Windows Ordner auswählen möchten:
     a. Klicken Sie auf **Durchsuchen**.

        Das Microsoft-Windows-Standardfenster "Ordner suchen" wird geöffnet.

     b. Wählen Sie im nächsten Fenster den Ordner aus, dessen Dateioperationen Sie überwachen möchten, und klicken Sie auf **OK**.
   - Um den Überwachungsbereich manuell festzulegen, fügen Sie mithilfe einer der unterstützten Masken einen Pfad hinzu:
     - <*.ext> – alle Dateien mit der Erweiterung <ext> unabhängig von ihrem Speicherort
     - <*\name.ext> – alle Dateien mit dem Namen name und der Erweiterung <ext> unabhängig von ihrem Speicherort
     - <\dir*> – alle Dateien im Verzeichnis <\dir>
     - <\dir*\name.ext> – alle Dateien mit dem Namen name und der Erweiterung <ext> im Verzeichnis <\dir> und allen Unterverzeichnissen

   > Stellen Sie bei der manuellen Angabe des Überwachungsbereichs sicher, dass der Pfad dem folgenden Format entspricht: <Laufwerksbuchstabe>:\<Maske>. Wenn der Laufwerksbuchstabe fehlt, fügt Kaspersky Security 10.1 für Windows Server den angegebenen Überwachungsbereich nicht hinzu.

6. Klicken Sie auf der Registerkarte **Vertrauenswürdige Benutzer** auf die Schaltfläche **Hinzufügen**.

   Das Microsoft-Windows-Standardfenster **Auswählen: Benutzer oder Gruppen** wird geöffnet.

7. Wählen Sie die Benutzer oder Benutzergruppen aus, die Dateioperationen in den ausgewählten Überwachungsbereichen ausführen dürfen, und klicken Sie auf **OK**.

Standardmäßig stuft Kaspersky Security 10.1 für Windows Server alle Benutzer, die nicht zur Liste der vertrauenswürdigen Benutzer hinzugefügt wurden, als nicht vertrauenswürdig ein (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 274) und erstellt für sie kritische Ereignisse.

8. Wählen Sie die Registerkarte **Datei-Operations-Marker** aus.
9. Gehen Sie wie folgt vor, um bei Bedarf mehrere Datei-Operations-Marker auszuwählen:
   a. Wählen Sie die Option **Dateioperationen anhand der folgenden Marker erkennen** aus.
   b. Aktivieren Sie in der Liste der verfügbaren Dateioperationen (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 274) die Kontrollkästchen aller Operationen, die Sie überwachen möchten.

Standardmäßig überwacht Kaspersky Security 10.1 für Windows Server alle verfügbaren Dateioperationen, wenn die Option **Dateioperationen anhand von allen identifizierbaren Markern erkennen** ausgewählt ist.

10. Wenn Sie möchten, dass Kaspersky Security 10.1 für Windows Server die Prüfsumme der Dateien nach ihrer Bearbeitung ermittelt, gehen Sie wie folgt vor:
    a. Aktivieren Sie im Block **Berechnung der Prüfsumme** das Kontrollkästchen **Prüfsumme der geänderten Datei berechnen, wenn möglich**.

       Wenn das Kontrollkästchen aktiviert ist, ermittelt Kaspersky Security 10.1 für Windows Server die Prüfsumme der geänderten Datei, in der eine Dateioperation gefunden wurde, die mindestens einem Datei-Operations-Marker entspricht.

       Wenn die Dateioperation anhand mehrerer Marker gleichzeitig gefunden wird, so wird nur die endgültige Prüfsumme der Datei nach allen Änderungen ermittelt.

       Ist das Kontrollkästchen deaktiviert, berechnet Kaspersky Security 10.1 für Windows Server keine Prüfsumme für geänderte Dateien.

       In den folgenden Fällen wird keine Berechnung der Prüfsumme vorgenommen:

       - Wenn infolge der Dateioperation die Datei nicht mehr verfügbar ist (weil z. B. die Zugriffsrechte für die Datei geändert wurden)
       - Wenn in der Datei eine Dateioperation gefunden wurde, die daraufhin gelöscht wurde

       Das Kontrollkästchen ist standardmäßig deaktiviert.

    b. Wählen Sie in der Dropdown-Liste **Prüfsumme anhand von Algorithmus berechnen** eine der folgenden Optionen aus:

       - **MD5-Hash**
       - **SHA256-Hash**

11. Wenn Sie nicht alle Dateioperationen überwachen möchten, aktivieren Sie in der Liste der verfügbaren Dateioperationen (siehe Abschnitt "Über die Regeln zur Überwachung von Datei-Operationen" auf Seite 274) die Kontrollkästchen neben den Operationen, die Sie überwachen möchten.
12. Gehen Sie wie folgt vor, um bei Bedarf Ausnahmen für den Überwachungsbereich hinzuzufügen:
    a. Wählen Sie die Registerkarte **Ausnahmen** aus.
    b. Aktivieren Sie das Kontrollkästchen **Ausgeschlossene Überwachungsbereiche berücksichtigen**.

Das Kontrollkästchen aktiviert oder deaktiviert die Anwendung von Ausnahmen für Ordner, in denen keine Dateioperationen überwacht werden müssen.

Wenn dieses Kontrollkästchen aktiviert ist, überspringt Kaspersky Security 10.1 für Windows Server bei der Ausführung der Aufgabe zur Überwachung der Datei-Integrität die Überwachungsbereiche, die zur Liste mit Ausnahmen hinzugefügt wurden.

Wenn das Kontrollkästchen deaktiviert ist, protokolliert Kaspersky Security 10.1 für Windows Server Ereignisse für alle angegebenen Überwachungsbereiche.

Standardmäßig ist das Kontrollkästchen deaktiviert und die Ausnahmeliste leer.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Ordner zum Hinzufügen auswählen** wird geöffnet.

d. Wählen Sie im geöffneten Fenster den Ordner aus, den Sie aus dem Überwachungsbereich ausschließen möchten.

e. Klicken Sie auf **OK**.

   Der angegebene Ordner wird zur Liste der ausgeschlossenen Bereiche hinzugefügt.

13. Klicken Sie im Fenster **Überwachungsbereich** auf **OK**.

    Die angegebenen Einstellungen der Regeln werden im ausgewählten Überwachungsbereich der Aufgabe "Überwachung der Datei-Integrität" gelten.

Protokollanalyse

Dieser Abschnitt enthält Informationen über die Aufgabe zur Protokollanalyse und die Aufgabeneinstellungen.

In diesem Abschnitt

Über die Aufgabe Protokollanalyse

Während der Ausführung der Aufgabe zur Protokollanalyse überwacht Kaspersky Security 10.1 für Windows Server die Integrität der geschützten Umgebung auf Basis der Ergebnisse der Analyse der Windows-Ereignisprotokolle. Das Programm informiert den Administrator, wenn Anzeichen für untypisches Verhalten im System gefunden werden; solche Anzeichen können auf Angriffsversuche auf den Computer hindeuten.

Kaspersky Security 10.1 für Windows Server liest die Daten der Windows-Ereignisprotokolle aus und ermittelt Verstöße entsprechend den vom Benutzer festgelegten Regeln oder den Einstellungen der heuristischen Analyse, die von der Aufgabe zur Protokollanalyse verwendet wird.

Vordefinierte Regeln und heuristische Analyse.

Mit der Aufgabe Protokollanalyse können Sie den Status des geschützten Systems überwachen, indem Sie die vordefinierten Regeln anwenden, die auf bestehenden Heuristiken basieren. Die heuristische Analyse ermittelt

das Vorhandensein von anomaler Aktivität auf dem geschützten Server, die ein Merkmal von versuchten Angriffen sein kann. Die Vorlagen für die Ermittlung von anomaler Aktivität finden Sie in den verfügbaren Heuristiken in den vordefinierten Regeleinstellungen.

In der Regelliste sind sieben Heuristiken für die Protokollanalyse verfügbar. Sie können die Verwendung jeder Regel aktivieren und deaktivieren. Sie können vorhandene Regeln nicht löschen und keine neuen Regeln erstellen.

Sie können die auslösenden Kriterien für Regeln, die Ereignisse überwachen, für die folgenden Operationen konfigurieren:

- Verarbeitung von Brute-Force
- Verarbeitung der Netzwerkanmeldung

In den Einstellungen der Aufgabe können Sie auch Ausnahmen anpassen. Die heuristische Analyse wird nicht ausgelöst, wenn die Anmeldung von einem vertrauenswürdigen Benutzer oder von einer vertrauenswürdigen IP-Adresse durchgeführt wurde.

Kaspersky Security 10.1 für Windows Server 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 Bericht über Aufgabenausführung der Aufgabe zur Protokollanalyse.

Benutzerdefinierte Regeln der Aufgabe Protokollanalyse

Mithilfe der Einstellungen der Aufgabenregeln können Sie Auslösekriterien für Regeln beim Fund bestimmter Ereignisse im angegebenen Windows-Protokoll angeben und bearbeiten. Standardmäßig enthält die Regelliste der Aufgabe zur Protokollanalyse vier Regeln. Sie können die Verwendung dieser Regeln aktivieren und deaktivieren, Regeln löschen und ihre Einstellungen bearbeiten.

Sie können für jede Regel folgende Auslösekriterien anpassen:

- Liste der IDs der Einträge im Windows-Ereignisprotokoll

  Die Regel wird ausgelöst, sobald ein neuer Eintrag im Windows-Ereignisprotokoll gefunden wird, dessen Parameter die für diese Regel angegebene Ereignis-ID enthalten. Sie können IDs für jede angegebene Regel hinzufügen und löschen.

- Ereignisquelle

  Sie können für jede Regel ein Unterprotokoll des Windows-Ereignisprotokolls festlegen. Das Programm wird nur in diesem Unterprotokoll nach Einträgen mit den angegebenen Ereignis-IDs suchen. Sie können eines der Standard-Unterprotokolle (Programm, Sicherheit oder System) auswählen, oder ein benutzerdefiniertes Unterprotokoll angeben, in dem Sie den Namen im Feld zur Auswahl der Quelle angeben.

  Das Programm prüft nicht, ob das angegebene Unterprotokoll tatsächlich im Windows-Ereignisprotokoll vorhanden ist.

Wenn die Regel ausgelöst wird, protokolliert Kaspersky Security 10.1 für Windows Server ein "Kritisches Ereignis" im Bericht über Aufgabenausführung der Protokollanalyse.

Standardmäßig übernimmt die Aufgabe zur Protokollanalyse keine benutzerdefinierten Regeln.

Bevor Sie die Aufgabe zur Protokollanalyse starten, vergewissern Sie sich, dass die Systemaudit-Richtlinie korrekt eingerichtet ist. Weitere Informationen finden Sie im Microsoft-Artikel https://technet.microsoft.com/en-us/library/cc952128.aspx.

Regeln für vorkonfigurierte Aufgaben anpassen

► *Um die vorkonfigurierten Regeln für die Aufgabe zur Protokollanalyse anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.
2. Im Ergebnisfenster der ausgewählten Administrationsgruppe führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen (s. Abschnitt "**Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

   Das Fenster **Einstellungen der Protokollanalyse** wird geöffnet.
4. Wählen Sie die Registerkarte **Vorkonfigurierte Regeln** aus.
5. Deaktivieren oder aktivieren Sie das Kontrollkästchen **Vorkonfigurierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Security 10.1 für Windows Server die heuristische Analyse zum Erkennen anomaler Aktivität auf dem geschützten Server.

   Ist dieses Kontrollkästchen nicht aktiviert, ist die heuristische Analyse deaktiviert und Kaspersky Security 10.1 für Windows Server verwendet zum Erkennen anomaler Aktivität die vorinstallierten oder benutzerdefinierte Regeln.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert.

   Für die Ausführung der Aufgabe muss zumindest eine Regel für die Protokollanalyse ausgewählt sein.
6. Wählen Sie aus der Liste der vorkonfigurierten Regeln jene Regeln aus, die Sie für die Protokollanalyse

verwenden möchten:

- Ein möglicher Versuch, das Kennwort anhand von Brute-Force zu knacken, wurde entdeckt
- Anzeichen für eine Gefährdung der Windows-Protokolle wurden gefunden
- Verdächtige Aktivitäten des neu installierten Dienstes wurden gefunden
- Eine verdächtige Authentifizierung mit eindeutiger Angabe von Anmeldedaten wurde gefunden
- Anzeichen für den Angriff Kerberos forged PAC (MS14-068) wurden gefunden
- Verdächtige Veränderungen in der privilegierten Gruppe Administratoren wurden gefunden
- Verdächtige Aktivitäten während der Anmeldesitzung im Netzwerk wurden gefunden

7. Um die ausgewählten Regeln anzupassen, klicken Sie auf die Schaltfläche **Erweiterte Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

8. Geben Sie im Block **Verarbeitung von Brute-Force** die Anzahl der Versuche sowie den Zeitraum an, in dem die Versuche ausgeführt wurden, die als Auslösekriterien der heuristischen Analyse dienen sollen.
9. Geben Sie im Block **Verarbeitung der Netzwerkanmeldung** den Anfang und das Ende der Zeitspanne an, innerhalb der das Ausführen eines Anmeldeversuches von Kaspersky Security 10.1 für Windows Server als anomale Aktivität betrachtet wird.
10. Wählen Sie die Registerkarte **Ausnahmen** aus.
11. Um Benutzer hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Klicken Sie auf **Durchsuchen**.
    b. Wählen Sie einen Benutzer aus.
    c. Klicken Sie auf **OK**.

       Der angegebene Benutzer wird zur Liste der vertrauenswürdigen Benutzer hinzugefügt.
12. Um IP-Adressen hinzuzufügen, die als vertrauenswürdig betrachtet werden, gehen Sie wie folgt vor:
    a. Geben Sie die IP-Adresse ein.
    b. Klicken Sie auf die Schaltfläche **Hinzufügen**.
13. Die angegebene IP-Adresse wird zur Liste der vertrauenswürdigen IP-Adressen hinzugefügt.
14. Passen Sie auf der Registerkarte **Aufgabenverwaltung** den geplanten Aufgabenstart an (siehe Abschnitt "Zeitplan-Einstellungen für den Aufgabenstart anpassen" auf Seite 148).
15. Klicken Sie auf **OK**.

Die Einstellungen der Aufgabe zur Protokollanalyse werden gespeichert.

Regeln für die Protokollanalyse anpassen

► *Um eine neue benutzerdefinierte Regel für die Protokollanalyse hinzuzufügen und anzupassen, gehen Sie wie folgt vor:*

1. Erweitern Sie in der Struktur der Verwaltungskonsole von Kaspersky Security Center den Knoten **Verwaltete Geräte** und wählen Sie die Administrationsgruppe aus, für die Sie die Programmeinstellungen anpassen möchten.

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

   - Wählen Sie die Registerkarte **Richtlinien** und öffnen Sie das Fenster **Eigenschaften: <Richtlinienname>**, um die Programmeinstellungen für eine Servergruppe anzupassen **(s. Abschnitt „Richtlinie anpassen" auf S.** 111**)**.
   - Um die Programmeinstellungen für einen einzelnen Server anzupassen, wählen Sie die Registerkarte **Geräte** und öffnen Sie das Fenster **Programmeinstellungen** (siehe Abschnitt "**Lokale Aufgaben im Fenster Programmeinstellungen von Kaspersky Security Center anpassen**" auf Seite 125).

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

3. Klicken Sie im Abschnitt **System-Diagnose** im Block **Protokollanalyse** auf die Schaltfläche **Einstellungen**.

   Das Fenster **Protokollanalyse** wird geöffnet.

4. Deaktivieren oder aktivieren Sie auf der Registerkarte **Regeln für die Protokollanalyse** das Kontrollkästchen **Benutzerdefinierte Regeln für die Protokollanalyse verwenden**.

