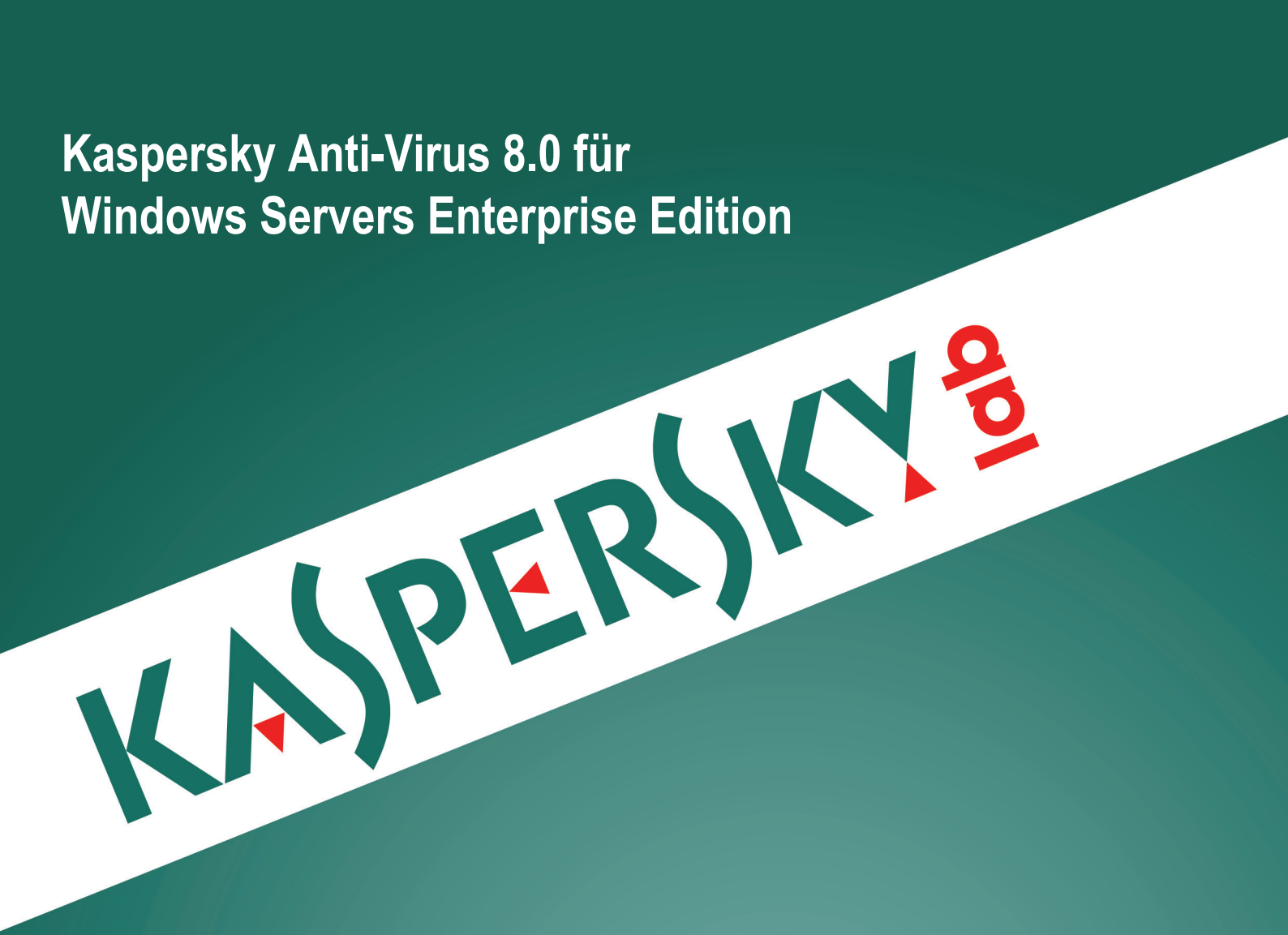
Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition



Administratorhandbuch

PROGRAMMVERSION: 8.0 SERVICE PACK 2

Sehr geehrter Benutzer!

Wir danken Ihnen, dass Sie unser Programm ausgewählt haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und die damit verbundenen Fragen beantworten wird.

Das Dokument kann zukünftig ohne besondere Ankündigung geändert werden. Die neueste Version des Dokumentes finden Sie auf der Seite von Kaspersky Lab unter http://www.kaspersky.com/de/docs.

Redaktionsdatum: 26.02.2015

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

INHALT

ÜBER DIESES DOKUMENT

Das Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers® Enterprise Edition (im Folgenden auch "Kaspersky Anti-Virus" genannt) wendet sich an Fachleute, die verantwortlich sind für die Installation und Verwaltung von Kaspersky Anti-Virus sowie für den technischen Support von Unternehmen, die Kaspersky Anti-Virus nutzen.

Dieses Handbuch bietet Informationen zur Konfiguration und Verwendung des Programms.

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

IN DIESEM ABSCHNITT

IN DIESEM DOKUMENT

Das Administratorhandbuch für Kaspersky Anti-Virus enthält folgenden Abschnitte.

Informationsquellen zu Kaspersky Anti-Virus

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

Kaspersky Anti-Virus

Dieser Abschnitt beschreibt die Funktionen, Komponenten und den Lieferumfang von Kaspersky Anti-Virus sowie die Hard- und Softwarevoraussetzungen für das Programm.

Lizenzierung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzierung des Programms zusammenhängen.

Nutzung der Konsole von Kaspersky Anti-Virus und Zugriff auf die Programmfunktionen

Dieser Abschnitt enthält Informationen zur Konsole von Kaspersky Anti-Virus sowie über die Verwaltung von Kaspersky Anti-Virus über eine auf dem geschützten Server bzw. auf einem anderen Computer installierte Konsole von Kaspersky Anti-Virus.

Kaspersky Anti-Virus-Symbol im Infobereich der Taskleiste

Dieser Abschnitt enthält Informationen über das Symbol von Kaspersky Anti-Virus im Infobereich der Task-Leiste.

Dienst von Kaspersky Anti-Virus starten und anhalten

Dieser Abschnitt informiert über den Start und die Beendigung der Dienste von Kaspersky Anti-Virus.

Schutzstatus und Informationen über Kaspersky Anti-Virus anzeigen

Dieser Abschnitt enthält Anweisungen darüber, wie die Informationen über den aktuellen Schutzstatus des Servers, die Informationen über Kaspersky Anti-Virus und den Status seiner Komponenten zu lesen sind.

Anpassen der allgemeinen Einstellungen von Kaspersky Anti-Virus in der Konsole von Kaspersky Anti-Virus

Dieser Abschnitt enthält Informationen über die Anpassung der allgemeinen Einstellungen des Programms in der Konsole von Kaspersky Anti-Virus.

Aufgaben in Kaspersky Anti-Virus verwalten

Dieser Abschnitt enthält Informationen über die Aufgaben von Kaspersky Anti-Virus, ihre Erstellung, die Festlegung der Einstellungen für ihre Ausführung, den Start und das Beenden von Aufgaben sowie die Anpassung der Einstellungen für den automatischen Start und das automatische Anhalten von Aufgaben nach Zeitplan.

Update der Datenbanken und Module für Kaspersky Anti-Virus

Dieser Abschnitt enthält Informationen über die Aufgaben zum Update der Datenbanken und Module von Kaspersky Anti-Virus, über die Verteilung der Updates und das Rollback eines Datenbanken-Updates in Kaspersky Security, sowie Anweisungen zum Anpassen der Aufgabeneinstellungen für Updates von Datenbanken und Programm-Modulen.

Echtzeitschutz

Dieser Abschnitt informiert über folgende Echtzeitschutzaufgaben: **Echtzeitschutz für Dateien** und **Skript-Untersuchung**. Darüber hinaus enthält dieser Abschnitt Anweisungen zum Anpassen der Einstellungen für Aufgaben zum Echtzeitschutz sowie zum Anpassen der Sicherheitseinstellungen des geschützten Servers.

Virensuche

Dieser Abschnitt enthält Informationen über die Aufgaben zur Untersuchung auf Befehl und Anweisungen zum Anpassen der Einstellungen der Aufgaben zur Untersuchung auf Befehl sowie zum Anpassen der Sicherheitseinstellungen für Aufgaben zur Untersuchung auf Befehl.

Vertrauenswürdige Zone

Dieser Abschnitt enthält Informationen über die vertrauenswürdige Zone für Kaspersky Anti-Virus, Anweisungen zum Hinzufügen von Objekten in die vertrauenswürdige Zone sowie zur Anwendung der vertrauenswürdigen Zone in den Aufgaben von Kaspersky Anti-Virus.

Isolierung möglicherweise infizierter Objekte. Verwendung der Quarantäne

Dieser Abschnitt enthält Informationen über die Isolierung von möglicherweise infizierten Objekten, also über die Verschiebung dieser Objekte in die Quarantäne sowie über die Anpassung der Quarantäne-Einstellungen.

Sicherungskopieren von Objekten vor Desinfektion / Löschen. Verwendung des Backups

Dieser Abschnitt enthält Informationen über die Erstellung von Sicherungskopien für gefundene schädliche Objekte, bevor diese desinfiziert oder gelöscht werden, sowie über die Anpassung der Einstellungen des Backups.