   Wenn dieses Kontrollkästchen aktiviert ist, verwendet Kaspersky Security 10.1 für Windows Server die benutzerdefinierten Regeln für die Protokollanalyse entsprechend den eingestellten Einstellungen der jeweiligen Regel. Sie können Regeln für die Protokollanalyse hinzufügen, entfernen oder anpassen.

   Wenn das Kontrollkästchen deaktiviert ist, können benutzerdefinierte Regeln weder hinzugefügt noch geändert werden. Kaspersky Security 10.1 für Windows Server übernimmt die Standard-Regeleinstellungen.

   Das Kontrollkästchen ist in der Grundeinstellung aktiviert. Lediglich die Regel "Ein Pop-up-Fenster einer App wurde gefunden" ist aktiv.

   Sie können kontrollieren, ob die vordefinierten Regeln für die Protokollanalyse übernommen werden. Aktivieren Sie die Kontrollkästchen neben den Regeln, die Sie für die Protokollanalyse übernehmen möchten.

5. Um eine neue benutzerdefinierte Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Regeln für die Protokollanalyse** wird geöffnet.

6. Geben Sie im Block **Allgemein** die folgenden Daten der neuen Regel ein:

   - **Name**
   - **Quelle**

     Wählen Sie das Protokoll aus, dessen Ereignisse für die Analyse verwendet werden sollen. Die folgenden Arten des Windows-Ereignisprotokolls sind verfügbar:

     - Programm
     - Sicherheit
     - System

     Sie können ein neues benutzerdefiniertes Protokoll hinzufügen, indem Sie den Namen des Protokolls in das Feld **Quelle** eingeben.

7. Geben Sie im Block **Auslöseeinstellungen** die ID der Einträge an, durch die die Regel ausgelöst wird:
   a. Geben Sie den Zahlenwert der ID ein.
   b. Klicken Sie auf die Schaltfläche **Hinzufügen**.

      Die angegebene Regel-ID wird zur Liste hinzugefügt. Sie können für jede Regel eine unbegrenzte Anzahl von IDs hinzufügen.
   c. Klicken Sie auf **OK**.

   Die Regel für die Protokollanalyse wird zur allgemeinen Regelliste hinzugefügt.

Arbeiten mit Kaspersky Security 10.1 für Windows Server aus der Befehlszeile

Dieser Abschnitt beschreibt die Arbeit mit Kaspersky Security 10.1 für Windows Server aus der Befehlszeile.

In diesem Kapitel

Befehle der Befehlszeile

Sie können die Basisbefehle zur Verwaltung von Kaspersky Security 10.1 für Windows Server aus der Befehlszeile des geschützten Servers erteilen, wenn Sie bei der Installation von Kaspersky Security 10.1 für Windows Server den Punkt Befehlszeilen-Tool zur Installation ausgewählt haben.

Mit Hilfe der Befehlszeile können Sie nur Funktionen steuern, für die Sie in Kaspersky Security 10.1 für Windows Server zugriffsberechtigt sind.

Bestimmte Befehle von Kaspersky Security 10.1 für Windows Server werden in folgenden Modi ausgeführt:

- Synchronmodus: Die Kontrolle kehrt sofort nach Abschluss der Befehlsausführung zur Konsole zurück.
- Asynchronmodus: Die Kontrolle kehrt sofort nach dem Befehlsstart zur Konsole zurück.

► *Um die Ausführung eines synchronen Befehls zu unterbrechen,*

drücken Sie die Tasten **Strg+C**.

Gehen Sie entsprechend der folgenden Regeln vor, wenn Sie Befehle für Kaspersky Security 10.1 für Windows Server eingeben:

- Beachten Sie bei der Eingabe von Schlüsseln und Befehlen die Groß- und Kleinschreibung.
- Trennen Sie Schlüssel durch Leerzeichen voneinander.
- Wenn der Name einer Datei, den Sie als Wert für einen Schlüssel angeben, ein Leerzeichen enthält, setzen Sie den Dateinamen (und den entsprechenden Pfad) in Anführungszeichen, z. B.: "`C:\TEST\test cpp.exe`".
- Bei Bedarf können Sie in Masken für Dateinamen oder Pfade Platzhalterzeichen verwenden. Beispiele: "`C:\Temp\Temp*\`", "`C:\Temp\Temp???.doc`", "`C:\Temp\Temp*.doc`"

Mithilfe der Befehlszeile können Sie das gesamte Spektrum an Operationen zur Steuerung und Verwaltung von Kaspersky Security 10.1 für Windows Server ausführen (siehe Tabelle unten).

Tabelle 43. Befehle für Kaspersky Security 10.1 für Windows Server

Befehl	Beschreibung
KAVSHELL APPCONTROL (siehe Abschnitt "Ergänzen der Regelliste für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL" auf Seite 300)	Ergänzt die Liste der gebildeten Regeln für die Kontrolle des Programmstarts entsprechend dem ausgewählten Prinzip für das Hinzufügen.
KAVSHELL APPCONTROL /CONFIG (siehe Abschnitt "Verwaltung der Aufgabe Kontrolle des Programmstarts. KAVSHELL APPCONTROL /CONFIG" auf Seite 297).	Verwaltung des Ausführungsmodus der Aufgabe zur Kontrolle des Programmstarts.
KAVSHELL APPCONTROL /GENEARTE (siehe Abschnitt "Automatisches Erstellen von Erlaubnisregeln. KAVSHELL APPCONTROL /GENERATE" auf Seite 298).	Erstellt eine Aufgabe zum automatischen Erstellen von Erlaubnisregeln für die Kontrolle des Programmstarts.
KAVSHELL VACUUM (siehe Abschnitt "Log-Dateien für Kaspersky Security 10.1 für Windows Server defragmentieren.KAVSHELL VACUUM" auf Seite 310)	Defragmentiert die Log-Dateien für Kaspersky Security 10.1 für Windows Server.
KAVSHELL PASSWORD	Verwaltet die Einstellungen des Kennwortschutzes.
KAVSHELL HELP (siehe Abschnitt "Hilfe für Befehle in Kaspersky Security 10.1 für Windows Server anzeigen.KAVSHELL HELP" auf Seite 290)	Zeigt die Hilfe für Befehle in Kaspersky Security 10.1 für Windows Server an.
KAVSHELL START (siehe Abschnitt "Kaspersky Security Service starten und anhalten. KAVSHELL START, KAVSHELL STOP" auf Seite 290)	Startet den Dienst von Kaspersky Security 10.1 für Windows Server.
KAVSHELL STOP (siehe Abschnitt "Kaspersky Security Service starten und anhalten. KAVSHELL START, KAVSHELL STOP" auf Seite 290)	Stoppt den Dienst von Kaspersky Security 10.1 für Windows Server.
KAVSHELL SCAN (siehe Abschnitt "Ausgewählten Bereich untersuchen.KAVSHELL SCAN" auf Seite 291)	Erstellt und startet eine temporäre Aufgabe zur Untersuchung auf Befehl mit einem Untersuchungsbereich und Sicherheitsparametern, die durch Befehlsschlüssel vorgegeben werden.

Befehl	Beschreibung
KAVSHELL SCANCRITICAL (siehe Abschnitt "Aufgabe zur Untersuchung wichtiger Bereiche starten.KAVSHELL SCANCRITICAL" auf Seite 295)	Startet die Systemaufgabe Untersuchung wichtiger Bereiche.
KAVSHELL TASK (siehe Abschnitt "Angegebene Aufgabe asynchron verwalten.KAVSHELL TASK" auf Seite 296)	Startet / Hält an / Setzt fort / Beendet die angegebene Aufgabe im asynchronen Modus. / Gibt den aktuellen Aufgabenstatus / eine Statistik für die Aufgabe zurück.
KAVSHELL RTP (siehe Abschnitt "Aufgaben zum Echtzeitschutz starten und stoppen.KAVSHELL RTP" auf Seite 297)	Startet oder beendet alle Echtzeitschutz-Aufgaben.
KAVSHELL UPDATE (siehe Abschnitt "Aufgabe zum Datenbanken-Update von Kaspersky Security 10.1 für Windows Server starten.KAVSHELL UPDATE" auf Seite 302)	Startet die Aufgabe zum Datenbanken-Update von Kaspersky Security 10.1 für Windows Server mit den festgelegten Befehlszeilenparametern.
KAVSHELL ROLLBACK (siehe Abschnitt "Rollback von Datenbanken-Updates von Kaspersky Security 10.1 für Windows Server.KAVSHELL ROLLBACK" auf Seite 306)	Kehrt zur vorherigen Version der Datenbanken zurück.
KAVSHELL LICENSE (siehe Abschnitt "Programm aktivieren. KAVSHELL LICENSE" auf Seite 307)	Verwaltet die Aktivierungsschlüssel und Aktivierungscodes.
KAVSHELL TRACE (siehe Abschnitt "Protokoll zur Ablaufverfolgung aktivieren, anpassen und deaktivieren.KAVSHELL TRACE" auf Seite 308)	Aktiviert oder deaktiviert das Führen des Protokolls zur Ablaufverfolgung, Verwalten der Parameter für das Protokolls zur Ablaufverfolgung.
KAVSHELL DUMP (siehe Abschnitt "Anlegen von Dump-Dateien ein- und ausschalten.KAVSHELL DUMP" auf Seite 311)	Aktiviert bzw. deaktiviert die Erstellung von Dump-Dateien für Prozesse von Kaspersky Security 10.1 für Windows Server bei einem Absturz von Prozessen.
KAVSHELL IMPORT (siehe Abschnitt "Einstellungen importieren.KAVSHELL IMPORT" auf Seite 312)	Importiert die allgemeinen Einstellungen, Funktionen und Aufgaben für Kaspersky Security 10.1 für Windows Server aus einer zuvor erstellten Konfigurationsdatei.

Befehl	Beschreibung
KAVSHELL EXPORT (siehe Abschnitt "Einstellungen exportieren.KAVSHELL EXPORT" auf Seite 313)	Exportiert alle Einstellungen und vorhandene Aufgaben von Kaspersky Security 10.1 für Windows Server in eine Konfigurationsdatei.
KAVSHELL DEVCONTROL (siehe Abschnitt "Liste der Regeln für die Gerätekontrolle ergänzen.KAVSHELL DEVCONTROL" auf Seite 302)	Ergänzt die Liste der erstellten Regeln für die Gerätekontrolle entsprechend dem ausgewählten Prinzip für das Hinzufügen.

Hilfe für Befehle in Kaspersky Security 10.1 für Windows Server anzeigen. KAVSHELL HELP

Um eine Liste aller Befehle für Kaspersky Security 10.1 für Windows Server zu öffnen, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Um die Beschreibung und Syntax eines Befehls zu erhalten, führen Sie einen der folgenden Befehle aus:

```
KAVSHELL HELP <Befehl>

KAVSHELL <Befehl> /?
```

Beispiele für den Befehl KAVSHELL HELP

Um ausführliche Informationen zu dem Befehl KAVSHELL SCAN zu erhalten, führen Sie folgenden Befehl aus:

```
KAVSHELL HELP SCAN
```

Kaspersky Security Service starten und anhalten KAVSHELL START, KAVSHELL STOP

Um Kaspersky Security Service zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL START
```

Wenn Kaspersky Security Service gestartet wird, werden standardmäßig folgende Aufgaben gestartet: Echtzeitschutz für Dateien und Untersuchung bei Systemstart, sowie andere Aufgaben, für deren Zeitplan die Startfrequenz **Bei Programmstart** gilt.

Um Kaspersky Security Service anzuhalten, führen Sie folgenden Befehl aus:

```
KAVSHELL STOP
```

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Angegebenen Bereich untersuchen. KAVSHELL SCAN

Um eine Untersuchung für bestimmte Bereich des geschützten Servers zu starten, verwenden Sie den Befehl `KAVSHELL SCAN`. Die Schlüssel dieses Befehls legen die Einstellungen des Untersuchungsbereichs und die Sicherheitseinstellungen des ausgewählten Knotens fest.

Eine Aufgabe zur Untersuchung auf Befehl, die mit dem Befehl `KAVSHELL SCAN` gestartet wurde, ist temporär. Sie wird nur während ihrer Ausführung in der Konsole für Kaspersky Security 10.1 angezeigt (die Aufgabeneinstellungen können nicht in der Konsole von Kaspersky Security 10.1 angezeigt werden). Das Protokoll über die Leistung der Aufgabe wird gleichzeitig erzeugt. Es wird in den **Berichten über Aufgabenausführung** der Konsole für Kaspersky Security 10.1 angezeigt. Auf die mithilfe des SCAN-Befehls erstellten und gestarteten Aufgaben können die Programmrichtlinien von Kaspersky Security Center angewandt werden.

Wenn Sie den Pfad in einer Aufgabe zur Untersuchung bestimmter Bereiche angeben, können Sie Umgebungsvariable verwenden. Wenn Sie eine Umgebungsvariable verwenden, die einem Benutzer zugeordnet ist, führen Sie den Befehl `KAVSHELL SCAN` mit den Rechten dieses Benutzers aus.

Der Befehl `KAVSHELL SCAN` wird synchron ausgeführt.

Um eine bestehenden Aufgabe zur Untersuchung auf Befehl aus der Befehlszeile zu starten, verwenden Sie den Befehl KAVSHELL TASK (siehe Abschnitt "Angegebene Aufgabe asynchron verwalten.KAVSHELL TASK" auf Seite 296).

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 Bericht über Aufgabenausführung>] [/ANSI] [/ALIAS:<Alias des Aufgabenamens>]
```

Der Befehl KAVSHELL SCAN enthält sowohl obligatorische als auch Reserveschlüssel, deren Verwendung optional ist (s. Tabelle unten).

Beispiele für den Befehl KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Tabelle 44. Schlüssel des Befehls KAVSHELL SCAN.

Schlüssel	Beschreibung
Untersuchungsbereich. Obligatorischer Schlüssel.	
<Dateien> <Ordner> <Netzwerkpfad>	Untersuchungsbereich – Liste mit Dateien, Ordnern, Netzwerkpfaden und vordefinierten Bereichen. Geben Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) an. Im folgenden Beispiel wird der Ordner Folder4 ohne Pfad angegeben. Er befindet sich im Ordner, aus dem der Befehl KAVSHELL ausgeführt wird: KAVSHELL SCAN Folder4 Wenn der Name des Objektes, das Sie untersuchen möchten, ein Leerzeichen enthält, muss dieser Name in Klammern stehen. Wenn Sie einen Ordner ausgewählt haben, untersucht Kaspersky Security 10.1 für Windows Server auch alle eingebetteten Unterordner für diesen Ordner. Um eine Gruppe der Datei zu untersuchen, können Sie die Zeichen * und ? verwenden.
/MEMORY	Objekte im Arbeitsspeicher untersuchen.
/SHARED	Freigegebene Ordner auf dem Server untersuchen.
/STARTUP	Autostart-Objekte untersuchen.
/REMDRIVES	Wechseldatenträger untersuchen.
/FIXDRIVES	Festplatten untersuchen.
/MYCOMP	Alle Bereiche des geschützten Servers untersuchen.
/L: <Name einer Datei mit einer Liste der Untersuchungsbereiche>	Name einer Datei mit einer Liste der Untersuchungsbereiche, einschließlich dem vollständigen Dateipfad. Trennen Sie die Untersuchungsbereiche in der Datei durch ein Zeilenwechselsymbol. Sie können vordefinierte Untersuchungsbereiche angeben, wie unten am Beispiel einer Datei mit einer Liste von Untersuchungsbereichen gezeigt wird: C:\ D:\Docs*.doc E:\My Documents /STARTUP /SHARED
Zu untersuchende Objekte (File types). Wenn Sie keine Werte für diesen Schlüssel angeben, untersucht Kaspersky Security 10.1 für Windows Server die Objekte nach Format.	
/FA	Alle Objekte untersuchen.
/FC	Objekte, die nach Format untersucht werden (Standard). Kaspersky Security 10.1 für Windows Server untersucht nur Objekte, die dem Format nach als infizierbar gelten.
/FE	Objekte nach Erweiterung untersuchen. Kaspersky Security 10.1 für Windows Server untersucht nur Objekte, die der Erweiterung nach als infizierbar gelten.

Schlüssel	Beschreibung
/NEWONLY	Nur neue und veränderte Dateien untersuchen. Wenn Sie diesen Schlüssel nicht angeben, untersucht Kaspersky Security 10.1 für Windows Server alle Objekte.
/AI: **Aktion für infizierte und andere Objekte**. Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Security 10.1 für Windows Server die Aktion **Überspringen** aus.	
DISINFECT	Desinfizieren, irreparable Objekte überspringen
DISINFDEL	Desinfizieren, irreparable Objekte überspringen
DELETE	Löschen Die Einstellungen DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Security 10.1 für Windows Server beibehalten, um die Kompatibilität mit den vorherigen Versionen zu gewährleisten. Diese Einstellungen können anstelle der Befehle /AI und /AS verwendet werden: In diesem Fall werden möglicherweise infizierte Objekte von Kaspersky Security 10.1 für Windows Server nicht bearbeitet.
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
/AS: **Aktion für möglicherweise infizierte Objekte**/ Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Security 10.1 für Windows Server die Aktion **Überspringen** aus.	
QUARANTINE	Quarantäne
DELETE	Löschen
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
Ausnahmen	
/E:ABMSPO	Dieser Schlüssel schließt zusammengesetzte Objekte der folgenden Typen aus: A – SFX-Archive B – E-Mail-Datenbanken M – Dateien mit E-Mailformaten S – Archive (SFX-Archive einschließlich) P – gepackte Objekte O – eingebettete OLE-Objekte
/EM:<"Masken">	Dateien nach Maske ausschließen Sie können mehrere Masken angeben, z. B. EM:"*.txt;*.png; C\Videos*.avi".
/ET:<Anzahl der Sekunden>	Verarbeitung eines Objektes abbrechen, wenn sie länger dauert, als der in Sekunden festgelegte Wert. In der Grundeinstellung ist die Untersuchungsdauer nicht beschränkt.
/ES:<Größe>	Zusammengesetzte Objekte, deren Größe den in MB festgelegten Wert überschreitet, von Untersuchung ausschließen. Kaspersky Security 10.1 für Windows Server untersucht standardmäßig alle Objektgrößen.

Schlüssel	Beschreibung
/TZOFF	Ausnahmen der vertrauenswürdigen Zone verschieben.
Erweiterte Einstellungen (Options)	
/NOICHECKER	iChecker-Technologie deaktivieren (standardmäßig aktiviert).
/NOISWIFT	iSwift-Technologie deaktivieren (standardmäßig aktiviert).
/ANALYZERLEVEL:<Analysestufe>	Verwendung der heuristischen Analyse aktivieren, Analyseniveau einstellen. Hierzu gehören die folgenden Ebenen der heuristischen Analyse: 1 – oberflächlich; 2 – mittel; 3 – tief Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Security 10.1 für Windows Server die heuristische Analyse nicht.
/ALIAS:<Alias des Aufgabenamens>	Dieser Schlüssel weist einer Aufgabe zur Untersuchung auf Befehl einen temporären Namen zu, mit dem auf die Aufgabe zugegriffen werden kann, während sie ausgeführt wird, z.B. um mit dem Befehl TASK eine Statistik anzuzeigen. Der Alias des Aufgabenamens muss unter den alternativen Namen für die Aufgaben aller Funktionalkomponenten von Kaspersky Security 10.1 für Windows Server einmalig sein. Wenn dieser Schlüssel nicht vorgegeben ist, erhält die Aufgabe den alternativen Name scan_<kavshell_pid> (z.B. scan_1234). In der Konsole für Kaspersky Security 10.1 erhält die Aufgabe den Namen Scan objects (<Datum und Uhrzeit>), z. B. Scan objects 8/16/2007 05:13:14 PM.
Einstellungen für Berichte über Aufgabenausführung (Report settings)	
/W:<Name des Berichts über Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Security 10.1 für Windows Server den Bericht über Aufgabenausführung mit dem durch diesen Schlüssel vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse in der Aufgabe. Im Bericht werden die Ereignisse aufgezeichnet, die durch die Einstellungen für den Bericht über Aufgabenausführung und den Ereignisbericht von Kaspersky Security 10.1 für Windows Server 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 "Berichte über Aufgabenausführung" der Konsole für Kaspersky Security 10.1 angezeigt. Wenn Kaspersky Security 10.1 für Windows Server keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen, es erfolgt aber eine Fehlermeldung.

Schlüssel	Beschreibung
/ANSI	Der Schlüssel erlaubt es, die Ereignisse in den Bericht über Aufgabenausführung in der ANSI-Codierung zu schreiben. Der ANSI Schlüssel wird nicht verwendet, wenn der W Schlüssel nicht angegeben wird. Wenn der ANSI Schlüssel nicht angegeben wird, wird der Bericht über Aufgabenausführung in der ANSI-Codierung geführt.

Aufgabe Untersuchung wichtiger Bereiche starten. KAVSHELL SCANCRITICAL

Verwenden Sie den Befehl `KAVSHELL SCANCRITICAL`, um die Systemaufgabe zur Untersuchung wichtiger Bereiche auf Befehl mit den Einstellungen zu starten, die in der Konsole für Kaspersky Security 10.1 festgelegt wurden.

Syntax des Befehls KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<Dateiname für den Bericht über Aufgabenausführung>]
```

Beispiele für den Befehl KAVSHELL SCANCRITICAL

Um die Aufgabe zur Untersuchung auf Befehl Untersuchung wichtiger Bereiche auszuführen und den Bericht über Aufgabenausführung im aktuellen Ordner in der Datei scancritical.log zu speichern, führen Sie folgenden Befehl aus:

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

Sie können den Speicherort des Berichts über Aufgabenausführung je nach Syntax des Schlüssels /W einstellen (s. Tabelle unten).

Tabelle 45. Syntax des Schlüssels /W des Befehls KAVSHELL SCANCRITICAL

Schlüssel	Beschreibung
/W:<Name des Berichts über Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Security 10.1 für Windows Server den Bericht über Aufgabenausführung mit dem durch diesen Schlüssel vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse in der Aufgabe. Im Bericht werden die Ereignisse aufgezeichnet, die durch die Parameter für den Bericht über Aufgabenausführung und den Ereignisbericht des Programms in der Konsole "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Log-Datei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Log-Datei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Log-Datei im Protokoll überschrieben. Sie können die Log-Datei während der Aufgabenausführung anzeigen. Das Protokoll wird im Knoten **Berichte über Aufgabenausführung** der Konsole für Kaspersky Security 10.1 angezeigt. Wenn Kaspersky Security 10.1 für Windows Server keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen, es erfolgt aber eine Fehlermeldung.

Asynchrone Aufgabenverwaltung. KAVSHELL TASK

Mit dem Befehl `KAVSHELL TASK` können Sie eine bestimmte Aufgabe verwalten: Starten, Anhalten, Fortsetzen und Beenden einer Aufgabe, sowie Anzeigen des aktuelles Status und einer Statistik der Aufgabe. Der Befehl wird asynchron ausgeführt.

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL TASK

```
KAVSHELL TASK [<Alias des Aufgabenamens> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Beispiele für den Befehl KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

Der Befehl `KAVSHELL TASK` kann sowohl mit einem oder mehreren Schlüsseln als auch ohne Schlüssel ausgeführt werden (s. Tabelle unten).

Tabelle 46. Schlüssel des Befehls KAVSHELL TASK

Schlüssel	Beschreibung
Ohne Schlüssel	Gibt eine Liste aller vorhandenen Serveraufgaben in Kaspersky Security 10.1 für Windows Server zurück. Die Liste enthält die Felder: Alias des Aufgabennamens, Aufgabenkategorie (Systemaufgabe oder benutzerdefinierte Aufgabe) und den aktuellen Aufgabenstatus.
<Alias des Aufgabenamens>	Verwenden Sie anstatt des Aufgabennamens im Befehl SCAN TASK einen alternativen Namen (Task alias). Dies ist ein zusätzlicher Kurzname, den Kaspersky Security 10.1 für Windows Server an Aufgaben vergibt. Um die alternativen Namen der Aufgaben von Kaspersky Security 10.1 für Windows Server anzuzeigen, führen Sie den Befehl KAVSHELL TASK ohne einen Schlüssel aus.
/START	Die angegebene Aufgabe im asynchronen Modus starten.
/STOP	Beenden einer angegebenen Aufgabe.
/PAUSE	Anhalten einer angegebenen Aufgabe.
/RESUME	Asynchrones Fortsetzen einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (zum Beispiel, **Läuft**, **Abgeschlossen**, **Angehalten**, **Beendet**, **Fehlgeschlagen**, **Wird gestartet**, **Wird wiederhergestellt**)

Schlüssel	Beschreibung
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet wurden.

Rückgabecodes für den Befehl KAVSHELL TASK (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TASK" auf Seite 316).

Echtzeitschutz-Aufgaben starten und beenden. KAVSHELL RTP

Mit dem Befehl `KAVSHELL RTP` können Sie alle Aufgaben des Echtzeitschutzes starten oder beenden.

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Beispiele für den Befehl KAVSHELL RTP

Um alle Aufgaben zum Echtzeitschutz zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL RTP /START
```

Der Befehl `KAVSHELL RTP` kann einen beliebigen der beiden obligatorischen Schlüssel enthalten (s. Tabelle unten).

Tabelle 47. Schlüssel des Befehls KAVSHELL RTP

Schlüssel	Beschreibung
/START	Startet alle Echtzeitschutz-Aufgaben: Echtzeitschutz für Dateien, Skript-Untersuchung und Verwendung von KSN.
/STOP	Beenden aller Echtzeitschutz-Aufgaben.

Verwaltung der Aufgabe Kontrolle des Programmstarts. KAVSHELL APPCONTROL /CONFIG

Mithilfe des Befehls `KAVSHELL APPCONTROL/CONFIG` können Sie den Ausführungsmodus der Aufgabe Kontrolle des Programmstarts anpassen und den Upload von DLL-Modulen überwachen.

Syntax des Befehls KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<vollständiger Pfad zur xml-Datei>
```

Beispiele für den Befehl KAVSHELL APPCONTROL /CONFIG

► *Um die Aufgabe zur Kontrolle des Programmstarts im Modus **Aktiv** auszuführen, ohne das DLL-Modul zu laden, und die Einstellungen der Aufgabe nach Abschluss zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Sie können die Einstellungen der Aufgabe zur Kontrolle des Programmstarts mithilfe von Schlüsseln anpassen (s. Tabelle unten).

Tabelle 48. Schlüssel des Befehls KAVSHELL APPCONTROL/CONFIG

Schlüssel	Beschreibung
`/mode:<applyrules|statistics>`	Funktionsmodus der Aufgabe zur Kontrolle des Programmstarts. Wählen Sie eine der folgenden Ausführungsmodi für die Aufgabe: • Aktiv – Regeln für die Kontrolle des Programmstarts übernehmen • statistics – Nur Statistik
`/dll:<no|yes>`	Deaktivieren oder Aktivieren von "Upload von DLL-Modulen überwachen".
`/savetofile: <vollständiger Pfad der xml-Datei>`	Festgelegte Regeln in die angegebene Datei im xml-Format exportieren.
`/savetofile: <vollständiger Name der xml-Datei>`	Liste der Regeln in einer Datei speichern.
`/savetofile: <vollständiger Name der xml-Datei> /sdc`	Liste der Regeln für die Kontrolle für Installationspakete in einer Datei speichern.
`/clearsdc`	Alle Regeln für die Kontrolle für Installationspakete aus der Liste löschen.

Automatisches Erstellen von Erlaubnisregeln. KAVSHELL APPCONTROL /GENERATE

Mithilfe des Befehls `KAVSHELL APPCONTROL/GENERATE` können Sie die Listen der Regeln für die Kontrolle des Programmstarts erstellen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL/GENERATE <Ordnerpfad> |/source: <Pfad der Datei mit
der Ordnerliste> [/masks: <edms>] [/runapp] [/rules: <ch|cp|h>] [/strong] [/user:
<Benutzer oder Benutzergruppe>] [/export: <vollständiger Pfad zur xml-Datei>]
[/import: <a|r|m>] [/prefix: <Präfix für die Regelnamen>] [/unique]
```

Beispiele für den Befehl KAVSHELL APPCONTROL/GENERATE

► *Um Regeln für die Dateien aus den angegebenen Ordnern zu erstellen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

► *Um im angegebenen Ordner Regeln für ausführbare Dateien aller verfügbaren Erweiterungen zu erstellen und die erstellten Regeln nach Abschluss der Aufgabe in die angegebene xml-Datei zu speichern, führen Sie den folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /GENERATEc:\folder /masks:edms
/export:c\rules\appctrlrules.xml
```

Je nach der Syntax der Schlüssel können Sie die Einstellungen für das automatische Erstellen der Regeln für die Kontrolle des Programmstarts anpassen (s. Tabelle unten).

Tabelle 49. Schlüssel des Befehls KAVSHELL APPCONTROL/GENERATE

Schlüssel	Beschreibung
Gültigkeitsbereich der Regeln mit dem Status "erlaubt"	
<Ordnerpfad>	Pfad des Ordners, der die ausführbaren Dateien enthält, für die automatisch Erlaubnisregeln erstellt werden sollen.
/source:<Pfad der Datei mit der Ordnerliste>	Pfad der Datei im txt-Format, in der die Liste der Ordner mit den ausführbaren Dateien enthalten ist, für die automatisch Erlaubnisregeln erstellt werden sollen.
/masks: <edms>	Erweiterungen der ausführbaren Dateien, für die Erlaubnisregeln für die Kontrolle des Programmstarts erstellt werden sollen. Sie können Dateien mit den folgenden Erweiterungen zum Verarbeitungsbereich der zu erstellenden Regeln einschließen: • e – Dateien mit der Erweiterung exe • d – Dateien mit der Erweiterung dll • m – Dateien mit der Erweiterung msi • s – Skripte
/runapp	Bei der Erstellung von Erlaubnisregeln Programme berücksichtigen, die zum Zeitpunkt der Ausführung der Aufgabe auf dem geschützten Server gestartet sind.