Registrieren von Ereignissen. Berichte von Kaspersky Anti-Virus

Dieser Abschnitt informiert über die Verwendung folgender Berichte von Kaspersky Anti-Virus: Systemaudit-Bericht, Berichte über die Ausführung der Aufgaben von Kaspersky Anti-Virus und Ereignisbericht von Kaspersky Anti-Virus.

Nutzung von Schlüsseln in Kaspersky Anti-Virus

In diesem Abschnitt wird beschrieben, wie ein Schlüssel zum Programm hinzugefügt wird, wie ein Schlüssel aus dem Programm gelöscht wird und wie Informationen über hinzugefügte Schlüssel angezeigt werden können.

Benachrichtigungen anpassen

Dieser Abschnitt enthält Informationen über Möglichkeiten zur Benachrichtigung von Benutzern und Administratoren von Kaspersky Anti-Virus über Programmereignisse und den Schutzstatus des Servers sowie Anleitungen zur Anpassung von Benachrichtigungen.

Verwaltung hierarchischer Speicher

Dieser Abschnitt enthält Informationen über die Antiviren-Untersuchung von Dateien, die sich in den hierarchischen Speichern und den Backup-Systemen befinden.

Import und Export von Parametern

Dieser Abschnitt enthält Informationen über den Export der Einstellungen für die Ausführung von Kaspersky Anti-Virus bzw. der Einstellungen für die Ausführung der verschiedenen Programmkomponenten in eine Konfigurationsdatei im XML-Format, sowie über den Import dieser Einstellungen aus der Konfigurationsdatei ins Programm.

Verwaltung von Kaspersky Anti-Virus aus der Befehlszeile

Dieser Abschnitt enthält Informationen und Anweisungen über die Verwaltung von Kaspersky Anti-Virus über die Befehlszeile.

Verwaltung von Kaspersky Anti-Virus aus Kaspersky Security Center

Dieser Abschnitt enthält Informationen und Anweisungen über die Verwaltung von Kaspersky Anti-Virus und die Anpassung der Einstellungen von Kaspersky Anti-Virus mithilfe der Administrationskonsole von Kaspersky Security Center.

Kaspersky Anti-Virus-Indikatoren

Dieser Abschnitt informiert über die Indikatoren von Kaspersky Anti-Virus: Leistungsindikatoren für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps.

Technischer Support

Dieser Abschnitt beschreibt die Möglichkeiten für die technische Unterstützung und die Support-Richtlinien.

Glossar

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

Kaspersky Lab

Dieser Abschnitt bietet Informationen über ZAO Kaspersky Lab.

Informationen zum Code von Drittherstellern

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

Markenhinweise

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 gelb unterlegten Blöcken und sind mit "Beispiel" überschrieben.

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Das *Update* ist ... 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 **Aktivieren**.	Die Namen von Elementen der Programmoberfläche sind fett geschrieben (z. B. Eingabefelder, Menüpunkte, Schaltflächen).
➧ *Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:*	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 ZU KASPERSKY ANTI-VIRUS

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 ABSCHNITT

QUELLEN FÜR DIE SELBSTSTÄNDIGE INFORMATIONSSUCHE

Für Kaspersky Anti-Virus stehen Ihnen folgende Informationsquellen zur Verfügung:

- Seite von Kaspersky Anti-Virus auf der Webseite von Kaspersky Lab
- Seite von Kaspersky Anti-Virus auf der Webseite des Technischen Supports (Wissensdatenbank)
- Elektronisches Hilfesystem
- Dokumentation

Wenn Sie keine Lösung für Ihr Problem finden, können Sie sich an den Technischen Support von Kaspersky Lab wenden.

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

Seite von Kaspersky Anti-Virus auf der Webseite von Kaspersky Lab

Auf der Seite von Kaspersky Anti-Virus (http://www.kaspersky.com/de/anti-virus-windows-server-enterprise) stehen Ihnen allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und Besonderheiten zur Verfügung.

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

Seite über Kaspersky Anti-Virus in der Wissensdatenbank

Die *Wissensdatenbank* ist ein spezieller Bereich auf der Support-Webseite.

Auf der Seite von Kaspersky Anti-Virus in der Wissensdatenbank (http://support.kaspersky.com/de/wsee8) 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 Anti-Virus, sondern auch auf andere Programme von Kaspersky Lab. Außerdem können Artikel der Wissensdatenbank auch Neuigkeiten über den Technischen Support enthalten.

Im Handbuch zur Software-Verteilung finden Sie typische Vorgehensweisen zur Installation von Kaspersky Anti-Virus in einem Unternehmensnetzwerk.

Im Installationshandbuch finden Sie Informationen über die Ausführung folgender Aufgaben:

- Vorbereitung der Installation, Installation und Aktivierung von Kaspersky Anti-Virus
- Vorbereitung von Kaspersky Anti-Virus zur Ausführung
- Reparatur und Entfernen von Kaspersky Anti-Virus

Das Administratorhandbuch bietet Informationen zur Konfiguration und Verwendung von Kaspersky Anti-Virus.

Das Handbuch für die Implementierung zum Schutz von Netzwerkspeichern bietet Informationen zur Konfiguration und Verwendung von Kaspersky Anti-Virus zum Schutz von Netzwerkspeichern.

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) besprechen.

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

KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus schützt Server mit Microsoft® Windows®-Betriebssystem sowie NetApp Storage-Systeme vor Viren und anderen Bedrohungen für die Computersicherheit, die bei der Übertragung von Dateien eindringen können. Kaspersky Anti-Virus ist zum Einsatz in lokalen Netzwerken mittlerer und großer Unternehmen vorgesehen. Als Benutzer von Kaspersky Anti-Virus gelten Netzwerkadministratoren des Unternehmens und Mitarbeiter, die für die Antiviren-Sicherheit des Unternehmensnetzwerks zuständig sind.

Sie können Kaspersky Anti-Virus auf Servern installieren, die folgende Funktionen ausführen:

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

Sie können Kaspersky Anti-Virus auf folgende Arten verwalten:

- Über die Konsole für Kaspersky Anti-Virus, die auf einem Server mit Kaspersky Anti-Virus oder auf einem anderen Computer installiert ist.
- Mithilfe eines Befehls in der Befehlszeile.
- Über die Administrationskonsole von Kaspersky Security Center.

Sie können die Anwendung Kaspersky Security Center verwenden, die der zentralisierten Verwaltung des Schutzes mehrerer Server dient, auf denen jeweils eine Exemplar von Kaspersky Anti-Virus installiert ist.

Sie können die Leistungsindikatoren von Kaspersky Anti-Virus für die Anwendung "Systemmonitor" sowie Indikatoren und SNMP-Traps analysieren.

Komponenten und Funktionen von Kaspersky Anti-Virus

Im Lieferumfang des Programms sind folgende Komponenten enthalten:

- Echtzeitschutz für Dateien

  Kaspersky Anti-Virus untersucht Objekte, wenn darauf zugegriffen wird. Kaspersky Anti-Virus untersucht folgende Objekte:

  - Dateien
  - alternative Datenströme der Dateisysteme (NTFS-Streams)
  - MBR und Bootsektoren von lokalen Festplatten und Wechseldatenträgern

- Skript-Untersuchung

  Kaspersky Anti-Virus kontrolliert die Ausführung von Skripts, die mit Microsoft Windows Script Technologies (oder Active Scripting) erstellt worden sind, z. B. VBScript- oder JScript®-Skripts. Die Ausführung von Skripts wird nur erlaubt, wenn das betreffende Skript von Kaspersky Anti-Virus als sicher eingestuft wurde. Kaspersky Anti-Virus verbietet die Ausführung von Skripts, die als gefährlich eingestuft wurden. Wenn Kaspersky Anti-Virus ein Skript als potenziell gefährlich eingestuft hat, führt er die von Ihnen festgelegte Aktion aus: Die Ausführung des Skripts wird verboten oder erlaubt.

- Schutz von Netzwerkspeichern

  Wenn Kaspersky Anti-Virus 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.

- Virensuche

  Kaspersky Anti-Virus überprüft den angegebenen Bereich einmalig auf Viren und andere Bedrohungen der Computersicherheit. Kaspersky Anti-Virus überprüft Daten, den Arbeitsspeicher des Servers sowie Autostart-Objekte.

Das Programm verfügt über folgenden Funktionen:

- Update der Datenbanken und Programm-Module

  Für den Download von Updates für die Datenbanken und Programm-Module verwendet Kaspersky Anti-Virus die FTP- oder HTTP-Update-Server von Kaspersky Lab, den Administrationsserver von Kaspersky Security Center oder andere Update-Quellen.

- Quarantäne

  Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft worden sind, werden in die Quarantäne verschoben, d. h. die Objekte werden von ihrem ursprünglichen Speicherort in den *Quarantäne-Ordner* verschoben. Aus Sicherheitsgründen werden die Objekte im Quarantäne-Ordner in verschlüsselter Form gespeichert.

- Backup

  Bevor ein Objekt mit dem Status *Infiziert* oder *Möglicherweise infiziert* desinfiziert oder gelöscht wird, speichert Kaspersky Anti-Virus 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 Server zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Anti-Virus und dem Status der Antiviren-Sicherheit des Servers zusammenhängen, anpassen.