Schlüssel	Beschreibung
Verhalten bei der automatischen Erstellung von Erlaubnisregeln	
/rules: <ch|cp|h>	Aktionen angeben, die von der Aufgabe während der Erstellung der Erlaubnisregeln für die Kontrolle des Programmstarts ausgeführt werden: • ch – digitales Zertifikat verwenden. Wenn das Zertifikat fehlt, SHA256-Hash verwenden. • cp – digitales Zertifikat verwenden. Wenn das Zertifikat fehlt, den Wert des Pfades der ausführbaren Datei verwenden. • h – SHA256-Hash verwenden.
/strong	Bei der automatischen Erstellung der Erlaubnisregeln für die Kontrolle des Programmstarts Header und Fingerabdruck des digitalen Zertifikats verwenden. Der Befehl wird ausgeführt, wenn für den Schlüssel /rules folgender Wert angegeben wird: <ch|cp|>.
/user: <Benutzer oder Benutzergruppe>	Benutzername oder Name der Benutzergruppe, für die die Regeln angewendet werden sollen. Das Programm kontrolliert den Start von Programmen durch den angegebenen Benutzer und/oder die angegebene Benutzergruppe.
Verhalten nach Abschluss der automatischen Erstellung von Erlaubnisregeln	
/export: <vollständiger Pfad der xml-Datei>	Erstellte Regeln in einer xml-Datei speichern.
/unique	Informationen über den Server hinzufügen, für dessen Programme die Erlaubnisregeln für die Kontrolle des Programmstarts erstellt werden.
\prefix: <Präfix für die Regelnamen>	Präfix für den Namen der erstellten Erlaubnisregeln für die Kontrolle des Programmstarts.
/import: <a|r|m>	Erstellte Regeln in die Liste der festgelegten Regeln für die Kontrolle des Programmstarts entsprechend dem angegebenen Ergänzungsprinzip für neue Regeln importieren. : • a – **Zu den bestehenden Regeln hinzufügen** (identische Regeln werden verdoppelt) • r – **Bestehende Regeln ersetzen** (bestehende Regeln werden durch neue Regeln ersetzt) • m – **Mit bestehenden Regeln zusammenführen** (neue Regeln, deren Einstellungen nicht mit den Einstellungen schon bestehender Regeln übereinstimmen, werden hinzugefügt)

Ergänzen der Regelliste für die Kontrolle des Programmstarts. KAVSHELL APPCONTROL

Mithilfe des Befehls `KAVSHELL APPCONTROL` können Sie entsprechend dem ausgewählten Prinzip Regeln aus einer xml-Datei zur Regelliste der Aufgabe zur Kontrolle des Programmstarts hinzufügen sowie alle festgelegten Regeln aus der Liste löschen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <vollständiger Pfad zur xml-Datei> | /replace <vollständiger Pfad zur xml-Datei> | /merge <vollständiger Pfad zur xml-Datei> | /clear
```

Beispiel für den Befehl KAVSHELL APPCONTROL

► *Um Regeln aus einer xml-Datei nach dem Prinzip "Zu den bestehenden Regeln hinzufügen" zu den festgelegten Regeln für die Kontrolle des Programmstarts hinzuzufügen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Je nach Syntax der Schlüssel können Sie das Prinzip für das Hinzufügen neuer Regeln aus der angegebenen xml-Datei zur Liste der festgelegten Regeln für die Aufgabe Kontrolle des Programmstarts wählen (s. Tabelle unten).

Tabelle 50. Schlüssel des Befehls `KAVSHELL APPCONTROL`.

Schlüssel	Beschreibung
/append <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts durch Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Zu den bestehenden Regeln hinzufügen** (Regeln mit identischen Einstellungen werden verdoppelt).
/replace <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts durch Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Bestehende Regeln ersetzen** (Regeln mit identischen Einstellungen werden nicht hinzugefügt, die Regel wird hinzugefügt, wenn zumindest eine Regeleinstellung eindeutig ist).
/merge <vollständiger Pfad der xml-Datei>	Liste der Regeln für die Kontrolle des Programmstarts durch Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen: **Mit bestehenden Regeln zusammenführen** (neue Regeln werden nicht dupliziert, wenn identische Regeln bereits vorhanden sind).
/clear	Liste der Regeln für die Kontrolle des Programmstarts leeren

Liste der Regeln zur Gerätekontrolle aus einer Datei ergänzen. KAVSHELL DEVCONTROL

Mithilfe des Befehls `KAVSHELL DEVCONTROL` können Sie entsprechend dem ausgewählten Prinzip Regeln aus einer xml-Datei zur Regelliste der Aufgabe zur Gerätekontrolle hinzufügen sowie alle festgelegten Regeln aus der Liste löschen.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <vollständiger Pfad zur xml-Datei> | /replace <vollständiger Pfad zur xml-Datei> | /merge <vollständiger Pfad zur xml-Datei> | /clear
```

Beispiel für den Befehl KAVSHELL DEVCONTROL

► *Um Regeln aus einer xml-Datei nach dem Prinzip **Zu den bestehenden Regeln hinzufügen** zu den festgelegten Regeln zur Gerätekontrolle hinzuzufügen, führen Sie den folgenden Befehl aus:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Je nach Syntax der Schlüssel können Sie das Prinzip für das Hinzufügen neuer Regeln aus der angegebenen xml-Datei zur Liste der festgelegten Regeln für die Aufgabe zur Gerätekontrolle wählen (s. Tabelle unten).

Tabelle 51. Schlüssel des Befehls `KAVSHELL DEVCONTROL`

Schlüssel	Beschreibung
/append <vollständiger Pfad der xml-Datei>	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Zu den bestehenden Regeln hinzufügen** (Regeln mit identischen Einstellungen werden verdoppelt).
/replace <vollständiger Pfad der xml-Datei>	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen – **Bestehende Regeln ersetzen** (Regeln mit identischen Einstellungen werden nicht hinzugefügt, die Regel wird hinzugefügt, wenn zumindest eine Regeleinstellung eindeutig ist).
/merge <vollständiger Pfad der xml-Datei>	Liste der Regeln zur Gerätekontrolle mit Regeln aus der angegebenen xml-Datei ergänzen. Prinzip für das Hinzufügen: **Mit bestehenden Regeln zusammenführen** (neue Regeln werden nicht dupliziert, wenn identische Regeln bereits vorhanden sind).
/clear	Liste der Regeln zur Gerätekontrolle leeren.

Aufgabe zum Update der Programm-Datenbanken von Kaspersky Security 10.1 für Windows Server starten. KAVSHELL UPDATE

Mit dem Befehl `KAVSHELL UPDATE` können Sie die Aufgabe zum Datenbanken-Update von Kaspersky Security

10.1 für Windows Server im Synchronmodus starten.

Die Aufgabe zum Datenbanken-Update von Kaspersky Security 10.1 für Windows Server, die mit dem Befehl `KAVSHELL UPDATE` gestartet wird, ist temporär. Sie wird nur während ihrer Ausführung in der Konsole für Kaspersky Security 10.1 angezeigt. Der Bericht über Aufgabenausführung wird gleichzeitig erzeugt. Es wird in den **Berichten über Aufgabenausführung** der Konsole für Kaspersky Security 10.1 angezeigt. Für Update-Aufgaben, die mit dem Befehl `KAVSHELL UPDATE` erstellt und gestartet wurden, sowie für Update-Aufgabe, die in der Konsole für Kaspersky Security 10.1 angelegt wurden, können die Richtlinien der Anwendung Kaspersky Security Center übernommen werden. Informationen darüber, wie Kaspersky Security 10.1 für Windows Server auf Computer mithilfe der Anwendung Kaspersky Security Center verwaltet wird, finden Sie im Abschnitt "Verwaltung von Kaspersky Security 10.1 für Windows Server mithilfe von Kaspersky Security Center".

Wenn Sie in dieser Aufgabe den Pfad eine Update-Quelle angeben, können Sie Umgebungsvariable verwenden. Wenn Sie eine Umgebungsvariable verwenden, die einem Benutzer zugeordnet ist, führen Sie den Befehl `KAVSHELL UPDATE` mit den Rechten dieses Benutzers aus.

Syntax des Befehls KAVSHELL UPDATE

```
KAVSHELL UPDATE < Update-Quelle | /AK | /KL> [/NOUSEKL] [/PROXY:<Adresse>:<Port>]
[/AUTHTYPE:<0-2>] [/PROXYUSER:<Benutzername>] [/PROXYPWD:<Kennwort>]
[/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/USEPROXYFORLOCAL] [/NOFTPPASSIVE]
[/TIMEOUT:<Sekunden>] [/REG:<Code iso3166>] [/W:<Name des Berichts über
Aufgabenausführung>] [/ALIAS:<Alias des Aufgabennamens>]
```

Der Befehl KAVSHELL UPDATE enthält sowohl obligatorische als auch Reserveschlüssel, deren Verwendung optional ist (s. Tabelle unten).

Beispiele für den Befehl KAVSHELL UPDATE

► *Um eine benutzerdefinierte Aufgabe zum Datenbanken-Update zu starten, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE
```

► *Um eine Aufgabe zum Datenbanken-Update zu starten, dessen Updatedateien im Netzwerkordner \\server\bases gespeichert sind, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE \\server\bases
```

► *Um eine Aufgabe zum Update vom FTP-Server ftp://dnl-ru1.kaspersky-labs.com/ zu starten und alle Ereignisse der Aufgabe in die Log-Datei c:\update_report.log zu schreiben, führen Sie folgenden Befehl aus:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

► *Um die Datenbanken-Updates von Kaspersky Security 10.1 für Windows Server vom Update-Server von Kaspersky Lab zu erhalten und die Verbindung mit der Update-Quelle über einen Proxyserver herzustellen (Proxyserver-Adresse: proxy.company.com, Port: 8080) sowie zur Verwendung der integrierten Authentizitätsprüfung von Microsoft Windows (NTLM-authentication) für den Serverzugriff führen Sie unter dem Benutzerkonto (Benutzername: inetuser, Kennwort: 123456) folgenden Befehl aus:*

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

Tabelle 52. Schlüssel des Befehls KAVSHELL UPDATE

Schlüssel	Beschreibung
Update-Quelle (obligatorischer Schlüssel). Geben Sie eine oder mehrere Quellen an. Kaspersky Security 10.1 für Windows Server 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 Server.
/AK	Kaspersky Security Center-Administrationsserver als Update-Quelle
/KL	Update-Server von Kaspersky Lab als Update-Quelle
/NOUSEKL	Die Kaspersky-Lab-Update-Server nicht verwenden, wenn die anderen angegebenen Update-Quellen nicht verfügbar sind (Quellen, die standardmäßig verwendet werden).
Proxyserver-Einstellungen	
/PROXY:<Adresse>:<Port>	Netzwerkname oder IP-Adresse des Proxyservers und dessen Port. Wenn dieser Schlüssel nicht angegeben ist, verwendet stellt Kaspersky Security 10.1 für Windows Server automatisch die Einstellungen des Proxyservers fest, der im lokalen Netzwerk verwendet wird.
/AUTHTYPE:<0-2>	Dieser Schlüssel bestimmt die Authentifizierungsmethode für den Zugriff auf den Proxyserver. Folgende Werte sind möglich: **0** – integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Security 10.1 für Windows Server greift unter dem Benutzerkonto **Lokales System** (**SYSTEM**) auf den Proxyserver zu; **1** – integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Security 10.1 für Windows Server greift unter dem Benutzerkonto, dessen Login-Daten durch die Schlüssel /PROXYUSER und /PROXYPWD angegeben werden, auf den Proxyserver zu; **2** – Authentifizierung mit Benutzername und Kennwort, die durch die Schlüssel /PROXYUSER und /PROXYPWD (basic authentication) angegeben werden. Wenn für den Zugriff auf den Proxyserver keine Authentifizierung erforderlich ist, muss dieser Schlüssel nicht angegeben werden.

Schlüssel	Beschreibung
/PROXYUSER:<Benutzername>	Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn Sie den Schlüsselwert /AUTHTYPE:0 angeben, werden die Schlüssel /PROXYUSER:<Benutzername> und /PROXYPWD:< Kennwort > ignoriert.
/PROXYPWD:<Kennwort>	Benutzerkennwort, das für den Zugriff auf den Proxyserver verwendet werden soll. Wenn Sie den Schlüsselwert /AUTHTYPE:0 angeben, werden die Schlüssel /PROXYUSER:<Benutzername> und /PROXYPWD:< Kennwort > ignoriert. Wenn Sie den Schlüssel /PROXYUSER angeben und den Schlüssel /PROXYPWD auslassen, wird das Kennwort als leer betrachtet.
/NOPROXYFORKL	Proxyserver-Einstellungen für die Verbindung zu den Kaspersky-Lab-Update-Servern nicht verwenden (Sie werden standardmäßig verwendet)
/USEPROXYFORCUSTOM	Proxyserver-Parameter für die Verbindung zu benutzerdefinierten Update-Quellen verwenden (Sie werden standardmäßig nicht verwendet).
/USEPROXYFORLOCAL	Proxyserver-Parameter für die Verbindung zu lokalen Update-Quellen verwenden. Wenn kein Wert angegeben wurde, wird der Wert **Für lokale Adressen keinen Proxyserver verwenden** verwendet.
Allgemeine Parameter eines FTP- und HTTP-Servers	
/NOFTPPASSIVE	Wenn dieser Schlüssel angegeben ist, verwendet Kaspersky Security 10.1 für Windows Server den FTP-Server im aktiven Modus für eine Verbindung zum geschützten Server. Wenn dieser Schlüssel nicht angegeben ist, verwendet Kaspersky Security 10.1 für Windows Server nach Möglichkeit den passiven Modus des FTP-Servers.
/TIMEOUT:<Anzahl der Sekunden>	Wartezeit für Verbindung mit einem FTP- oder HTTP-Server. Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Security 10.1 für Windows Server den voreingestellten Standardwert 10 s. Als Wert für diesen Schlüssel können nur ganze Zahlen eingegeben werden.
/REG:<Code iso3166>	Regionale Einstellungen. Dieser Schlüssel wird beim Update-Download von den Update-Servern von Kaspersky Lab verwendet. Kaspersky Security 10.1 für Windows Server optimiert den Update-Download auf den geschützten Server, indem der geografisch am nächsten liegenden Update-Server ausgewählt wird. Geben Sie als Schlüsselwert den Buchstabencode des Landes an, in dem sich der geschützte Server befindet. Beachten Sie dabei ISO-Standard 3166-1 (z.B. /REG:gr oder /REG:RU). Wenn dieser Schlüssel nicht angegeben oder ein nicht existierender Landescode angegeben wird, erkennt Kaspersky Security 10.1 für Windows Server den Ort des geschützten Computers anhand der regionalen Einstellungen des Servers, auf dem die Konsole für Kaspersky Security 10.1 installiert ist.

Schlüssel	Beschreibung
/ALIAS:<Alias des Aufgabenamens>	Dieser Schlüssel weist der Aufgabe einen temporären Namen zu, mit dem darauf zugegriffen werden kann, während sie ausgeführt wird. Mit dem Befehl TASK können Sie beispielsweise eine Aufgabenstatistik anzeigen lassen. Der Alias des Aufgabenamens muss unter den alternativen Namen für die Aufgaben aller Funktionalkomponenten von Kaspersky Security 10.1 für Windows Server einmalig sein. Wenn dieser Schlüssel nicht angegeben wird, erhält die Aufgabe den Alias update_<kavshell_pid> (z.B. update_1234) In der Konsole für Kaspersky Security 10.1 erhält die Aufgabe den Namen Update-databases (<Datum und Uhrzeit>) (z. B. Update-databases 8/16/2007 5:41:02 PM).
/W:<Name des Berichts über Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Security 10.1 für Windows Server den Bericht über Aufgabenausführung mit dem durch diesen Schlüssel vorgegebenen Namen. Die Log-Datei enthält eine Statistik über die Aufgabenausführung, Zeitpunkt, zu dem die Aufgabe gestartet und beendet wurde, und Informationen über Ereignisse in der Aufgabe. Im Bericht werden die Ereignisse aufgezeichnet, die durch die Einstellungen für den Bericht über Aufgabenausführung und den Ereignisbericht von Kaspersky Security 10.1 für Windows Server 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 **Berichte über Aufgabenausführung** der Konsole für Kaspersky Security 10.1 angezeigt. Wenn Kaspersky Security 10.1 für Windows Server keine Log-Datei anlegen kann, wird die Befehlsausführung nicht abgebrochen oder es erfolgt aber eine Fehlermeldung.

Rückgabecodes für den Befehl KAVSHELL UPDATE (auf Seite 317).

Rollback von Datenbanken-Updates von Kaspersky Security 10.1 für Windows Server. KAVSHELL ROLLBACK

Mit dem Befehl `KAVSHELL ROLLBACK` können Sie die Systemaufgabe Rollback des Datenbank-Updates von Kaspersky Security 10.1 für Windows Server ausführen. Dadurch werden die Datenbanken von Kaspersky Security 10.1 für Windows Server mit den zuvor installierten Updates wieder hergestellt. Der Befehl wird synchron ausgeführt.

Syntax des Befehls

```
KAVSHELL ROLLBACK
```

Rückgabecode für den Befehl KAVSHELL ROLLBACK (auf Seite 318)

Verwalten der Protokollanalyse. KAVSHELL TASK LOG-INSPECTOR

Der Befehl `KAVSHELL TASK LOG-INSPECTOR` kann verwendet werden, um die Integrität der Umgebung auf der Grundlage der Windows-Ereignisprotokollanalyse zu überwachen.

Syntax des Befehls

```
KAVSHELL TASK LOG-INSPECTOR
```

Befehlsbeispiele

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Tabelle 53. KAVSHELL TASK LOG-INSPECTOR zum Ändern des Befehls

Schlüssel	Beschreibung
/START	Die angegebene Aufgabe im asynchronen Modus starten.
/STOP	Beenden einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (zum Beispiel, **Läuft**, **Abgeschlossen**, **Angehalten**, **Beendet**, **Fehlgeschlagen**, **Wird gestartet**, **Wird wiederhergestellt**)
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet wurden.

Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR" auf Seite 316).

Programm aktivieren. KAVSHELL LICENSE

Mit dem Befehl `KAVSHELL LICENSE` können Sie in Kaspersky Security 10.1 für Windows Server Schlüssel und Aktivierungscodes verwalten.

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<Schlüsseldatei | Aktivierungscode> [/R] |
/DEL:<Schlüsselnummer | Nummer des Aktivierungscodes>]
```

Beispiele für den Befehl KAVSHELL LICENSE

► *Führen Sie zur Programmaktivierung den folgenden Befehl aus:*

```
KAVSHELL.EXE LICENSE / ADD: <Aktivierungscode oder Nummer des Schlüssels>
```

► *Um Informationen über die hinzugefügten Schlüssel zu erhalten, führen Sie folgenden Befehl aus:*

```
KAVSHELL LICENSE
```

► *Um einen hinzugefügten Schlüssel mit der Nummer 0000-000000-00000001 zu entfernen, führen Sie folgenden Befehl aus:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

Der Befehl `KAVSHELL LICENSE` kann sowohl mit als auch ohne Schlüssel ausgeführt werden (s. Tabelle unten).

Tabelle 54. Schlüssel des Befehls KAVSHELL LICENSE

Schlüssel	Beschreibung
Ohne Schlüssel	Der Befehl gibt folgende Informationen über die hinzugefügten Schlüssel zurück: • Nummer des Schlüssels. • Lizenztyp (kommerziell oder Probe) • Gültigkeitsdauer der Lizenz, die zum Schlüssel gehört. • Status des Schlüssels (aktiv oder Reserve) Wenn der Wert * angegeben ist, wurde der Schlüssel als Reserveschlüssel hinzugefügt.
/ADD:<Name der Schlüsseldatei oder Aktivierungscode>	Fügt den Schlüssel mithilfe der angegebenen Datei oder des Aktivierungscodes hinzu. Wenn Sie den Pfad einer Schlüsseldatei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable sind dagegen nicht zugelassen.
/R	Der Aktivierungscode oder der Schlüssel /R ergänzt den Aktivierungscode oder Schlüssel /ADD und weist darauf hin, dass der Aktivierungscode bzw. Schlüssel als Reserve hinzugefügt wird.
/DEL:<Schlüsselnummer oder Aktivierungscode>	Löscht den Schlüssel mit der angegebenen Nummer oder den angegebenen Aktivierungscode.

Rückgabecodes für den Befehl KAVSHELL LICENSE (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL LICENSE" auf Seite 318).

Erstellung eines Protokolls zur Ablaufverfolgung aktivieren, anpassen und deaktivieren. KAVSHELL TRACE

Mit dem Befehl `KAVSHELL TRACE` können Sie das Anlegen eines Ablaufverfolgungsberichts für alle Subsysteme von Kaspersky Security 10.1 für Windows Server aktivieren oder deaktivieren, und die entsprechende Protokollierungsstufe festlegen.

Die Informationen in der Dump-Datei des Speichers und in den Protokolldateien werden von Kaspersky Security 10.1 für Windows Server unverschlüsselt aufgezeichnet.

Syntax des Befehls KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<Ordner mit Dateien des Ablaufverfolgungsprotokolls>
[/S:<maximale Größe einer Log-Datei in MB>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Wenn ein Protokoll zur Ablaufverfolgung geführt wird und Sie seine Parameter ändern möchten, geben Sie den Befehl `KAVSHELL TRACE` mit dem Schlüssel /ON ein und geben Sie die Parameter für den Bericht mit

den Schlüsselwerten /S und /LVL an (s. Tabelle unten).

Tabelle 55. Schlüssel des Befehls KAVSHELL TRACE

Schlüssel	Beschreibung
/ON	Führen eines Protokolls zur Ablaufverfolgung aktivieren
/F:<Ordner für Log-Dateien des Ablaufverfolgungsprotokolls>	Dieser Schlüssel gibt den vollständigen Pfad des Ordners an, in dem die Log-Dateien des Ablaufverfolgungsprotokolls gespeichert werden (obligatorischer Schlüssel). Wenn Sie den Pfad eines nicht vorhandenen Ordners angeben, wird kein Protokoll zur Ablaufverfolgung erstellt. Sie können Netzwerkpfade im UNC-Format (Universal Naming Convention) angeben. Pfade von Ordnern auf Netzlaufwerken des geschützten Servers sind nicht zulässig. Wenn der Name eines Ordners, dessen Pfad Sie als Schlüsselwert angeben, ein Leerzeichen enthält, schreiben Sie den Pfad in Anführungszeichen (z. B. /F:"C\Trace Folder"). Wenn Sie den Pfad von Log-Dateien des 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 Security 10.1 für Windows Server, die Daten in eine neue Datei zu schreiben. Die bisherige Berichtsdatei wird gespeichert. Wenn Sie diesen Schlüssel nicht angeben, beträgt die maximale Größe für eine Log-Datei 50 MB.
/LVL:debug|info|warning|error|critical	Dieser Schlüssel legt die Genauigkeitsstufe des Protokolls fest. Auf der maximalen Stufe (**Debug-Informationen**) werden alle Ereignisse protokolliert, auf der minimalen Stufe (**Kritische Ereignisse**) nur kritische Ereignisse. Wenn dieser Schlüssel nicht angegeben ist, werden Ereignisse mit der Genauigkeitsstufe **Debug-Informationen** im Protokoll zur Ablaufverfolgung aufgezeichnet.
/OFF	Dieser Schlüssel deaktiviert das Führen des Protokolls zur Ablaufverfolgung.

Beispiele für den Befehl KAVSHELL TRACE

► *Um das Anlegen eines Protokolls zur Ablaufverfolgung mit der Genauigkeitsstufe **Debug-Informationen** und einer maximalen Größe der Log-Datei von 200 MB zu aktiveren und die Log-Datei im Ordner C:\Trace Folder zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Um das Anlegen eines Protokolls zur Ablaufverfolgung mit der Genauigkeitsstufe **Wichtige Ereignisse** zu aktiveren und die Log-Datei im Ordner C:\Trace Folder zu speichern, führen Sie*

folgenden Befehl aus:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Um die Erstellung eines Protokolls zur Ablaufverfolgung zu aktivieren, führen Sie folgenden Befehl aus:*

```
KAVSHELL TRACE /OFF
```

Rückgabecodes für den Befehl KAVSHELL TRACE (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL TRACE" auf Seite 318).

Log-Dateien für Kaspersky Security 10.1 für Windows Server defragmentieren. KAVSHELL VACUUM

Mithilfe des Befehls `KAVSHELL VACUUM` können Sie Log-Dateien für Ereignisse des Programms defragmentieren. Damit können Fehler bei der Ausführung des Systems bzw. von Kaspersky Security 10.1 für Windows Server verhindert werden, die entstehen, wenn Sie Berichte dauerhaft speichern.

Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Es wird empfohlen, den Befehl `KAVSHELL VACUUM` für die Optimierung der Speicherung von Berichtsdateien bei häufigen Starts der Aufgaben zur Untersuchung auf Befehl oder der Update-Aufgabe zu verwenden.
Bei der Ausführung des Befehls erneuert Kaspersky Security 10.1 für Windows Server die logische Struktur der Log-Dateien des Programms, die auf dem geschützten Server im angegebenen Pfad gespeichert sind.

Standardmäßig werden die Log-Dateien der Ereignisse bei der Ausführung des Programms im Pfad C:\ProgramData\Kaspersky Lab\Kaspersky Security 10.1 für Windows Server\10.1\Reports gespeichert. Wenn Sie manuell einen anderen Pfad angegeben haben, an dem Sie Berichte speichern, defragmentiert der Befehl `KAVSHELL VACUUM` die Dateien im Ordner, der in den Einstellungen der Berichte von Kaspersky Security 10.1 für Windows Server angegeben ist.

Eine große Anzahl von zu defragmentierenden Log-Dateien für Ereignisse verlängert die Zeit für die Ausführung des Befehls `KAVSHELL VACUUM`.

Während der Ausführung des Befehls `KAVSHELL VACUUM` ist die Ausführung der Aufgaben Echtzeitschutz und Server-Kontrolle unmöglich. Der Defragmentierungsvorgang sperrt den Zugang auf die Berichte von Kaspersky Security 10.1 für Windows Server und verbietet ein Protokollieren von Ereignissen. Damit das Schutzniveau des Computers nicht verringert wird, wird empfohlen, die Ausführung des Befehls `KAVSHELL VACUUM` im Voraus zur arbeitsfreien Zeit zu planen.

► *Um eine Defragmentierung der Log-Dateien für Ereignisse bei der Ausführung von Kaspersky*

Security 10.1 für Windows Server durchzuführen, führen Sie den folgenden Befehl aus:

```
KAVSHELL VACUUM
```

Der Befehl kann beim Start mit Berechtigungen des Benutzerkontos des lokalen Administrators ausgeführt werden.

iSwift-Datenbank leeren. KAVSHELL FBRESET

Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server erstellt im Systemverzeichnis %SYSTEMDRIVE%\System Volume Information die Dateien fidbox.dat und fidbox.dat, die Informationen über bereits untersuchte, virenfreie Objekte enthalten. Je größer die Anzahl der Dateien, die von Kaspersky Security 10.1 für Windows Server untersucht worden sind, desto größer ist die Datei fidbox.dat. Diese Datei enthält nur aktuelle Informationen über die tatsächlich im System vorhandenen Dateien: Wenn eine Datei im System gelöscht wird, löscht Kaspersky Security 10.1 für Windows Server die entsprechenden Informationen aus der Datei fidbox.dat.

Um diese Datei zu leeren, verwenden Sie den Befehl `KAVSHELL FBRESET`.

Berücksichtigen Sie folgende Besonderheiten bei der Arbeit mit dem Befehl `KAVSHELL FBRESET`:

- Wenn die Datei fidbox.dat mithilfe des Befehls KAVSHELL FBRESET geleert wird, hält Kaspersky Security 10.1 für Windows Server den Schutz nicht an (im Gegensatz zum manuellen Löschen der Datei fidbox.dat).
- Nachdem die Datei fidbox.dat geleert wurde, kann sich die durch Kaspersky Security 10.1 für Windows Server verursachte Belastung des Servers erhöhen. Dabei untersucht Anti-Virus alle Dateien, auf die nach dem Leeren der Datei fidbox.dat zum ersten Mal zugegriffen wird. Nach der Untersuchung trägt Kaspersky Security 10.1 für Windows Server erneut Informationen über ein untersuchtes Objekt in die Datei fidbox.dat ein. Bei einem erneuten Zugriff auf dieses Objekt erlaubt die iSwift-Technologie es, die Datei nicht erneut zu scannen, falls sie nicht verändert wurde.

Zur Ausführung des Befehls `KAVSHELL FBRESET` muss die Befehlszeile im Benutzerkonto SYSTEM gestartet werden.

Anlegen von Dump-Dateien ein- und ausschalten. KAVSHELL DUMP

Mit dem Befehl `KAVSHELL DUMP` können Sie das Erstellen von Speicherauszügen (Dump-Dateien), die bei Abstürzen für die Prozesse von Kaspersky Security 10.1 für Windows Server erstellt werden, aktivieren oder deaktivieren (siehe folgende Tabelle). Außerdem können Sie jederzeit Speicher-Images der von Kaspersky Security 10.1 für Windows Server ausgeführten Prozesse anfertigen.

Damit die Dump-Datei erfolgreich erstellt werden kann, muss der Befehl `KAVSHELL DUMP` unter dem lokalen Systemkonto (SYSTEM) ausgeführt werden.

Syntax des Befehls KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<Ordner mit Dump-Datei>|/SNAPSHOT /F:<Ordner mit
Dump-Datei> / P:<pid> | /OFF>
```

Beispiele für den Befehl KAVSHELL DUMP

► *Um die Erstellung einer Dump-Datei zu aktivieren und die erstellte Dump-Datei im Ordner C:\Dump Folder zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

► *Um ein Speicherabbild eines Prozesses mit dem Bezeichner 1234 anzufertigen und im Ordner C:/Dumps zu speichern, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

► *Um die Erstellung einer Dump-Datei zu aktivieren, führen Sie folgenden Befehl aus:*

```
KAVSHELL DUMP /OFF
```

Tabelle 56. Schlüssel des Befehls KAVSHELL DUMP

Schlüssel	Beschreibung
/ON	Aktiviert die Erstellung einer Dump-Datei für einen Prozess im Falle seines Absturzes.
/F:<Pfad der Dump-Dateien>	Dieser Schlüssel ist obligatorisch. Er gibt den Pfad des Ordners an, in dem die Dump-Datei gespeichert wird. Wenn Sie den Pfad eines nicht vorhandenen Ordners angeben, wird keine Dump-Datei erstellt. Sie können die Netzwerkpfade im UNC-Format (Universal Naming Convention) verwenden. Pfade von Ordnern auf Netzlaufwerken des geschützten Servers sind nicht zulässig. Wenn Sie einen Pfad für Dump-Dateien angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariable sind dagegen nicht zulässig.
/SNAPSHOT	Fertigt ein Speicher-Image eines bestimmten laufenden Prozesses von Kaspersky Security 10.1 für Windows Server an und speichert die Dump-Datei im Ordner, dessen Pfad durch den Schlüssel /F definiert wird.
/P	Prozess-PID, die im Task-Manager von Microsoft Windows angezeigt wird.
/OFF	Deaktiviert die Erstellung einer Dump-Datei im Falle seines Absturzes.

Rückgabecodes für den Befehl KAVSHELL DUMP (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL DUMP" auf Seite 319).

Einstellungen importieren. KAVSHELL IMPORT

Mit dem Befehl `KAVSHELL IMPORT` können Sie Einstellungen, Funktionen und Aufgaben von Kaspersky Security

10.1 für Windows Server aus einer Konfigurationsdatei in Kaspersky Security 10.1 für Windows Server auf den geschützten Server importieren. Mit dem Befehl `KAVSHELL EXPORT` können Sie eine Konfigurationsdatei erstellen.

> Für die Ausführung dieses Befehls ist evtl. die Eingabe eines Kennworts erforderlich. Für die Eingabe des aktuellen Kennworts verwenden Sie den Schlüssel `[/pwd:<password>]`.