- Import und Export von Parametern

  Sie können die Einstellungen von Kaspersky Anti-Virus in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Anti-Virus importieren. In einer Konfigurationsdatei können entweder alle Einstellungen für Kaspersky Anti-Virus oder nur die Einstellungen einzelner Komponenten gespeichert werden.

IN DIESEM ABSCHNITT

NEUERUNGEN

Das Programm bietet folgende Neuerungen:

- Schutzfunktion für Netzwerkspeicher nach RPC- und ICAP-Protokoll
- Unterstützung folgender Server-Betriebssysteme in Microsoft Windows:
  - Microsoft Windows Server® 2012 Datacenter;
  - Microsoft Windows Server 2012 Essentials;
  - Microsoft Windows Server 2012 Foundation;
  - Microsoft Windows Server 2012 Standard;
  - Microsoft Windows Server 2012 R2 Datacenter;
  - Microsoft Windows Server 2012 R2 Essentials;
  - Microsoft Windows Server 2012 R2 Foundation;
  - Microsoft Windows Server 2012 R2 Standard.
- Unterstützung folgender Desktop-Betriebssysteme in Microsoft Windows:
  - Microsoft Windows 8:
  - Microsoft Windows 8 Enterprise;
  - Microsoft Windows 8 Professional;

- Microsoft Windows 8.1;
- Microsoft Windows 8.1 Enterprise;
- Microsoft Windows 8.1 Professional.

LIEFERUMFANG

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

- Installationsassistent von Kaspersky Anti-Virus starten
- Installationsassistent der Konsole von Kaspersky Anti-Virus starten
- Installationsassistent für das Plug-In zur Steuerung von Kaspersky Anti-Virus über das Kaspersky Security Center starten
- Installationsanleitung, Administratorhandbuch und Handbuch zur Software-Verteilung lesen
- Die Seite von Kaspersky Anti-Virus auf der Webseite von Kaspersky Lab aufrufen
- Die Webseite des Technischen Supports aufrufen

Im Ordner \x86 befinden sich die Dateien zur Installation von Kaspersky Anti-Virus, der Konsole für Kaspersky Anti-Virus und das Plug-in zur Verwaltung von Kaspersky Anti-Virus über Kaspersky Security Center auf einem Server unter einem 32-Bit-Betriebssystem von Microsoft Windows; im Ordner \x64 befinden sich die Dateien zur Installation von Kaspersky Anti-Virus, der Konsole für Kaspersky Anti-Virus und das Plug-in zur Verwaltung von Kaspersky Anti-Virus über Kaspersky Security Center auf einem Server unter einem 64-Bit-Betriebssystem von Microsoft Windows.

Die Ordner \x86 und \x64 enthalten folgende Unterordner:

- Der Ordner \server enthält die Dateien für die Installation der Schutzkomponenten von Kaspersky Anti-Virus.
- Der Ordner \client enthält die Dateien für die Installation der Konsole von Kaspersky Anti-Virus (Komponentensatz "Administrationswerkzeuge").
- Der Ordner \plugin enthält die Installationsdatei für das Verwaltungs-Plug-in für Kaspersky Anti-Virus über Kaspersky Security Center.

Die Dateien, die zum Lieferumfang von Kaspersky Anti-Virus gehören, werden in der folgenden Tabelle näher beschrieben.

Tabelle 2. Dateien im Lieferumfang von Kaspersky Anti-Virus

DATEI	ZIEL
setup.exe	Datei zum Starten des Begrüßungsprogramms.
\setup	In diesem Ordner befinden sich die Dateien des Begrüßungsprogramms.
kav8.0_wsee_install_guide_de.pdf	Installationsanleitung.
kav8.0_wsee_admin_guide_de.pdf	Administratorhandbuch.
kav8.0_wsee_deploy_guide_de.pdf	Handbuch zur Software-Verteilung, in dem typischen Szenarien zur Implementierung eines Schutzsystems beschrieben werden.
autorun.inf	Datei für den Autostart des Begrüßungsprogramms.
release_notes.txt	Diese Datei enthält Versionshinweise.
x86(x64)\server\setup.exe	Assistent zur Installation von Kaspersky Anti-Virus auf dem geschützten Server; startet die Datei des Installationspakets kavws.msi mit den im Assistenten gewählten Installationsparametern.
x86(x64)\server\kavws.msi	Installationspaket des Dienstes Windows Installer; installiert Kaspersky Anti-Virus auf dem geschützten Server.

DATEI	ZIEL
x86(x64)\server\kavws.kpd	Datei mit der Beschreibung des Installationspakets zur Remote-Installation von Kaspersky Anti-Virus über Kaspersky Security Center (besitzt die Erweiterung .kpd (Kaspersky Package Definition). Sie enthält den Namen des Installationspakets, allgemeine Angaben zu Kaspersky Anti-Virus (Versionsnummer und Erstellungsdatum) sowie Beschreibungen der Rückgabecodes des Installationsprogramms. Diese Datei kann außerdem Schlüssel der Befehlszeile enthalten, die die Parameter der Installation über Kaspersky Security Center vorgeben.
x86(x64)\server\kavws.kud	Datei mit der Beschreibung des Installationspakets zur Remote-Installation von Kaspersky Anti-Virus über Kaspersky Security Center im Kaspersky Unicode Definition Format. Wird bei der Datei kavws.kpd genutzt.
x86(x64)\client\setup.exe	Assistent zur Installation des Komponentensatzes "Administrationswerkzeuge" (dazu gehört die Konsole von Kaspersky Anti-Virus); startet die Datei des Installationspakets kavwstools.msi mit den im Assistenten gewählten Installationsparametern.
x86(x64) \client\kavwstools.msi	Die Installationspaket des Dienstes Windows Installer; installiert auf dem Computer die Konsole von Kaspersky Anti-Virus.
x86(x64) \plugin\klcfginst.exe	Installationsprogramm für das Plug-In zur Steuerung von Kaspersky Anti-Virus über das Kaspersky Security Center. Installieren Sie das Plug-In auf jedem Rechner, auf dem die Administrationskonsole von Kaspersky Security Center installiert ist, wenn Sie Kaspersky Anti-Virus mit dieser Konsole verwalten möchten.

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 Anti-Virus.

IN DIESEM ABSCHNITT

ANFORDERUNGEN AN DEN SERVER, AUF DEM KASPERSKY ANTI-VIRUS INSTALLIERT WIRD

Vor der Installation von Kaspersky Anti-müssen Virus andere Antiviren-Anwendungen vom Server deinstalliert werden.

Sie können Anti-Virus installieren, ohne Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition oder Kaspersky Anti-Virus 6.0 bzw. 8.0 für Windows Servers deinstallieren zu müssen.

Hardwarevoraussetzungen für den Server

Generelle Voraussetzungen:

- x86-kompatible Systeme mit Single-Core- und Multi-Core-Konfigurationen; x86-64-kompatible Systeme mit Single-Core- und Multi-Core-Konfigurationen
- 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 Berichten – 1 GB (empfohlen)
  - zum Speichern von Berichten – 2 GB (empfohlen)

Minimalkonfiguration:

- Prozessor – 1 Intel® Core™ 1,4 GHz
- Arbeitsspeicher – 1 GB
- Speicherplatz auf dem Datenträger – 4 GB freier Speicherplatz

Empfohlene Konfiguration:

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

Softwarevoraussetzungen für den Server

Sie können Kaspersky Anti-Virus auf einem Server installieren, der unter einem 32-Bit- oder 64-Bit-Betriebssystem von Microsoft® Windows® läuft.

Für die Installation und Ausführung von Kaspersky Anti-Virus muss auf dem Server Microsoft Windows Installer 3.1 vorhanden sein.

Sie können Kaspersky Anti-Virus auf einem Server installieren, der unter einem der folgenden 32-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 Core Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher

Sie können Kaspersky Anti-Virus auf einem Server installieren, der unter einem der folgenden 64-Bit-Betriebssysteme von Microsoft Windows läuft:

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 Core Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 R2 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 R2 Core Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Hyper-V® Server 2008 R2 mit Service Pack 1 oder höher;
- Windows Server 2012 Essentials, Standard, Foundation bzw. Datacenter Edition
- Windows Server 2012 R2 Essentials, Standard, Foundation bzw. Datacenter Edition;
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2

Sie können Kaspersky Anti-Virus auf folgenden Terminal-Servern installieren:

- Microsoft Terminal Services auf der Grundlage des Windows 2003 Servers;
- Microsoft Remote Desktop Services auf der Grundlage des Windows 2008 Servers
- Microsoft Remote Desktop Services auf der Grundlage des Windows 2012 Servers
- Microsoft Remote Desktop Services auf der Grundlage des Windows 2012 Servers R2;
- Citrix Presentation Server™ 4.0, 4,5;
- Citrix® XenApp® 4.5, 5.0, 6.0, 6.5;
- Citrix XenDesktop® 7.0, 7.1, 7.5.

ANFORDERUNGEN AN DEN GESCHÜTZTEN NETZWERKSPEICHER

Kaspersky Anti-Virus 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.
- 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
- 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 series.

ANFORDERUNGEN AN DEN COMPUTER, AUF DEN DIE KONSOLE FÜR KASPERSKY ANTI-VIRUS 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 Anti-Virus 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 Anti-Virus muss auf dem Computer Microsoft Windows Installer 3.1 vorhanden sein.

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

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Microsoft Windows XP Professional mit Service Pack 2 oder höher;
- Microsoft Windows Vista® Editions
- Microsoft Windows 7 Editions
- Microsoft Windows 8:
- Microsoft Windows 8 Enterprise bzw. Professional;
- Microsoft Windows 8.1;
- Microsoft Windows 8.1 Enterprise bzw. Professional.

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

- Windows Server 2003 Standard bzw. Enterprise Edition mit Service Pack 2
- Windows Server 2003 R2 Standard / Enterprise mit Service Pack SP2
- Windows Server 2008 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Server 2008 R2 Standard, Enterprise bzw. Datacenter Edition mit Service Pack 1 oder höher
- Windows Hyper-V Server 2008 R2 mit Service Pack SP1 oder höher
- Windows Server 2012 Essentials, Standard, Foundation bzw. Datacenter Edition
- Windows Server 2012 R2 Essentials, Standard, Foundation bzw. Datacenter Edition;
- Windows Hyper-V Server 2012
- Windows Hyper-V Server 2012 R2
- Microsoft Windows XP Professional Edition mit Service Pack 2 oder höher
- Microsoft Windows Vista Editions;
- Microsoft Windows 7 Editions
- Microsoft Windows 8:
- Microsoft Windows 8 Enterprise bzw. Professional;
- Microsoft Windows 8.1;
- Microsoft Windows 8.1 Enterprise bzw. Professional.

LIZENZIERUNG DES PROGRAMMS

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Lizenzierung des Programms zusammenhängen.

IN DIESEM ABSCHNITT

ÜBER DIE LIZENZ

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm. Dieses Recht wird Ihnen auf Basis eines Lizenzvertrags zur Verfügung gestellt.

Die Lizenz berechtigt zur Nutzung folgender Leistungen:

- Nutzung des Programms in Übereinstimmung mit den Bedingungen des Lizenzvertrags
- Technischer 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 *Testlizenz* ist eine kostenlose Lizenz, die zum Kennenlernen des Programms vorgesehen ist.

  Eine Testlizenz besitzt eine kurze Gültigkeitsdauer. Nach Ablauf der Testlizenz stellt Kaspersky Anti-Virus alle Funktionen ein. 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 weiterhin, wobei aber der Funktionsumfang eingeschränkt wird (dann ist beispielsweise das Update für die Datenbanken von Kaspersky Anti-Virus nicht mehr verfügbar). Zur weiteren Nutzung von Kaspersky Anti-Virus 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 ein optimaler Schutz vor Computerbedrohungen gewährleisten

ÜBER DEN LIZENZVERTRAG

Der Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen und Kaspersky Lab ZAO. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig durch, bevor Sie beginnen, mit dem Programm zu arbeiten.

Die Lizenzbedingungen können Sie wie folgt einsehen:

- Während der Installation von Kaspersky Anti-Virus.
- Im Dokument license.txt. Dieses Dokument gehört zum Lieferumfang des Programms.

Wenn Sie bei der Programminstallation dem Text des Lizenzvertrags zustimmen, gelten die Bedingungen des Lizenzvertrags als akzeptiert. Falls Sie die Bedingungen des Lizenzvertrags ablehnen, müssen Sie die Programminstallation abbrechen oder dürfen das Programm nicht verwenden.

ÜBER DAS LIZENZZERTIFIKAT

Ein *Lizenzzertifikat* ist ein Dokument, das Sie zusammen mit einer Schlüsseldatei oder einem Aktivierungscode erhalten.

Das Lizenzzertifikat enthält folgende Informationen über die entsprechende Lizenz:

- Lizenznummer
- Informationen über den Benutzer, der die Lizenz erhalten hat.
- Informationen über das Programm, das mit dieser Lizenz aktiviert werden kann.
- Quantitative Einschränkungen im Hinblick auf die Lizenzierungseinheiten (beispielsweise Geräte, auf denen das Programm mit dieser Lizenz verwendet werden darf).
- Datum für den Beginn der Lizenzgültigkeit
- Datum für das Ende der Lizenzgültigkeit, oder Gültigkeitsdauer der Lizenz
- Lizenztyp

ÜBER DEN SCHLÜSSEL

Ein *Schlüssel* ist eine Bitsequenz, mit deren Hilfe Sie das Programm aktivieren können, um es dann in Übereinstimmung mit dem Lizenzvertrag zu nutzen. Der Schlüssel wird von den Kaspersky-Lab-Experten generiert.

Mithilfe der *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.

Ein Schlüssel kann von Kaspersky Lab gesperrt werden, falls die Bedingungen des Lizenzvertrags verletzt 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 jeweils nur ein aktiver Aktivierungscode installiert werden.

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 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 von Ihnen angegebene E-Mail-Adresse geschickt, nachdem Sie Kaspersky Anti-Virus gekauft oder eine Testversion von Kaspersky Anti-Virus angefordert haben.

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

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

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

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab. (http://support.kaspersky.com/de).
- Erhalt der Schlüsseldatei auf der Website von Kaspersky Lab (https://activation.kaspersky.com/de/) auf Basis eines vorhandenen Aktivierungscodes.

NUTZUNG DER KONSOLE VON KASPERSKY ANTI-VIRUS UND ZUGRIFF AUF DIE PROGRAMMFUNKTIONEN

Dieser Abschnitt enthält Informationen zur Konsole von Kaspersky Anti-Virus sowie über die Verwaltung von Kaspersky Anti-Virus über eine auf dem geschützten Server bzw. auf einem anderen Computer installierte Konsole von Kaspersky Anti-Virus.

IN DIESEM ABSCHNITT

ÜBER DIE KONSOLE VON KASPERSKY ANTI-VIRUS

Die Konsole von Kaspersky Anti-Virus ist ein isoliertes Snap-in, das in die Microsoft Management Console eingefügt wird.

Sie können Kaspersky Anti-Virus über die Konsole von Kaspersky Anti-Virus in der MMC verwalten, die auf dem geschützten Server oder auf einem anderen Computer im Unternehmensnetzwerk installiert ist. Nachdem Sie die Anti-Virus-Konsole auf einem anderen Computer installiert haben, sind zusätzliche Einstellungen erforderlich (s. Pkt. "Zusätzliche Einstellungen nach der Installation der Kaspersky Anti-Virus-Konsole in der MMC auf einem anderen Computer" auf S. 24).

Wenn die Konsole für Kaspersky Anti-Virus und Kaspersky Anti-Virus auf verschiedenen Computern installiert sind, die zu verschiedenen Domains gehören, kann es vorkommen, dass nicht alle Informationen über Kaspersky Anti-Virus in der Konsole für Kaspersky Anti-Virus verfügbar sind. Beispielsweise wird nach dem Start einer Aufgabe in Kaspersky Anti-Virus der Status dieser Aufgabe in der Konsole möglicherweise nicht mehr aktualisiert.

Beim Installieren der Konsole von Kaspersky Anti-Virus speichert der Installationsassistent die Datei kavfs.msc im Installationsordner von Kaspersky Anti-Virus und fügt das Snap-in für Kaspersky Anti-Virus zur Liste der isolierten Microsoft Windows-Snap-ins hinzu.

Sie können die Konsole für Kaspersky Anti-Virus aus dem Menü **Start** öffnen. Auf dem geschützten Server können Sie die Konsole für Kaspersky Anti-Virus auch mithilfe des Kaspersky Anti-Virus-Symbols im Infobereich der Taskleiste öffnen.

Sie können die msc-Datei des Snap-ins von Kaspersky Anti-Virus starten oder das Snap-in von Kaspersky Anti-Virus in eine vorhandene MMC-Konsole als neues Element in deren Struktur einfügen (s. Abschnitt "Benutzeroberfläche des Konsolenfensters von Kaspersky Anti-Virus" auf S. 27).

In der 64-Bit-Version von Microsoft Windows können Sie das Snap-in von Kaspersky Anti-Virus nur in die MMC der 32-Bit-Version (MMC32) einfügen. Öffnen Sie dazu die MMC aus der Befehlszeile mit dem Befehl mmc.exe /32.

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

ZUSÄTZLICHE EINSTELLUNGEN NACH DER INSTALLATION DER KONSOLE VON KASPERSKY ANTI-VIRUS AUF EINEM ANDEREN COMPUTER

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus über eine auf einem anderen Computer installierte Konsole von Kaspersky Anti-Virus zu verwalten:

- Auf dem geschützten Server:
  - Fügen Sie die Benutzer der Konsole von Kaspersky Anti-Virus zur Gruppe KAVWSEE Administrators hinzu.
  - Wenn auf dem geschützten Server die Windows-Firewall aktiviert ist, muss die Netzwerkverbindung für den Prozess des Verwaltungsdienstes von Kaspersky Anti-Virus kavfsgt.exe zulässig sein.

    Ab Windows Server 2008 ist die Windows-Firewall für alle Server-Betriebssysteme von Windows standardmäßig aktiviert.
- Wenn Sie auf dem Computer mit installierter Konsole von Kaspersky Anti-Virus bei der Installation der Konsole das Kontrollkästchen **Netzwerkverbindungen für die Konsole von Kaspersky Anti-Virus erlauben** nicht aktiviert haben, müssen Sie Netzwerkverbindungen für die Konsole von Kaspersky Anti-Virus zulassen.