Syntax des Befehls KAVSHELL IMPORT

```
KAVSHELL IMPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiele für den Befehl KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Tabelle 57. Schlüssel des Befehls KAVSHELL IMPORT

Schlüssel	Beschreibung
<Name und Pfad der Konfigurationsdatei>	Name der Konfigurationsdatei, aus der die Parameter importiert werden. Wenn Sie einen Dateipfad angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariablen sind dagegen nicht zugelassen.

Rückgabecodes für den Befehl KAVSHELL IMPORT (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL IMPORT" auf Seite 319).

Einstellungen exportieren. KAVSHELL EXPORT

Mit dem Befehl `KAVSHELL EXPORT` können Sie alle Einstellungen von Kaspersky Security 10.1 für Windows Server und die aktuellen Aufgaben in eine Konfigurationsdatei exportieren, um sie auf anderen Servern in Kaspersky Security 10.1 für Windows Server zu importieren.

Syntax des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiele für den Befehl KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Tabelle 58. Schlüssel des Befehls KAVSHELL EXPORT

Schlüssel	Beschreibung
<Name und Pfad der Konfigurationsdatei>	Name der Konfigurationsdatei, in der die Parameter gespeichert werden. Sie können der Konfigurationsdatei eine beliebige Erweiterung zuweisen. Wenn Sie einen Dateipfad angeben, können Sie die Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariablen sind dagegen nicht zugelassen.

Rückgabecodes für den Befehl KAVSHELL EXPORT (siehe Abschnitt "Rückgabecodes für den Befehl KAVSHELL EXPORT" auf Seite 320).

Integration in MS Operation Management Suite. KAVSHELL OMSINFO

Mithilfe des Befehls KAVSHELL OMSINFO können Sie den Programmstatus sowie Informationen über die von den Antiviren-Datenbanken und dem KSN-Dienst gefundenen Bedrohungen anzeigen. Die Informationen über Bedrohungen werden den verfügbaren Ereignisberichten entnommen.

Syntax des Befehls KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <vollständiger Pfad zur erstellten Datei samt Dateiname>
```

Beispiele für den Befehl KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Tabelle 59. Schlüssel des Befehls KAVSHELL OMSINFO

Schlüssel	Beschreibung
<Pfad zur erstellten Datei samt Dateiname>	Name der erstellten Datei, die Informationen über den Programmstatus und die erkannten Bedrohungen enthalten wird.

Rückgabecodes der Befehlszeile

In diesem Abschnitt

Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP

Tabelle 60. Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist der Dienst von Kaspersky Security 10.1 für Windows Server bereits gestartet oder schon beendet)
-7	Service ist nicht registriert
-8	Der automatische Start des Dienstes ist deaktiviert.
-9	Versuch zum Starten des Dienstes unter einem anderen Benutzerkonto war erfolglos (in der Grundeinstellung arbeitet der Dienst von Kaspersky Security 10.1 für Windows Server unter dem Systemkonto).
-99	Unbekannter Fehler

Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL

Tabelle 61. Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL

Feedback-Code	Beschreibung
0	Vorgang erfolgreich ausgeführt (Es wurden keine Bedrohungen gefunden)
1	Vorgang abgebrochen
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (Datei mit Liste der Untersuchungsbereiche nicht gefunden)
-5	Ungültige Befehlssyntax oder Untersuchungsbereich nicht festgelegt
-80	Infizierte und andere gefundene Objekte
-81	Möglicherweise infizierte Objekte
-82	Es wurden Verarbeitungsfehler erkannt.
-83	Es wurden nicht untersuchte Objekte gefunden.
-84	Es wurden beschädigte Objekte gefunden.
-85	Das Erstellen eines Berichts über Aufgabenausführung ist fehlgeschlagen.
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL TASK LOG-INSPECTOR

Tabelle 62. Rückgabecode für den Befehl KAVSHELL TASK LOG-INSPECTOR

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-6	Ungültiger Vorgang (zum Beispiel ist der Dienst von Kaspersky Security 10.1 für Windows Server bereits gestartet oder schon beendet)
402	Aufgabe ist schon gestartet (für Schlüssel /STATE)

Rückgabecodes für den Befehl KAVSHELL TASK

Tabelle 63. Rückgabecodes für den Befehl KAVSHELL TASK

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (Aufgabe nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist die Aufgabe nicht gestartet, schon gestartet oder kann nicht angehalten werden)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel
401	Aufgabe nicht gestartet (für Schlüssel /STATE)
402	Aufgabe ist schon gestartet (für Schlüssel /STATE)
403	Aufgabe ist schon angehalten (für Schlüssel /STATE)
-404	Fehler bei Vorgangsausführung (Ändern des Aufgabenstatus führte zum Absturz)

Rückgabecodes für den Befehl KAVSHELL RTP

Tabelle 64. Rückgabecodes für den Befehl KAVSHELL RTP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keine bzw. alle Aufgaben des Echtzeitschutzes nicht gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel Aufgabe ist schon gestartet oder schon beendet)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL UPDATE

Tabelle 65. 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 Security 10.1 für Windows Server hat die Authentifizierungsprüfung beim Verbinden mit der Update-Quelle nicht bestanden.
-236	Die Datenbanken von Kaspersky Embedded Systems Security sind beschädigt.
-301	Ungültiger Schlüssel

Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Tabelle 66. Rückgabecodes für den Befehl KAVSHELL ROLLBACK

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-99	Unbekannter Fehler
-221	Backup-Kopie der Datenbanken nicht gefunden
-222	Backup-Kopie der Datenbanken ist beschädigt

Rückgabecodes für den Befehl KAVSHELL LICENSE

Tabelle 67. Rückgabecodes für den Befehl KAVSHELL LICENSE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Unzureichende Rechte für die Schlüsselverwaltung
-4	Kein Schüssel mit der angegebenen Nummer gefunden
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Schlüssel nicht hinzugefügt)
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel
-303	Die Lizenz erstreckt sich auf ein anderes Programm

Rückgabecodes für den Befehl KAVSHELL TRACE

Tabelle 68. Rückgabecodes für den Befehl KAVSHELL TRACE

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keinen Pfad gefunden, der als Pfad zum Ordner mit den Log-Dateien für den Ablaufverfolgungsbericht führt)

Feedback-Code	Beschreibung
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch, den Befehl KAVSHELL TRACE/OFF auszuführen, wenn Erstellen des Protokolls zur Ablaufverfolgung schon deaktiviert ist)
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL FBRESET

Tabelle 69. Rückgabecodes für den Befehl KAVSHELL FBRESET

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL DUMP

Tabelle 70. Rückgabecodes für den Befehl KAVSHELL DUMP

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (keinen Pfad gefunden, der als Pfad zum Ordner mit der Dump-Datei führt; keinen Prozess mit PID gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch, den Befehl KAVSHELL DUMP /OFF auszuführen, wenn Erstellen der Dump-Datei deaktiviert ist)
-99	Unbekannter Fehler

Rückgabecodes für den Befehl KAVSHELL IMPORT

Tabelle 71. Rückgabecodes für den Befehl KAVSHELL IMPORT

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (zu importierende Konfigurationsdatei nicht gefunden)

Feedback-Code	Beschreibung
-5	Ungültige Syntax
-99	Unbekannter Fehler
501	Der Vorgang wurde erfolgreich ausgeführt. Bei der Befehlsausführung ist jedoch ein Fehler bzw. Kommentar aufgetreten (z. B. Kaspersky Security 10.1 für Windows Server hat die Einstellungen einer bestimmten funktionellen Komponente nicht importiert).
-502	Zu importierende Datei ist nicht vorhanden oder hat ein unbekanntes Format
-503	Inkompatible Einstellungen (Konfigurationsdatei aus einem anderen Programm oder einer höheren oder inkompatiblen Version von Kaspersky Security 10.1 für Windows Server exportiert)

Rückgabecodes für den Befehl KAVSHELL EXPORT

Tabelle 72. Rückgabecodes für den Befehl KAVSHELL EXPORT

Feedback-Code	Beschreibung
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-5	Ungültige Syntax
-10	Konfigurationsdatei konnte nicht erstellt werden (beispielsweise kein Zugang zum Ordner, welcher im Pfad vorgegeben wurde)
-99	Unbekannter Fehler
501	Der Vorgang wurde erfolgreich ausgeführt. Bei der Befehlsausführung ist jedoch ein Fehler bzw. Kommentar aufgetreten (z. B. Kaspersky Security 10.1 für Windows Server hat die Einstellungen einer bestimmten funktionellen Komponente nicht exportiert).

Leistungskontrolle. Indikatoren in Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt informiert über die Indikatoren von Kaspersky Security 10.1 für Windows Server: Leistungsindikatoren für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps.

In diesem Kapitel

Leistungsindikatoren für das Programm Systemmonitor

Dieser Abschnitt enthält Informationen über Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows, die von Kaspersky Security 10.1 für Windows Server während der Installation registriert werden.

In diesem Abschnitt

Über SNMP-Indikatoren in Kaspersky Security 10.1 für Windows Server

Die Komponente **Leistungsindikatoren** gehört zu den standardmäßig installierten Komponenten von Kaspersky Security 10.1 für Windows Server. Während der Installation registriert Kaspersky Security 10.1 für Windows Server seine Leistungsindikatoren für das Programm Systemmonitor von Microsoft Windows.

Mit den Indikatoren von Kaspersky Security 10.1 für Windows Server können Sie die Leistung des Programms bei der Ausführung von Echtzeitschutz-Aufgaben kontrollieren. Sie können Engstellen beim Zusammenwirken mit anderen Anwendungen und bei ungenügenden Ressourcen überwachen. Außerdem können Sie nicht so optimale

Einstellungen von Kaspersky Security 10.1 für Windows Server und Abstürze diagnostizieren.

Sie können die Leistungsindikatoren für Kaspersky Security 10.1 für Windows Server aufrufen, indem Sie die Konsole **Optimierung** im Element **Administration** der Windows-Systemsteuerung öffnen.

Die folgenden Abschnitte erklären die Indikatoren, nennen die empfohlenen Intervalle für das Ablesen der Werte und entsprechende Grenzwerte. Außerdem werden Empfehlungen zur Konfiguration von Kaspersky Security 10.1 für Windows Server bei Grenzwertüberschreitungen gegeben.

Gesamtzahl der abgelehnten Anfragen

Tabelle 73. Gesamtzahl der abgelehnten Anfragen

Name	Gesamtzahl der abgelehnten Anfragen (Total number of requests denied)
Definition	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die nicht von den Programmprozessen angenommen wurden. Es wird ab dem letzten Start von Kaspersky Security 10.1 für Windows Server gezählt. Das Programm überspringt Objekte, deren Verarbeitungsanfragen von aktiven Prozessen durch Kaspersky Security 10.1 für Windows Server zurückgewiesen werden.
Ziel	Ein Indikator kann überwachen: • Qualitätsverluste beim Echtzeitschutz wegen hoher Belastung der Arbeitsprozesse von Kaspersky Security 10.1 für Windows Server • Unterbrechung des Echtzeitschutzes wegen Abweisungen vom File-Interception-Dispatcher
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Summe der abgelehnten Anfragen für die Verarbeitung entspricht der Summe der übersprungenen Objekte Folgende Situationen sind abhängig vom "Verhalten" des Indikators möglich: • Der Indikator zeigt mehrere abgelehnte Anfragen im Laufe einer längeren Zeit: Alle Prozesse von Kaspersky Security 10.1 für Windows Server waren vollständig ausgelastet, deshalb konnte Kaspersky Security 10.1 für Windows Server die Objekte nicht untersuchen. Um das Überspringen von Objekten auszuschließen, erhöhen Sie die Menge an Programmprozessen für Aufgaben des Echtzeitschutzes. Sie können die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** von Kaspersky Security 10.1 für Windows Server verwenden. • Die Summe der abgelehnten Anfragen übersteigt den kritischen Schwellenwert erheblich und steigt schnell an: Der File-Interception-Dispatcher ist ausgefallen. Kaspersky Security 10.1 für Windows Server untersucht Objekte nicht beim Öffnen. Kaspersky Security 10.1 für Windows Server neu starten

Gesamtzahl der übersprungenen Anfragen

Tabelle 74. Gesamtzahl der übersprungenen Anfragen

Name	Gesamtzahl der übersprungenen Anfragen (Total number of requests skipped).
Definition	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server das Objekt und erhöht den Wert des Indikators **Gesamtzahl der übersprungenen Anfragen** um 1.
Ziel	Der Indikator kann einen Produktivitätsverlust wegen ausbleibender Datenströme vom File-Interception-Dispatcher überwachen.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Ein Indikatorwert, der ungleich Null ist, bedeutet, dass ein oder mehrere Datenströme des File-Interception-Dispatchers hängen geblieben sind und stillstehen. Der Indikatorwert entspricht der Anzahl der Datenströme, die zurzeit stillstehen. Wenn das Untersuchungstempo nicht befriedigt, starten Sie Kaspersky Security 10.1 für Windows Server neu, um die angehaltenen Datenströme wiederherzustellen.

Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Tabelle 75. 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 Security 10.1 für Windows Server gezählt. Kaspersky Security 10.1 für Windows Server überspringt Objekte, deren Verarbeitungsanfragen vom File-Interceptor-Treiber zurückgewiesen werden.

Ziel	Der Indikator kann mögliche Qualitätsverluste des Echtzeitschutzes erkennen und beseitigen, die aufgrund nicht genügender Systemressourcen eintreten.
Normalwert / Grenzwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert ungleich Null ist, brauchen die Prozesse von Kaspersky Security 10.1 für Windows Server für die Anfragenbearbeitung einen größeren Arbeitsspeicher. Es ist möglich, dass es andere Prozesse gibt, die den ganzen Arbeitsspeicher in Anspruch nehmen.

Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Tabelle 76. 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 Security 10.1 für Windows Server und Gesamtstufe der Dateiaktivität auf dem Server zu überwachen.
Normalwert / Grenzwert	Der Indikatorwert kann schwanken, je nach Stufe der Dateiaktivität auf dem Server.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Nein

Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

Tabelle 77. Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

Name	Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers (Average number of file interception dispatcher streams).
Definition	Anzahl der Datenströme des File-Interception-Dispatchers in einem Arbeitsprozess. Mittelwert für alle Prozesse, die momentan an Echtzeitschutz-Aufgaben beteiligt sind.
Ziel	Dieser Indikator erlaubt es, mögliche Qualitätsverluste des Echtzeitschutzes zu erkennen und zu beseitigen, die auf vollständige Auslastung der Prozesse von Kaspersky Security 10.1 für Windows Server zurückgehen.
Normalwert / Grenzwert	Variiert / 40.

Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	In jedem aktiven Prozess können bis zu 60 Datenströme des File-Interception-Dispatchers angelegt werden. Wenn sich der Indikatorwert der Zahl 60 nähert, besteht das Risiko, dass kein aktiver Prozess mehr die Verarbeitung einer in der Warteschlange stehenden Anfrage vom File-Interception-Treiber abnimmt und Kaspersky Security 10.1 für Windows Server überspringt das Objekt. Vergrößern Sie die Anzahl der Prozesse von Kaspersky Security 10.1 für Windows Server für die Aufgaben des Echtzeitschutzes. Sie können die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** von Kaspersky Security 10.1 für Windows Server verwenden.

Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Tabelle 78. Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Name	Maximale Anzahl der Datenströme des File-Interception-Dispatchers (Maximum number of file interception dispatcher streams)
Definition	Anzahl der Datenströme des File-Interception-Dispatchers in einem Arbeitsprozess. Höchstwert für alle Prozesse, die momentan an Echtzeitschutz-Aufgaben beteiligt sind.
Ziel	Der Indikator kann einen Produktivitätsverlust wegen ungleichmäßiger Belastungsverteilung in den ausgeführten Arbeitsprozessen erkennen und beseitigen.
Normalwert / Grenzwert	Variiert / 40.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Wert dieses Indikators dauerhaft und erheblich von dem Indikatorwert **Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers** abweicht, verteilt Kaspersky Security 10.1 für Windows Server die Belastung ungleichmäßig auf die ausführenden Prozesse. Kaspersky Security 10.1 für Windows Server neu starten

Anzahl der Elemente in der Warteschlange der infizierten Objekte

Tabelle 79. Anzahl der Elemente in der Warteschlange der infizierten Objekte

Name	Anzahl der Elemente in der Warteschlange der infizierten Objekte (Number of items in the infected object queue)
Definition	Anzahl der infizierten Objekte, die momentan auf die Verarbeitung (Desinfektion oder Löschen) warten.
Ziel	Ein Indikator kann überwachen: • Unterbrechung des Echtzeitschutzes wegen möglichen Abweisungen vom File-Interception-Dispatcher • Überlastung der Prozesse wegen ungleichmäßiger Verteilung der Prozessorzeit zwischen den anderen laufenden Programmen und Kaspersky Security 10.1 für Windows Server • Virenepidemien
Normalwert / Grenzwert	Der Indikatorwert kann von Null abweichen, wenn Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server verarbeitet keine Objekte (möglicherweise aufgrund eines Absturzes des File-Interception-Dispatchers) Kaspersky Security 10.1 für Windows Server neu starten • Es steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Security 10.1 für Windows Server zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Computerbelastung durch andere Anwendungen senken). • Es ist eine Virenepidemie eingetreten. Vom Eintreten einer Virenepidemie zeugt außerdem eine große Menge an gefundenen infizierten oder möglicherweise infizierte Objekten in der Aufgabe Echtzeitschutz für Dateien. Informationen über die Anzahl der gefundenen Objekte können Sie der Aufgabenstatistik oder dem Bericht über Aufgabenausführung entnehmen.