IN DIESEM ABSCHNITT

BENUTZER VON KASPERSKY ANTI-VIRUS ZUR GRUPPE KAVWSEE ADMINISTRATORS AUF DEM GESCHÜTZTEN SERVER HINZUFÜGEN

Um Kaspersky Anti-Virus über eine auf einem anderen Computer installierte Konsole für Kaspersky Anti-Virus zu verwalten, muss das Benutzerkonto, mit dessen Rechten die Verbindung zu Kaspersky Anti-Virus hergestellt wird, auf dem geschützten Server Vollzugriff auf den Verwaltungsdienst des Programms (Kaspersky Anti-Virus Management) haben. Standardmäßig haben Benutzer, die der Gruppe "Administratoren" auf dem geschützten Server angehören, Zugriff auf diesen Dienst.

Detaillierte Informationen über die Dienste, die von Kaspersky Anti-Virus registriert werden, finden Sie im *Installationshandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition*.

Während der Installation registriert Kaspersky Anti-Virus auf dem geschützten Server die Gruppe KAVWSEE Administrators. Für die Benutzer dieser Gruppe ist der Zugang zum Verwaltungsdienst des Kaspersky Anti-Virus erlaubt. Sie können den Zugriff auf den Verwaltungsdienst von Kaspersky Anti-Virus für Benutzer erlauben oder sperren, indem Sie die Benutzer zur Gruppe KAVWSEE Administrators hinzufügen oder sie daraus entfernen.

Sie können unter dem lokalen Benutzerkonto eine Verbindung mit Kaspersky Anti-Virus herstellen, wenn auf dem geschützten Server das Benutzerkonto mit dem gleichen Namen und dem gleichen Kennwort angemeldet ist.

NETZWERKVERBINDUNGEN FÜR DEN DIENST VERWALTUNG VON KASPERSKY ANTI-VIRUS AUF DEM GESCHÜTZTEN SERVER ERLAUBEN

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

Um die Netzwerkverbindungen für den Dienst Verwaltung von Kaspersky Anti-Virus auf dem geschützten Server freizugeben, gehen Sie wie folgt vor:

1. Auf einem Server mit dem Betriebssystem Microsoft Windows Server 2008 klicken Sie auf **Start** → **Systemsteuerung** → **Sicherheit** → **Windows-Firewall**.
2. Wählen Sie im Fenster **Einstellungen für Windows-Firewall 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. Sie befindet sich im Ordner, den Sie bei der Installation der Konsole von Kaspersky Anti-Virus als Zielordner angegeben haben.
6. Klicken Sie auf **OK**.
7. Klicken Sie im Fenster **Einstellungen für Windows-Firewall** auf die Schaltfläche **OK**.

NETZWERKVERBINDUNGEN FÜR DIE KONSOLE VON KASPERSKY ANTI-VIRUS ERLAUBEN

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

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

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

Wenn die Konsole von Kaspersky Anti-Virus geöffnet war, während Sie die Verbindung zwischen dem geschützten Server und dem Computer, auf dem die Konsole installiert ist, angepasst haben, müssen Sie die Konsole schließen, auf die Beendigung des Prozesses zur Remote-Verwaltung von Kaspersky Anti-Virus 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 Computer, auf dem die Konsole von Kaspersky Anti-Virus installiert ist, die Konsole Komponentendienste: Klicken Sie auf **Start** → **Ausführen**, geben Sie den Befehl dcomcnfg ein und klicken Sie auf **OK**.
2. Öffnen Sie in der Konsole Komponentendienste den Knoten **Computer**, öffnen Sie das Kontextmenü für den Knoten **Arbeitsplatz** und wählen Sie **Eigenschaften** aus.
3. Klicken Sie im Fenster **Eigenschaften** auf der Registerkarte **COM-Sicherheit** in der Optionsgruppe **Zugriffsrechte** auf die Schaltfläche **Begrenzungen ändern**.
4. Vergewissern Sie sich im Fenster **Zugriffsberechtigungen**, dass für den Benutzer ANONYMOUS LOGON das Kontrollkästchen **Remotezugriff** aktiviert ist.
5. 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 Anti-Virus zu erlauben, gehen Sie wie folgt vor:*

  1. Schließen Sie die Konsole von Kaspersky Anti-Virus 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 mit Service Pack 2 oder höher auf **Start → Windows-Firewall**.

          Klicken Sie in Microsoft Windows Vista auf **Start → Systemsteuerung → Windows-Firewall** und wählen Sie im Fenster **Windows-Firewall 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 Anti-Virus). Geben Sie im Feld **Portnummer** die Nummer des Ports an:

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

       e. Klicken Sie auf **OK**.

       f. Klicken Sie auf der Registerkarte **Ausnahmen** auf die Schaltfläche **Programm hinzufügen**.

     - *In Microsoft Windows 7*:
       a. Klicken Sie auf **Start → Systemsteuerung → Windows-Firewall** und wählen Sie im Fenster **Windows-Firewall** den Punkt **Ein Programm oder Feature durch die Windows-Firewall zulassen Windows**.

       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 von Kaspersky Anti-Virus als Zielordner angegeben haben.
  4. Klicken Sie auf **OK**.
  5. Klicken Sie im Fenster **Windows-Firewall** (**Einstellungen für Windows-Firewall**) auf die Schaltfläche **OK**.

START DER KONSOLE VON KASPERSKY ANTI-VIRUS AUS DEM STARTMENÜ

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

Überzeugen Sie sich davon, dass die Konsole von Kaspersky Anti-Virus auf dem Computer installiert ist.

- *Um die Konsole von Kaspersky Anti-Virus aus dem Startmenü zu starten:*

  Wählen Sie den Punkt **Start → Programme → Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Administrations-Tools → Konsole für Kaspersky Anti-Virus**.

  - Wenn Sie planen, andere Snap-ins zur Konsole für Kaspersky Anti-Virus hinzuzufügen, öffnen Sie die Konsole im Autorenmodus. Wählen Sie dazu den Punkt **Start → Programme → Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Administrations-Tools**. Öffnen Sie das Kontextmenü des Programms **Konsole von Kaspersky Anti-Virus** und wählen Sie den Befehl **Autor**.
  - Wenn Sie die Konsole von Kaspersky Anti-Virus auf dem geschützten Server gestartet haben, öffnet sich das Konsolenfenster (s. Abschnitt "Benutzeroberfläche des Konsolenfensters von Kaspersky Anti-Virus" auf S. 27).
  - Wenn Sie die Konsole von Kaspersky Anti-Virus nicht auf dem geschützten Server, sondern auf einem anderen Computer gestartet haben, stellen Sie eine Verbindung mit dem geschützten Server her. Öffnen Sie dazu in der Konsolenstruktur das Kontextmenü des Knotens von Kaspersky Anti-Virus und wählen Sie den Befehl **Verbindung mit anderem Computer herstellen**. Wählen Sie im folgenden 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 bei Microsoft Windows angemeldet haben, nicht über die erforderlichen Rechte für den Zugriff auf den Dienst Verwaltung von Kaspersky Anti-Virus auf dem Server verfügen, dann aktiveren Sie das Kontrollkästchen **Verbindung mit Rechten des folgenden Benutzerkontos herstellen** und geben Sie ein anderes Benutzerkonto an, das über die entsprechenden Rechte verfügt (s. Abschnitt "Benutzer von Kaspersky Anti-Virus zur Gruppe KAVWSEE Administrators auf dem geschützten Server hinzufügen" auf S. 24).

BENUTZEROBERFLÄCHE DES KONSOLENFENSTERS VON KASPERSKY ANTI-VIRUS

Die Konsole von Kaspersky Anti-Virus wird in der Baumstruktur als Knoten mit dem Namen **Kaspersky Anti-Virus** angezeigt.

Nachdem eine Verbindung mit dem Programm Kaspersky Anti-Virus hergestellt wurde, das auf einem anderen Computer installiert ist, werden der Name des Computers, auf dem Kaspersky Anti-Virus installiert ist, sowie der Name des Benutzerkontos, mit dessen Rechten die Verbindung hergestellt wurde, zur Bezeichnung des Knotens hinzugefügt: **Kaspersky Anti-Virus <Computername> als <Name des Benutzerkontos>**. Wird eine Verbindung zum Programm Kaspersky Anti-Virus hergestellt, das auf demselben Computer installiert ist wie die Konsole für Kaspersky Anti-Virus, so ändert sich die Bezeichnung des Knotens nicht.

Standardmäßig enthält das Fenster der Konsole für Kaspersky Anti-Virus folgende Elemente:

- Konsolenstruktur
- Ergebnisfenster
- Schnellauswahlleiste
- Werkzeugleiste

Sie können außerdem die Beschreibungsleiste und den Aktionsbereich im Konsolenfenster für Kaspersky Anti-Virus aktivieren.

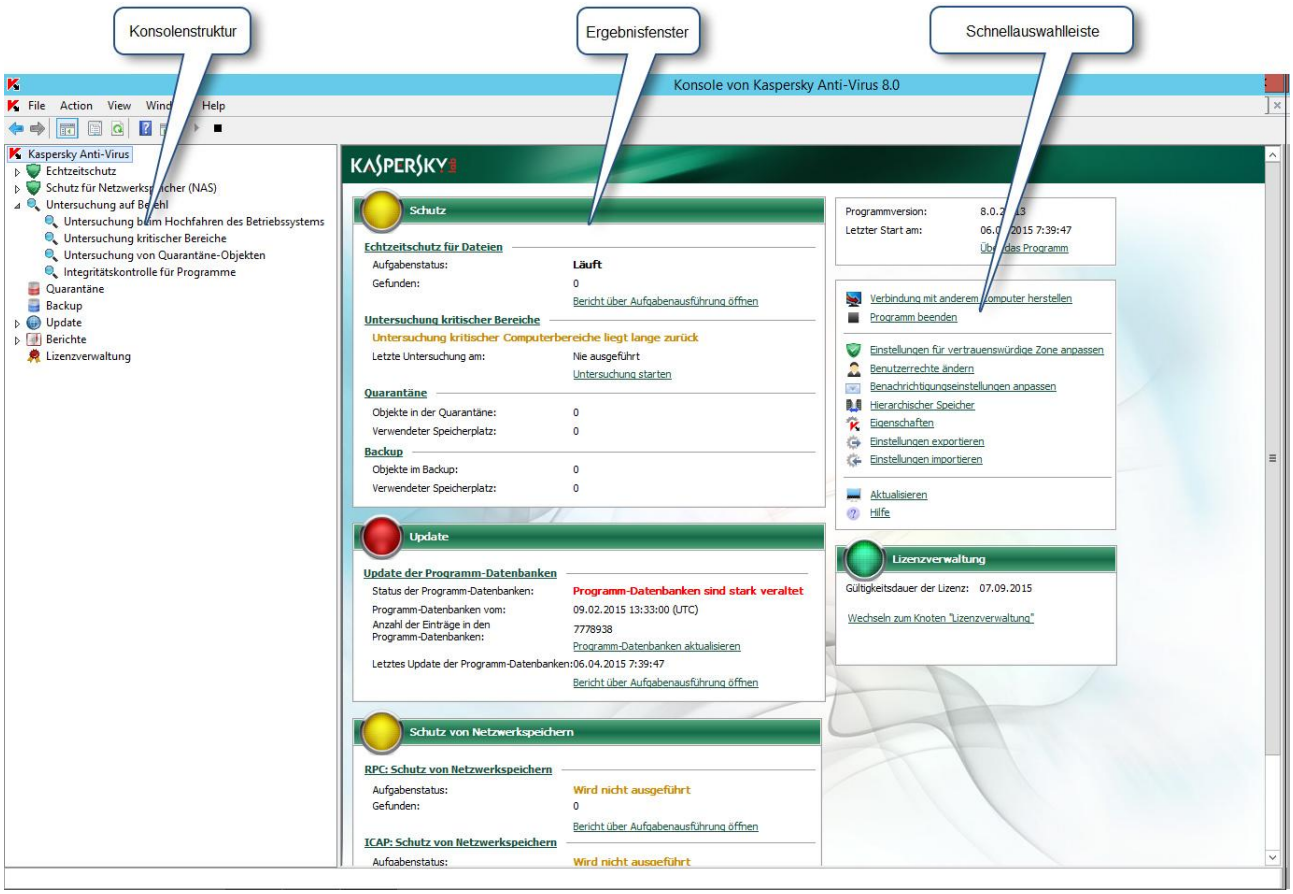


Abbildung 1: Hauptfenster der Konsole für Kaspersky Anti-Virus

Konsolenstruktur

Die Konsolenstruktur enthält einen Knoten für Kaspersky Anti-Virus und untergeordnete Knoten für die Programmkomponenten.

Der Knoten **Kaspersky Anti-Virus** enthält folgende untergeordneten Knoten:

- **Echtzeitschutz**: Verwalten des Echtzeitschutzes für Dateien und der Skript-Untersuchung. Jede Schutzkomponente hat ihr eigenes Steuerelement:
  - **Echtzeitschutz für Dateien**.
  - **Skript-Untersuchung**.
- **Schutz für Netzwerkspeicher (NAS)**: Verwaltung des Schutzes für Netzwerkspeicher.
  - **RPC: Schutz von Netzwerkspeichern**.
  - **ICAP: Schutz von Netzwerkspeichern**.
- **Untersuchung auf Befehl**: Verwalten der Aufgabe zur Virensuche. Jede Systemaufgabe hat ihr eigenes Steuerelement:
  - **Untersuchung beim Hochfahren des Betriebssystems**.
  - **Untersuchung kritischer Bereiche**.
  - **Untersuchung von Quarantäne-Objekten**.
  - **Integritätsprüfung des Programms**.

  Ein separates Steuerelement wird für jede benutzerdefinierte Aufgabe und für jede Gruppenaufgabe angelegt, der vom System der Remote-Verwaltung durch Kaspersky Security Center erstellt und an den Server weitergeleitet wird.
- **Quarantäne**: Verwaltung der Quarantäne-Einstellungen und Verwendung von in die Quarantäne verschobenen Objekten. Der Knoten enthält eine Liste mit den in diesen Speicher verschobenen Objekten.
- **Backup**: Verwalten der Parameter für das Backup und der dorthin verschobenen Objekte. Im Knoten steht eine Liste mit den Sicherungskopien von Objekten.
- **Update**: Verwaltung des Updates der Datenbanken und Programm-Module für Kaspersky Anti-Virus, sowie Verwaltung der Update-Verteilung (Speichern von Updates in einer lokalen Update-Quelle). Der Knoten enthält eingebettete Nodes für die Steuerung jeder Update-Systemaufgabe und für die Aufgabe Rollback des Programmdatenbank-Updates:
  - **Update der Programm-Datenbanken**.
  - **Update der Programm-Module**.
  - **Update-Verteilung**.
  - **Rollback des Datenbank-Updates**.

  Ein separates Steuerelement wird für jede Aufgabe angelegt, die vom System der Remote-Verwaltung durch Kaspersky Security Center erstellt und an den Server weitergeleitet wird.
- **Berichte**: Verwaltung von Berichten über die Aufgabenausführung für den Echtzeitschutz, den Schutz von Netzwerkspeichern, die Untersuchung auf Befehl und das Update; Verwaltung des Audit-Berichts von Kaspersky Anti-Virus.
- **Lizenzverwaltung**: Hinzufügen und Löschen von Schlüsseln für Kaspersky Anti-Virus, Anzeige von Informationen über Lizenzen.

Ergebnisfenster

Im Ergebnisfenster werden Informationen über den ausgewählten Knoten angezeigt. Wenn der Knoten für Kaspersky Anti-Virus ausgewählt wurde, wenden im Ergebnisfenster Daten über den aktuellen Schutzstatus des Servers, über Kaspersky Anti-Virus und den Zustand seiner Funktionskomponenten dargestellt.

Aufgabenfenster und Kontextmenü des Kaspersky Anti-Virus Knotens

Mithilfe der Links im Schnellzugriffsbereich und der Befehle des Kontextmenüs für den Knoten **Kaspersky Anti-Virus** können Sie folgende Vorgänge ausführen:

- **Verbindung mit anderem Computer herstellen** – Verbindung mit einem anderen Server herstellen, um Kaspersky Anti-Virus dort zu verwalten.
- **Programm starten bzw. beenden** – Kaspersky Anti-Virus starten bzw. beenden. Zur Ausführung dieser Vorgänge können Sie außerdem die Schaltflächen im Werkzeugfenster verwenden.

- **Einstellungen für vertrauenswürdige Zone anpassen** – vertrauenswürdige Prozesse und Ausnahmeregeln festlegen (s. Abschnitt "Ausnahmen zur vertrauenswürdigen Zone hinzufügen" auf S. 78). Zusätzlich können Sie die Aufgaben angeben, in denen die einzelnen Einstellungen der vertrauenswürdigen Zone gelten sollen.
- **Benutzerrechte ändern** – Berechtigungen für den Zugriff von Benutzern und Benutzergruppen auf die Funktionen von Kaspersky Anti-Virus ändern (s. Abschnitt "Rechte für den Zugriff auf die Funktionen von Kaspersky Anti-Virus anpassen" auf S. 31).
- **Benachrichtigungseinstellungen anpassen** – Einstellungen für Benachrichtigungen anpassen, mit denen Benutzer und Administratoren über Ereignisse in Kaspersky Anti-Virus informiert werden.
- **Hierarchischer Speicher** – Einstellungen für den hierarchischen Speicher anpassen.
- **Einstellungen exportieren** – Programmeinstellungen in eine Konfigurationsdatei im XML-Format exportieren (s. Abschnitt "Einstellungen exportieren" auf S. 110).
- **Einstellungen importieren** – Programmeinstellungen aus einer Konfigurationsdatei im XML-Format importieren (s. Abschnitt "Einstellungen importieren" auf S. 110).
- **Über das Programm** – Anzeige von Informationen über das Programm: Nummer der installierten Programmversion, Informationen über installierte Updates. Darüber hinaus können Sie zur Webseite von Kaspersky Lab und zur Webseite des Technischen Supports wechseln, sowie die Lizenzvereinbarung anzeigen.
- **Eigenschaften** - Anzeigen und Einstellen von allgemeinen Parametern für die Anti-Virus-Funktionen.