Anzahl der pro Sekunde verarbeiteten Objekte

Tabelle 80. 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 Servers erkannt und beseitigt werden, die wegen der Zuweisung zu geringer Prozessorzeit an die Arbeitsprozesse von Kaspersky Security 10.1 für Windows Server oder wegen Fehler bei der Ausführung von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server und von der Belastung des Servers durch Prozesse anderer Programme ab. Beobachten Sie längere Zeit das mittlere Anzeige-Niveau des Indikators. Wenn das Durchschnittsniveau des Indikators gesunken ist, kann diese auf eine der folgenden Situationen hinweisen: • Den aktiven Prozessen von Kaspersky Security 10.1 für Windows Server steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Security 10.1 für Windows Server zusätzliche Prozessorzeit ein (indem Sie beispielsweise die Serverbelastung durch andere Anwendungen senken). • Kaspersky Security 10.1 für Windows Server ist abgestürzt (mehrere Datenströme stehen still). Kaspersky Security 10.1 für Windows Server neu starten

SNMP-Indikatoren und -Traps in Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält Informationen zu den Indikatoren und Traps in Kaspersky Security 10.1 für Windows Server.

In diesem Abschnitt

Über SNMP-Indikatoren und -Traps in Kaspersky Security 10.1 für Windows Server

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 Security 10.1 für Windows Server mithilfe des SNMP-Protokolls (Simple Network Management Protocol) anzeigen.

Um die Indikatoren und Traps für Kaspersky Security 10.1 für Windows Server am Administrator-Arbeitsplatz anzuzeigen, starten Sie auf dem geschützten Server den SNMP-Dienst und am Administrator-Arbeitsplatz den SNMP-Dienst und den Dienst SNMP-Traps.

SNMP-Indikatoren in Kaspersky Security 10.1 für Windows Server

Dieser Abschnitt enthält eine Tabelle mit einer Beschreibung der Einstellungen der SNMP-Indikatoren von Kaspersky Security 10.1 für Windows Server.

In diesem Abschnitt

Leistungsindikatoren

Tabelle 81. Leistungsindikatoren

Indikatoren	Definition
currentRequestsAmount	Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden (auf Seite 324)

Indikatoren	Definition
currentInfectedQueueLength	Anzahl der Elemente in der Warteschlange für infizierte Objekte (siehe Abschnitt "Anzahl der Elemente in der Warteschlange der infizierten Objekte" auf Seite 326)
currentObjectProcessingRate	Anzahl der pro Sekunde verarbeiteten Objekte (auf Seite 327)
currentWorkProcessesNumber	Aktuelle Anzahl von Arbeitsprozessen, die von Kaspersky Security 10.1 für Windows Server genutzt werden

Indikatoren für Quarantäne

Tabelle 82. Indikatoren für Quarantäne

Indikatoren	Definition
totalObjects	Anzahl der Objekte, die sich momentan im Quarantäne-Ordner befinden.
totalSuspiciousObjects	Anzahl der möglicherweise infizierten Objekte, die sich momentan im Quarantäne-Ordner befinden
currentStorageSize	Volumen der Daten im Quarantäne-Ordner (MB)

Indikatoren für Backup

Tabelle 83. Indikatoren für Backup

Indikatoren	Definition
currentBackupStorageSize	Volumen der Daten im Backup-Ordner (MB)

Allgemeine Indikatoren

Tabelle 84. Allgemeine Indikatoren

Indikatoren	Definition
lastCriticalAreasScanAge	Der seit der letzten vollständigen Untersuchung der wichtigen Serverbereiche vergangene Zeitraum (in Sekunden angegebener Zeitraum seit dem letzten Abschluss der *Aufgabe zur Untersuchung wichtiger Bereiche*)
licenseExpirationDate	Gültigkeitsdauer der Lizenz. Wenn ein aktiver Schlüssel und ein Reserveschlüssel oder ein Aktivierungscode hinzugefügt wurden, wird das Ablaufdatum der Lizenz des Reserveschlüssels oder des Aktivierungscodes angezeigt.
currentApplicationUptime	Ausführungszeit von Kaspersky Security 10.1 für Windows Server seit dem letzten Start, in Hundertstelsekunden

Indikatoren	Definition
currentFileMonitorTaskStatus	Status der Aufgabe Echtzeitschutz für Dateien: **On** – wird ausgeführt; **Off** – wurde beendet oder angehalten.

Update-Indikatoren

Tabelle 85. Update-Indikatoren

Indikatoren	Definition
avBasesAge	"Alter" der Datenbanken (in Hundertstelsekunden angegebener Zeitraum zwischen Veröffentlichungsdatum der zuletzt installierten Datenbanken-Updates und dem gegenwärtigen Zeitpunkt)

Indikatoren für den Echtzeitschutz

Tabelle 86. Indikatoren für den Echtzeitschutz

Indikatoren	Definition
totalObjectsProcessed	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien untersuchten Objekte
totalInfectedObjectsFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen infizierten und anderen Objekte
totalSuspiciousObjectsFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen möglicherweise infizierten Objekte
totalVirusesFound	Anzahl der seit dem letzten Start der Aufgabe Echtzeitschutz für Dateien gefundenen Objekte
totalObjectsQuarantined	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die von Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server 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 Security 10.1 für Windows Server desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotDisinfected	Anzahl der infizierten und anderen Objekte, deren Desinfektion durch Kaspersky Security 10.1 für Windows Server 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 Security 10.1 für Windows Server desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien

Indikatoren	Definition
totalObjectsNotDeleted	Anzahl der infizierten, möglicherweise infizierten oder anderen Objekte, die Kaspersky Security 10.1 für Windows Server erfolglos zu desinfizieren versuchte. Gezählt seit dem letzten Start der zum Aufgabe Echtzeitschutz für Dateien
totalObjectsBackedUp	Anzahl der infizierten oder anderen Objekte, die von Kaspersky Security 10.1 für Windows Server ins Backup verschoben wurden. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien
totalObjectsNotBackedUp	Anzahl der infizierten oder anderen Objekte, die Kaspersky Security 10.1 für Windows Server erfolglos versuchte, ins Backup zu verschieben. Gezählt seit dem letzten Start der Aufgabe zum Echtzeitschutz für Dateien

SNMP-Traps

Die Einstellungen von SNMP-Traps in Kaspersky Security 10.1 für Windows Server sind in nachstehender Tabelle beschrieben.

Tabelle 87. SNMP-Traps in Kaspersky Security 10.1 für Windows Server

Trap	Beschreibung	Einstellungen
eventThreatDetected	Objekt gefunden.	eventDateAndTime eventSeverity computerName UserName objectName threatName detectType detectCertainty
eventBackupStorageSizeExceeds	Die maximale Größe des Backups wurde überschritten. Das Gesamtvolumen der Daten im Backup-Ordner hat den Wert überschritten, der durch die Einstellung **Maximale Größe des Backups (MB)** festgelegt ist. Kaspersky Security 10.1 für Windows Server erstellt weiterhin Backups für infizierte Objekte.	eventDateAndTime eventSeverity eventSource

Trap	Beschreibung	Einstellungen
eventThresholdBackupStorageSizeExceeds	Maximale Größe des Backups ist erreicht. Größe des freien Speicherplatzes im Backup, die in der Einstellung **Grenzwert für verfügbaren Speicherplatz (MB)** eingegeben wurde, ist gleich dem angegebenen Wert oder liegt darunter. Kaspersky Security 10.1 für Windows Server erstellt weiterhin Backups für infizierte Objekte.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Die maximale Größe der Quarantäne wurde überschritten. Das Gesamtvolumen der Daten im Quarantäne-Ordner hat den Wert überschritten, der durch die Einstellung **Maximale Größe der Quarantäne (MB)** festgelegt ist. Kaspersky Security 10.1 für Windows Server verschiebt möglicherweise infizierte Objekte weiterhin in die Quarantäne.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Maximale Größe der Quarantäne ist erreicht. Die Größe des freien Speicherplatzes im Quarantäne-Ordner, die mit der Einstellung **Grenzwert für verfügbaren Speicherplatz (MB)** eingegeben wurde, liegt unter dem angegebenen Wert. Kaspersky Security 10.1 für Windows Server verschiebt möglicherweise infizierte Objekte weiterhin in die Quarantäne.	eventDateAndTime eventSeverity eventSource

Trap	Beschreibung	Einstellungen
eventObjectNotQuarantined	Quarantänefehler.	eventSeverity eventDateAndTime eventSource UserName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Fehler beim Speichern einer Kopie des Objekts im Backup-Speicher.	eventSeverity eventDateAndTime eventSource objectName UserName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Quarantänefehler.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Backup-Fehler.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Antiviren-Datenbanken sind veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Datenbanken-Update zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).	eventSeverity eventDateAndTime eventSource days

Trap	Beschreibung	Einstellungen
eventAVBasesTotallyOutdated	Antiviren-Datenbanken sind stark veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Datenbanken-Update zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).	eventSeverity eventDateAndTime eventSource days
eventApplicationStarted	Kaspersky Security 10.1 für Windows Server läuft	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Security 10.1 für Windows Server wurde beendet.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	Untersuchung wichtiger Bereiche liegt lange zurück. Berechnet als Anzahl der Tage seit dem letzten Abschluss der *Aufgabe zur Untersuchung wichtiger Bereiche*	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Die Lizenz ist abgelaufen!	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	Wenn die Gültigkeitsdauer der Lizenz bald abläuft. Es werden die Tage gezählt, die bis zum Ablauf der Lizenz verbleiben.	eventSeverity eventDateAndTime eventSource days
eventTaskInternalError	Fehler bei Ausgabenausführung.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Fehler bei Ausführung einer Update-Aufgabe.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

In der Tabelle unten werden die Trap-Parameter und die entsprechenden Parameterwerte beschrieben.

Tabelle 88. Parameterwerte von SNMP-Traps

Einstellung	Beschreibung und mögliche Werte
eventDateAndTime	Zeitpunkt, zu dem ein Ereignis eingetreten ist.
eventSeverity	Ereigniskategorie des Ereignisses. Der Parameter nimmt die folgenden Werte an: • critical (1) – kritisch • warning (2) – Warnung • info (3) – informativ
UserName	Benutzername (z.B. des Benutzers, der versucht hat, Zugriff auf eine infizierte Datei zu erhalten).
computerName	Servername (beispielsweise Name des Servers, von dem ein Benutzer versucht hat, Zugriff auf eine infizierte Datei zu bekommen)
eventSource	Ereignisquelle: Funktionalkomponente, bei der ein Ereignis aufgetreten ist. Der Parameter nimmt die folgenden Werte an: • unknown (0) – Die Komponente ist unbekannt • quarantine (1) – Quarantäne • backup (2) – Backup • reporting (3) – Berichte über 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 Security 10.1 für Windows Server als Ganzem zu tun hat • systemAudit (8) – Systemaudit-Bericht
eventReason	Grund für Ereigniseintritt. Der Parameter nimmt die folgenden Werte an: • reasonUnknown(0) – der Grund ist unbekannt • reasonInvalidSettings (1) – nur für Ereignisse des Backups und der Quarantäne; Wird angezeigt, wenn der Quarantäne-Ordner oder der Backup-Ordner nicht verfügbar sind (unzureichende Zugriffsrechte oder Ordner wurde in den Quarantäneparametern falsch angegeben, z.B. ein Netzwerkpfad wurde angegeben). In diesem Fall verwendet Kaspersky Security 10.1 für Windows Server den Standardordner für Backup oder Quarantäne.
objectName	Objektname (beispielsweise Name der Datei, in der eine Bedrohung gefunden wurde).
threatName	Name des gefundenen Objekts gemäß der Klassifizierung der Viren-Enzyklopädie Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Security 10.1 für Windows Server beim Fund eines Objekts zurückgibt. Sie können den vollständigen Namen eines gefundenen Objekts im Bericht über Aufgabenausführung einsehen (siehe Abschnitt "Protokolleinstellungen anpassen" auf Seite 172).

Einstellung	Beschreibung und mögliche Werte
detectType	Typ des gefundenen Objekts. Der Parameter nimmt die folgenden Werte an: • undefined (0) – nicht definiert • virware – klassische Viren und Netzwerkwürmer • trojware – Trojaner • malware – sonstige Schadsoftware • adware – Adware • pornware – pornografische Programme • riskware – legale Programmen, die von Angreifern genutzt werden können, um den Computer oder die Daten zu schädigen
detectCertainty	Gewissheit für Erkennung einer Bedrohung. Der Parameter nimmt die folgenden Werte an: • Suspicion (möglicherweise infiziert) – Kaspersky Security 10.1 für Windows Server hat erkannt, dass ein Codeabschnitt des Objekts teilweise mit einem bekanntem Schadcode übereinstimmt. • Sure (infiziert)– Kaspersky Security 10.1 für Windows Server hat erkannt, dass ein Codeabschnitt des Objekts vollständig mit einem bekanntem Schadcode übereinstimmt.
days	Anzahl von Tagen (z. B. Anzahl der Tage bis zum Ablauf einer Lizenz).
errorCode	Fehlercode.
knowledgeBaseId	Adresse des Artikels in der Wissensdatenbank (beispielsweise Adresse des Artikels, der einen Fehler beschreibt).
taskName	Aufgabenname.
updaterErrorEventReason	Grund, aus dem das Update nicht übernommen wurde. Der Parameter nimmt die folgenden Werte an: • reasonUnknown(0) – der Grund ist unbekannt • reasonAccessDenied – Zugriff verweigert; • reasonUrlsExhausted – Das Ende der Liste mit Update-Quellen wurde erreicht; • reasonInvalidConfig – ungültige Konfigurationsdatei; • reasonInvalidSignature – ungültige Signatur; • reasonCantCreateFolder – Der Ordner kann nicht angelegt werden; • reasonFileOperError – Dateifehler; • reasonDataCorrupted – Das Objekt ist beschädigt; • reasonConnectionReset – Verbindungstrennung; • reasonTimeOut – Zeitüberschreitung bei Verbindung; • reasonProxyAuthError – Fehler bei Authentifizierung auf dem Proxyserver; • reasonServerAuthError – Fehler bei Authentifizierung auf dem Server; • reasonHostNotFound – Der Computer wurde nicht gefunden; • reasonServerBusy – Server nicht verfügbar; • reasonConnectionError – Verbindungsfehler; • reasonModuleNotFound – Das Objekt wurde nicht gefunden; • reasonBlstCheckFailed(16) – Fehler beim Überprüfen der schwarzen Schlüsselliste. Möglicherweise wurde während des Updatevorgangs Datenbanken-Updates veröffentlicht. Wiederholen Sie bitte das Update in einigen Minuten.