ZUGRIFFSRECHTE FÜR DIE FUNKTIONEN VON KASPERSKY ANTI-VIRUS

Standardmäßig haben die Benutzer der Gruppe "Administratoren" auf dem geschützten Server sowie die Benutzer der Gruppe KAVWSEE Administrators (s. Abschnitt "Benutzer von Kaspersky Anti-Virus zur Gruppe KAVWSEE Administrators auf dem geschützten Server hinzufügen" auf S. 24), die auf einem geschützten Server bei der Installation von Kaspersky Anti-Virus erstellt wird, Zugriff auf alle Funktionen von Kaspersky Anti-Virus.

Benutzer, die Zugriff auf diese Funktionen besitzen **Rechte ändern**, können den Zugriff auf Funktionen von Kaspersky Anti-Virus auch anderen Benutzern gewähren, die am geschützten Server angemeldet sind oder zur Domäne gehören.

Wenn ein Benutzer nicht in die Liste der Benutzer von Kaspersky Anti-Virus eingetragen ist, kann er die Konsole von Kaspersky Anti-Virus nicht öffnen.

Sie können für einen Benutzer oder eine Benutzergruppe von Kaspersky Anti-Virus eine der folgenden vordefinierten Stufen der Zugriffsberechtigung auf die Funktionen von Kaspersky Anti-Virus auswählen:

- **Vollständige Kontrolle** – Berechtigung zum Anzeigen und Ändern der allgemeinen Einstellungen für die Ausführung von Kaspersky Anti-Virus, der Einstellungen für die Komponenten von Kaspersky Anti-Virus, der Benutzerrechte von Kaspersky Anti-Virus sowie zum Anzeigen der Statistik der Programmausführung von Kaspersky Anti-Virus.
- **Änderung** – Berechtigung zum Anzeigen und Ändern der allgemeinen Einstellungen für die Ausführung von Kaspersky Anti-Virus, der Einstellungen für die Komponenten von Kaspersky Anti-Virus sowie zum Anzeigen der Statistik der Programmausführung von Kaspersky Anti-Virus und der Benutzerrechte von Kaspersky Anti-Virus.
- **Lesen** – Berechtigung zum Anzeigen der allgemeinen Einstellungen für die Ausführung von Kaspersky Anti-Virus, der Einstellungen für die Komponenten von Kaspersky Anti-Virus, der Statistik der Programmausführung von Kaspersky Anti-Virus und der Benutzerrechte von Kaspersky Anti-Virus.

Außerdem können Sie erweiterte Einstellungen für die Zugriffsrechte vornehmen (s. Abschnitt "Rechte für den Zugriff auf die Funktionen von Kaspersky Anti-Virus anpassen" auf S. 31): Zugriff auf die einzelnen Funktionen von Kaspersky Anti-Virus erlauben oder verbieten (s. Tabelle unten).

Tabelle 3. Beschränkung der Zugriffsrechte für die Funktionen von Kaspersky Anti-Virus

FUNKTION	BESCHREIBUNG
Aufgabenverwaltung	Berechtigung zum Starten, Beenden, Anhalten bzw. Fortsetzen der Aufgaben von Kaspersky Anti-Virus.
Erstellen und Löschen von Aufgaben	Berechtigung zum Erstellen und Löschen von Aufgabe zur Untersuchung auf Befehl.
Ändern von Parametern	Berechtigungen: • Allgemeine Einstellungen von Kaspersky Anti-Virus anzeigen und ändern • Einstellungen von Kaspersky Anti-Virus aus einer Konfigurationsdatei importieren bzw. in eine Konfigurationsdatei exportieren • Aufgabeneinstellungen anzeigen und ändern • Einstellungen für Berichte über die Aufgabenausführung, für den Systemaudit-Bericht und für Benachrichtigungen anzeigen und ändern.
Lesen von Parametern	Berechtigungen: • Allgemeine Einstellungen von Kaspersky Anti-Virus und Aufgabeneinstellungen anzeigen • Einstellungen von Kaspersky Anti-Virus in eine Konfigurationsdatei exportieren • Einstellungen für Berichte über die Aufgabenausführung, für den Systemaudit-Bericht und für Benachrichtigungen anzeigen
Verwalten von Quarantäne und Backup	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 die Aufgabenausführung und zum Leeren des Systemaudit-Berichts
Lesen von Berichten	Berechtigung zur Anzeige von Ereignissen in Berichten über die Aufgabenausführung und im Systemaudit-Bericht
Lesen der Statistik	Berechtigung zur Anzeige der Statistik über die Ausführung von Kaspersky Anti-Virus
Lizenzierung des Programms	Berechtigung zum Hinzufügen und Löschen von Schlüsseln zu Kaspersky Anti-Virus
Lesen von Benutzerrechten	Berechtigung zum Anzeigen von Benutzerlisten von Kaspersky Anti-Virus und der Zugriffsberechtigungen der einzelnen Benutzer
Ändern von Rechten	Berechtigungen: • Benutzer von Kaspersky Anti-Virus hinzufügen und löschen • Zugriffsberechtigungen von Benutzern für die Funktionen von Kaspersky Anti-Virus ändern

RECHTE FÜR DEN ZUGRIFF AUF DIE FUNKTIONEN VON KASPERSKY ANTI-VIRUS ANPASSEN

Um einen Benutzer (eine Gruppe) hinzuzufügen oder zu löschen oder die Zugriffsberechtigungen eines Benutzers (einer Gruppe) für die Funktionen von Kaspersky Anti-Virus zu ändern, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü des Knotens von Kaspersky Anti-Virus und wählen Sie **Benutzerrechte ändern** aus.

   Das Fenster **Berechtigungen für die Gruppe "Kaspersky Anti-Virus"** wird geöffnet.

2. Gehen Sie im Fenster **Berechtigungen für Kaspersky Anti-Virus** wie folgt vor:

   - Um der Benutzerliste für Kaspersky Anti-Virus einen Benutzer (eine Gruppe) hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie die entsprechenden Benutzer oder Gruppen aus.
   - Um einem hinzugefügten Benutzer (einer Gruppe) Zugriffsrechte für die Funktionen von Kaspersky Anti-Virus zu gewähren, wählen Sie in der Liste **Benutzer oder Gruppe** einen Benutzer (eine Gruppe) aus und aktivieren Sie im Block **Berechtigungen für die Gruppe "<Benutzer (Gruppe)>"** das Kontrollkästchen **Erlauben** für die folgenden Zugriffsberechtigungen:
     - **Vollständige Kontrolle**, um den Zugriff auf alle Funktionen von Kaspersky Anti-Virus zu gewähren.
     - **Lesen**, um den Zugriff auf die Funktionen **Statistik lesen**, **Einstellungen lesen**, **Berichte lesen** und **Rechte lesen** zu gewähren.
     - **Änderung**, um den Zugriff auf alle Funktionen von Kaspersky Anti-Virus zu gewähren, außer der Funktion **Rechte ändern**.
   - Um die Rechte (Sonderrechte) ausführlich anzupassen, klicken Sie auf die Schaltfläche **Erweitert**.

     Wählen Sie im Fenster **Erweiterte Sicherheitseinstellungen für Kaspersky Anti-Virus** den erforderlichen Benutzer oder die entsprechende Gruppe und klicken Sie auf die Schaltfläche **Ändern**. Aktivieren Sie dann im Fenster **Erlaubniselement für Kaspersky Anti-Virus** das Kontrollkästchen **Erlauben** oder **Verbieten** neben der Funktion, auf die Sie den Zugriff erlauben oder verbieten möchten (s. Abschnitt "Zugriffsrechte für die Funktionen von Kaspersky Anti-Virus" auf S. 29). Klicken Sie auf **OK**.

3. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

KASPERSKY ANTI-VIRUS-SYMBOL IM INFOBEREICH DER TASKLEISTE

Jedes Mal, wenn Kaspersky Anti-Virus nach dem Neustart des Servers automatisch gestartet wird, erscheint im Infobereich der Taskleiste das Kaspersky Anti-Virus-Symbol angezeigt. Es wird standardmäßig angezeigt, wenn Sie bei der Installation des Programms die Komponente **Kaspersky Anti-Virus-Symbol** installiert haben.

Das Kaspersky Anti-Virus-Symbol kann folgende Zustände annehmen:

- Aktiv (farbiges Symbol), wenn gerade eine der Aufgaben **Echtzeitschutz für Dateien** oder **Skript-Untersuchung** ausgeführt wird (s. S. 52).

- Inaktiv (schwarzweißes Symbol), wenn momentan keine Aufgaben des **Echtzeitschutz für Dateien**, des **Skript-Untersuchung** und der Skript-Untersuchung ausgeführt werden.

Sie können das Kontextmenü des Symbols von Kaspersky Anti-Virus mit der rechten Maustaste öffnen.

Das Kontextmenü enthält mehrere Befehle, die zur Anzeige der Programmfenster dienen (s. Tabelle unten).