Einstellung	Beschreibung und mögliche Werte
storageObjectNotAddedEventReason	Grund für Nichtverschieben eines Objektes in Backup oder Quarantäne. Der Parameter nimmt die folgenden Werte an: • reasonUnknown(0) – der Grund ist unbekannt • reasonStorageInternalError – Datenbankfehler, bitte stellen Sie Kaspersky Security 10.1 für Windows Server wieder her. • reasonStorageReadOnly – Datenbankfehler, bitte stellen Sie Kaspersky Security 10.1 für Windows Server wieder her. • reasonStorageIOError – Ein-/Ausgabefehler: a) Kaspersky Security 10.1 für Windows Server ist beschädigt, bitte stellen Sie Kaspersky Security 10.1 für Windows Server wieder her; b) das Laufwerk mit Kaspersky Security 10.1 für Windows Server ist beschädigt. • reasonStorageCorrupted – der Speicher ist beschädigt, bitte stellen Sie Kaspersky Security 10.1 für Windows Server wieder her. • reasonStorageFull – Die Datenbank ist voll. Bitte geben Sie Speicherplatz auf dem Datenträger frei. • reasonStorageOpenError – Die Datenbankdatei konnte nicht geöffnet werden. Bitte stellen Sie Kaspersky Security 10.1 für Windows Server wieder her. • reasonStorageOSFeatureError – Einige Funktionen des Betriebssystems entsprechen nicht den Anforderungen von Kaspersky Security 10.1 für Windows Server. • 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.

Kontaktaufnahme mit dem Technischen Support

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

In diesem Kapitel

Wie Sie technischen Support erhalten

Wenn Sie in der Dokumentation oder in anderen Informationsquellen zum Programm keine Lösung für Ihr Problem gefunden haben, empfehlen wir Ihnen, den Technischen Support zu kontaktieren. Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms.

Der Technische Support steht nur den Benutzern zur Verfügung, die eine kommerzielle Lizenz für die Programmnutzung gekauft haben. Benutzer, die eine Testlizenz verwenden, können den Technischen Support nicht nutzen.

Bevor Sie sich an unseren Technischen Support wenden, machen Sie sich bitte mit unseren Support-Regeln vertraut.

Eine Kontaktaufnahme mit den Experten des Technischen Supports ist auf folgende Weise möglich:

- Technischen Support anrufen
- Versand einer Anfrage an den Technischen Support von Kaspersky Lab über das Portal Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Technischer Support über Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) ist ein Portal für Unternehmen, die Programme von Kaspersky Lab verwenden. Über das Portal Kaspersky CompanyAccount können Benutzer mit Kaspersky-Lab-Experten mithilfe von Online-Anfragen kommunizieren. Über das Portal Kaspersky CompanyAccount kann der Status der Verarbeitung elektronischer Anfragen durch Kaspersky Lab-Spezialisten nachverfolgt sowie eine Chronik der elektronischen Anfragen gespeichert werden.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Ein Benutzerkonto ermöglicht Ihnen die zentralisierte Verwaltung von elektronischen Anfragen aller registrierter Mitarbeiter an Kaspersky Lab sowie die Verwaltung der Rechte dieser Mitarbeiter in Kaspersky CompanyAccount.

Das Portal Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch
- Russisch
- Französisch
- Japanisch

Mehr über Kaspersky CompanyAccount erfahren Sie auf der Website des Technischen Supports https://support.kaspersky.com/de/faq/companyaccount_help.

Protokolldatei und AVZ-Skript verwenden

Wenn Sie sich mit einem Problem an die Experten des Technischen Supports von Kaspersky Lab wenden, werden Sie möglicherweise darum gebeten, einen Bericht über Kaspersky Security 10.1 für Windows Server zu erstellen und den Bericht an den Technischen Support von Kaspersky Lab zu schicken. Zusätzlich können die Experten des Technischen Supports von Kaspersky Lab eine Protokolldatei anfordern. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Experten des Technischen Supports von Kaspersky Lab ein AVZ-Skript erstellen, das dann an Sie geschickt wird. Mit Hilfe von AVZ-Skripten können die laufenden Prozesse auf Bedrohungen analysiert, der Computer auf Bedrohungen untersucht, infizierte Dateien desinfiziert oder entfernt und ein Bericht über die Ergebnisse der Untersuchung des Computers erstellt werden.

Für eine effektivere Unterstützung im Falle des Auftretens von Fragen zur Arbeit des Programms können die Fachleute des Technischen Supports Sie bitten, zur Fehlersuche für den Zeitraum der Diagnose die Programmeinstellungen zu ändern. Hierzu können die folgenden Maßnahmen erforderlich werden:

- Aktivierung der Funktion zur Verarbeitung und Speicherung erweiterter Diagnosedaten.
- Feineinstellung verschiedener Programmkomponenten, die mithilfe der auf der Benutzeroberfläche standardmäßig zur Verfügung stehenden Mittel nicht möglich ist.
- Änderung der Einstellungen für die Speicherung und den Versand verarbeiteter Diagnosedaten.
- Konfiguration der Überwachung und Protokollierung des Netzwerkverkehrs in einer Datei.

AO Kaspersky Lab

Kaspersky Lab ist ein weltweit anerkannter Hersteller von Systemen zum Schutz von Computern vor digitalen Bedrohungen, einschließlich Viren und anderer Schadsoftware, unerwünschten E-Mails (Spam) sowie Netzwerk- und Hacker-Angriffen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach Angaben der IDC ist Kaspersky Lab in Russland der beliebteste Hersteller von Computerschutzsystemen für Heimanwender (IDC Endpoint Tracker 2014).

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern, der in 33 verschiedenen Ländern über insgesamt 38 Niederlassungen verfügt. Das Unternehmen beschäftigt über 3.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die persönliche Produktpalette umfasst Sicherheitsanwendungen für Desktop-, Laptop- und Tablet-Computer, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Schutz- und Steuerungslösungen und -technologien für Workstations und mobile Geräte, virtuelle Maschinen, File- und Webserver, Mail-Gateways und Firewalls. Zum Portfolio des Unternehmens gehören auch spezialisierte Produkte zum Schutz vor DDoS-Angriffen, zum Schutz von industriellen Steuerungssystemen und zur Verhinderung von Finanzbetrug. In Verbindung mit zentralisierten Management-Tools gewährleisten diese Lösungen einen effektiven, automatisierten Schutz für Unternehmen und Organisationen jeder Größe vor Computerbedrohungen. Die Produkte von Kaspersky Lab sind von großen Testlabors zertifiziert, mit Software verschiedener Hersteller kompatibel und für den Einsatz auf vielen Hardware-Plattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Jeden Tag decken sie Hunderttausende neuer Computerbedrohungen auf, erstellen Werkzeuge zur Erkennung und Desinfektion und fügen ihre Signaturen in Datenbanken ein, die von Kaspersky Lab-Anwendungen verwendet werden.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Software-Hersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu und ZyXEL. Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So erhielt Kaspersky Lab 2014 bei Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives neben einem anderen Hersteller die meisten "Advanced+"-Zertifikate und wurde schließlich mit dem "Top Rated"-Zertifikat ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 400 Millionen Anwender und über 270.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	https://www.kaspersky.de
Viren-Enzyklopädie:	https://de.securelist.com
Viren-Labor:	https://virusdesk.kaspersky.com/de (zur Untersuchung verdächtiger Dateien und Webseiten)
Webforum von Kaspersky Lab:	https://forum.kaspersky.com

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in der Datei legal_notices.txt, die sich im Installationsverzeichnis des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Marken und Dienstleistungszeichen sind Eigentum der jeweiligen Rechteinhaber.

AWS (Amazon Web Services) ist eine Marke von Amazon.com, Inc. oder seinen Tochtergesellschaften in den Vereinigten Staaten und/oder anderen Ländern.

Citrix, XenApp und XenDesktop sind Warenzeichen von Citrix Systems, Inc. und/oder einer oder mehrerer ihrer Tochtergesellschaften und können beim United States Patent and Trademark Office und in anderen Ländern eingetragen sein.

Dell und Dell Compellent sind Warenzeichen von Dell, Inc.

Celerra, EMC, Isilon, OneFS und VNX sind in den USA und/oder anderen Ländern registrierte Marken der EMC Corporation.

Hitachi ist eine Handelsmarke von Hitachi, Ltd.

IBM und System Storage sind Warenzeichen der International Business Machines Corporation, die in vielen Ländern weltweit registriert sind.

Excel, Hyper-V, JScript, MultiPoint, Microsoft, Outlook, Windows, Windows Server und Windows Vista sind Handelsmarken von Microsoft Corporation, die in den USA und anderen Ländern eingetragen sind.

NetApp und Data ONTAP sind Marken oder registrierte Marken von NetApp, Inc. in den USA und/oder anderen Ländern.

Linux ist ein registriertes Warenzeichen von Linus Torvalds in den USA und anderen Ländern.

Mozilla und Firefox sind Warenzeichen der Mozilla Foundation.

Oracle ist eine registrierte Handelsmarke von Oracle und/ oder von verbundenen Unternehmen.

Glossar

A

Aktiver Schlüssel

Der Schlüssel, der momentan vom Programm verwendet wird.

Administrationsserver

Programmkomponente von Kaspersky Security Center, mit der die zentralisierte Speicherung von Informationen über die im Unternehmensnetzwerk installierten Programme von Kaspersky Lab realisiert wird. Die Verwaltung dieser Programme erfolgt ebenfalls über diese Komponente.

Antiviren-Datenbanken

Datenbanken, die Informationen über Bedrohungen für die Computersicherheit enthalten, die Kaspersky Lab zum Zeitpunkt der Veröffentlichung der Antiviren-Datenbanken bekannt waren. Mithilfe der Einträge in den Antiviren-Datenbanken wird in den Untersuchungsobjekten schädlicher Code identifiziert.
Die Antiviren-Datenbanken werden von den Experten von Kaspersky Lab gepflegt und stündlich aktualisiert.

Archiv

Eine oder mehrere Dateien, die komprimiert und in einer einzigen Datei zusammengefasst wurden. Ein spezielles Archivierungsprogramm ist zum Komprimieren und Entpacken der Daten erforderlich.

Aufgabe

Das Kaspersky-Lab-Programm führt seine Funktionen in Form von Aufgaben aus, zum Beispiel: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers und Datenbanken-Update.

Aufgabeneinstellungen

Programmeinstellungen, die für den jeweiligen Aufgabentyp gelten.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die ordnungsgemäße Ausführung des auf dem Computer installierten Betriebssystems und der Software benötigt wird. Diese Objekte werden bei jedem Start des Betriebssystems ausgeführt. Es gibt Viren, die genau diese Objekte infizieren können, was beispielsweise dazu führen kann, dass das Betriebssystem nicht gestartet wird.

B

Backup

Ein spezieller Speicher für Backup-Kopien von Dateien, die vor dem Desinfektionsversuch oder dem Löschen der Dateien erstellt werden.

D

Dateimaske

Darstellung eines Dateinamens mithilfe von Platzhaltern. Die Standard-Platzhalter, die in Dateimasken verwendet werden, sind * und ?, wobei * eine beliebige Anzahl an Zeichen und ? ein beliebiges Einzelzeichen ersetzt.

Desinfektion

Verarbeitungsmethode für infizierte Objekte, die eine vollständige oder teilweise Wiederherstellung der Daten zum Ergebnis hat. Nicht alle infizierten Objekte können desinfiziert werden.

E

Echtzeitschutz

Ausführungsmodus des Programms, in dem Objekte in Echtzeit auf das Vorhandensein von schädlichem Code untersucht werden.

Das Programm fängt alle Versuche ab, ein Objekt zu öffnen (lesen, schreiben oder ausführen), und untersucht die Objekte auf Bedrohungen. Nicht infizierte Objekte werden an den Benutzer weitergegeben, während Objekte, die Bedrohungen enthalten oder möglicherweise infiziert sind, gemäß den Aufgabeneinstellungen verarbeitet werden (desinfiziert, gelöscht oder in Quarantäne verschoben).

Ereignispriorität

Eigenschaft eines Ereignisses, das während der Ausführung eines Kaspersky-Lab-Programms aufgetreten ist. Dem Ereignis wird eine von vier Signifikanzen zugewiesen:

- Kritisches Ereignis
- Fehler
- Warnung
- Info

Ereignisse vom gleichen Typ können je nach der Situation, in der sie auftreten, unterschiedliche Signifikanzen haben.

F

Fehlalarm

Eine Situation, in der ein Programm von Kaspersky Lab ein nicht infiziertes Objekt als infiziert betrachtet, weil dessen Code dem eines Virus ähnelt.

H

Heuristische Analyse

Technologie zur Erkennung von Bedrohungen, über die noch keine Informationen in den Datenbanken von Kaspersky Lab enthalten sind. Die heuristische Analyse erkennt Objekte, deren Verhalten eine Sicherheitsbedrohung

für das Betriebssystem darstellen kann. Objekte, die mithilfe der heuristischen Analyse gefunden werden, werden als möglicherweise infiziert eingestuft. Als möglicherweise infiziert kann beispielsweise ein Objekt gelten, das eine Befehlsfolge enthält, die für schädliche Objekte als charakteristisch gilt (Datei öffnen, in Datei schreiben).

I

Infizierbare Datei

Datei, die aufgrund ihrer Struktur bzw. ihres Formates von Betrügern als "Behälter" für die Aufbewahrung und Verteilung von schädlichem Code verwendet werden kann. In der Regel handelt es sich dabei um ausführbare Dateien mit den Erweiterungen com, exe und dll. Das Risiko für das Einschleusen von bösartigem Code in solche Dateien ist recht hoch.

Infiziertes Objekt

Objekt mit einem Abschnitt im Code, der vollständig mit dem Abschnitt im Code einer bekannten Schadsoftware übereinstimmt. Kaspersky Lab empfiehlt nicht, auf solche Objekte zuzugreifen.

K

Kaspersky Security Network (KSN)

Infrastruktur aus Cloud-Diensten, die Zugriff auf die Kaspersky Lab-Datenbank bietet. Diese Datenbank enthält laufend aktualisierte Informationen über die Reputation von Dateien, Webressourcen und Software. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Programme von Kaspersky Lab auf neue Bedrohungen, erhöht die Effektivität der Arbeit einiger Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

L

Laufzeit der Lizenz

Der Zeitraum, in dem Sie Zugriff auf die Programmfunktionen sowie das Recht zur Verwendung zusätzlicher Dienste haben. Die Dienste, die Sie verwenden können, sind vom Lizenztyp abhängig.

Lokale Aufgabe

Eine Aufgabe, die auf einem einzelnen Client-Computer festgelegt wurde und ausgeführt wird.

O

OLE-Objekt

Objekt, das mithilfe der Technologie "Object Linking and Embedding (OLE)" an eine andere Datei angehängt oder in dieser eingebettet ist. Beispiel für ein OLE-Objekt ist eine Tabelle von Microsoft Office Excel®, die in einem Microsoft Office Word-Dokument eingebettet ist.

Q

Quarantäne

Ordner, in den die Programme von Kaspersky Lab erkannte möglicherweise infizierte Objekte verschieben. Objekte werden in der Quarantäne in verschlüsselter Form gespeichert, um eine Einwirkung auf den Computer zu vermeiden.

P

Phishing

Eine Art des Internet-Betrugs mit dem Ziel, unberechtigten Zugriff zu den vertraulichen Daten der Benutzer zu erlangen.

R

Richtlinie

Die Richtlinie bestimmt die Einstellungen eines Programms und verwaltet den Zugriff auf die Konfiguration eines Programms, das auf Computern innerhalb einer Administrationsgruppe installiert ist. Für jedes Programm muss eine separate Richtlinie erstellt werden. Sie können für Programme, die auf Computern in jeder Administrationsgruppe installiert sind, eine unbegrenzte Anzahl an Richtlinien erstellen; allerdings kann nur eine einzige Richtlinie gleichzeitig auf ein Programm innerhalb einer Administrationsgruppe angewendet werden.

S

Schutzstatus

Aktueller Schutzstatus, der die Stufe der Computersicherheit bestimmt.

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.

V

Verdächtiges Objekt

Objekt, das den modifizierten Code eines bekannten Virus oder Code, der an einen Kaspersky Lab noch nicht bekannten Virus erinnert, enthält. Verdächtige Objekte werden mithilfe der heuristischen Analyse erkannt.

U

Update

Vorgang zum Ersetzen bestehender bzw. Hinzufügen neuer Dateien (Datenbanken oder Programm-Module), die von den Kaspersky-Lab-Update-Servern heruntergeladen wurden.

Sachregister

D

V