Tabelle 4. Befehle im Kontextmenü des Kaspersky Anti-Virus-Symbols

BEFEHL	BESCHREIBUNG
Konsole für Kaspersky Anti-Virus öffnen	Der Befehl öffnet die Konsole von Kaspersky Anti-Virus (falls installiert).
Über das Programm	Dieser Befehl öffnet das Fenster **Über das Programm** mit Informationen zu Kaspersky Anti-Virus. Wenn Sie als Benutzer von Kaspersky Anti-Virus registriert sind, enthält das Fenster **Über das Programm** Informationen über die installierten kritischen Updates.
Ausblenden	Kaspersky Anti-Virus-Symbol aus dem Infobereich der Taskleiste ausblenden. Um das Programmsymbol wieder anzuzeigen, wählen Sie im **Startmenü** den Punkt **Programme → Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Kaspersky Anti-Virus-Symbol**.

Unter Anpassen der allgemeinen Einstellungen für Kaspersky Anti-Virus können Sie festlegen, ob das Anti-Virus-Symbol angezeigt werden soll oder nicht, wenn das Programm nach einem Neustart des Servers automatisch gestartet wird (s. Abschnitt "Anpassen der allgemeinen Einstellungen von Kaspersky Anti-Virus in der Konsole von Kaspersky Anti-Virus" auf S. 36).

SCHUTZSTATUS UND INFORMATIONEN ÜBER KASPERSKY ANTI-VIRUS ANZEIGEN

- *Um Informationen über den Schutzstatus des Servers, der geschützten Netzwerkspeicher und Informationen über Kaspersky Anti-Virus anzuzeigen,*

  wählen Sie in der Konsolenstruktur den Knoten Kaspersky Anti-Virus.

Standardmäßig werden die Informationen im Ergebnisfeld der Konsole von Kaspersky Anti-Virus automatisch jede Minute aktualisiert. Sie können die Informationen auch manuell aktualisieren.

- *Und die Informationen im Knoten Kaspersky Anti-Virus manuell zu aktualisieren,*

  wählen Sie im Kontextmenü des Knotens Kaspersky Anti-Virus den Befehl **Aktualisieren**.

Im Ergebnisfenster der Konsole von Kaspersky Anti-Virus werden Informationen über den Schutzstatus des Servers, der geschützten Netzwerkspeicher sowie Informationen über Kaspersky Anti-Virus angezeigt (s. Tabelle unten).

Tabelle 5. Informationen über den Schutzstatus des Servers

BLOCK "SCHUTZ"	INFORMATIONEN
Statusanzeige für den Schutz des Servers	Der Indikator kann die folgende Form annehmen:  – die Aufgaben zum Echtzeitschutz von Dateien und zur Skript-Untersuchung werden ausgeführt, die Aufgabe zur Untersuchung kritischer Bereiche wurde vor weniger als 30 Tagen abgeschlossen (Standard);  – eine oder mehrere Aufgaben zum Echtzeitschutz wurden nicht gestartet, beendet oder das Ereignis *Untersuchung kritischer Computerbereiche liegt lange zurück* wurde ausgelöst  – Eine oder mehrere Aufgaben zum Echtzeitschutz wurden fehlerhaft abgeschlossen.
Echtzeitschutz für Dateien	**Aufgabenstatus** – aktueller Status der Aufgabe (zum Beispiel, *Wird ausgeführt* oder *Beendet*). **Gefunden** –Anzahl der Objekte, die Kaspersky Anti-Virus gefunden hat. Findet Kaspersky Anti-Virus beispielsweise in fünf Dateien ein und dasselbe Schadprogramm, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Skript-Untersuchung	**Aufgabenstatus** – aktueller Status der Aufgabe (zum Beispiel, *Wird ausgeführt* oder *Beendet*). **Gefundene gefährliche Skripte** – Anzahl der gefährlichen Skripte, die Kaspersky Anti-Virus seit dem Aufgabenstart gefunden hat.
Untersuchung kritischer Bereiche	*Untersuchung wichtiger Bereiche liegt lange zurück* – Ereignis, das auftritt, wenn die Untersuchungsaufgabe für wichtige Bereiche seit als 30 Tagen oder länger nicht ausgeführt wurde (Standard). Sie können den Grenzwert für die Auslösung dieses Ereignisses ändern. **Letzte Untersuchung am** – Datum und Uhrzeit der letzten Untersuchung der wichtigen Bereiche des Computers auf das Vorhandensein von Viren und anderen Bedrohungen der Computersicherheit.
Quarantäne	*Der Grenzwert für verfügbaren Speicherplatz in der Quarantäne wurde überschritten* – Ereignis, das auftritt, wenn der Grenzwert für den verfügbaren Speicherplatz in der Quarantäne den angegebenen Wert erreicht. Kaspersky Anti-Virus wird dabei weiterhin Objekte in die Quarantäne verschieben. *Die maximale Größe der Quarantäne wurde überschritten* – Ereignis, das auftritt, wenn die Größe der Quarantäne den angegebenen Wert erreicht hat. Kaspersky Anti-Virus wird dabei weiterhin Objekte in die Quarantäne verschieben. **Objekte in der Quarantäne** – Anzahl der Objekte, die sich momentan in der Quarantäne befinden. **Verwendeter Speicherplatz** – Volumen des verwendeten Speicherplatzes in der Quarantäne.
Backup	*Der Grenzwert für verfügbaren Speicherplatz im Backup wurde überschritten* – Ereignis, das auftritt, wenn der Grenzwert für den verfügbaren Speicherplatz im Backup den angegebenen Wert erreicht. Kaspersky Anti-Virus wird dabei weiterhin Objekte in das Backup verschieben. *Die maximale Größe des Backups wurde überschritten* – Ereignis, das auftritt, wenn die Größe des Backups den angegebenen Wert erreicht. Kaspersky Anti-Virus wird dabei weiterhin Objekte in das Backup verschieben. **Objekte im Backup** – Anzahl der Objekte, die sich momentan im Backup befinden. **Verwendeter Speicherplatz** – Volumen des verwendeten Speicherplatzes im Backup.

Tabelle 6. Informationen über den Zustand der Datenbanken und Module von Kaspersky Anti-Virus

BLOCK UPDATE	INFORMATIONEN
Statusindikator für Datenbanken und Programm-Module	Der Indikator kann die folgende Form annehmen:  – Programm-Datenbanken sind aktuell. Es sind keine kritischen Updates für Programm-Module verfügbar.  – Eines der folgenden Ereignisse ist eingetreten: *Programm-Datenbanken sind veraltet*, *Wichtiges Update für Programm-Module verfügbar*, *Rückruf eines wichtigen Updates der Programm-Module wurde angekündigt*, *Um die Aktualisierung der Programm-Module abzuschließen, muss der Computer neu gestartet werden*.  – Das Ereignis *Datenbanken sind stark veraltet* oder *Datenbanken sind beschädigt* ist eingetreten.
Update der Programm-Datenbanken	**Status der Programm-Datenbanken** – Bewertung der Aktualität der Programm-Datenbanken. Folgende Werte sind möglich: • **Programm-Datenbanken sind aktuell** – Die Programm-Datenbanken wurden vor höchstens 7 Tagen aktualisiert (Standard) • **Programm-Datenbanken sind veraltet** – Die Programm-Datenbanken wurden zuletzt vor 7–14 Tagen aktualisiert (Standard). • **Programm-Datenbanken sind stark veraltet** – Die Programm-Datenbanken wurden zuletzt vor mehr als 14 Tagen aktualisiert (Standard). Sie können die Grenzwerte für die Auslösung der Ereignisse *Programm-Datenbanken sind veraltet* und *Programm-Datenbanken sind stark veraltet* ändern. **Programm-Datenbanken vom** – Datum und Uhrzeit, zu dem die zuletzt installierten Updates der Programm-Datenbanken erschienen sind. Datum und Uhrzeit werden in UTC angegeben. **Anzahl der Einträge in den Programm-Datenbanken** – Anzahl der Einträge über Bedrohungen in den installierten Programm-Datenbanken. **Letztes Update der Programm-Datenbanken** – Datum und Uhrzeit der letzten Aktualisierung der Programm-Datenbanken. Datum und Uhrzeit werden in der lokalen Zeit des geschützten Servers angegeben.

Tabelle 7. Informationen zur Lizenzierung von Kaspersky Anti-Virus

BLOCK LIZENZIERUNG	INFORMATIONEN
Statusindikator der Lizenz	Der Indikator kann die folgende Form annehmen:  – Die Lizenz ist gültig, bis zum Ablauf der Gültigkeitsdauer der Lizenz verbleiben mehr als 14 Tage.  – Die verbliebene Gültigkeitsdauer der Lizenz beträgt 14 Tage oder weniger.  – Die Gültigkeitsdauer der Lizenz ist abgelaufen. Das Programm ist nicht aktiviert (es wurde kein Schlüssel hinzugefügt). Die Bedingungen des Lizenzvertrags wurden verletzt (z. B. weil der Schlüssel auf der schwarzen Schlüsselliste steht).
Gültigkeitsdauer der Lizenz	Ablaufdatum der mit dem aktiven Schlüssel verknüpften Lizenz. Wenn ein Reserveschlüssel hinzugefügt wurde, wird als Ablaufdatum der Lizenz das Ablaufdatum des Reserveschlüssels angegeben.

Der Block **Schutz von Netzwerkspeichern** (s. Tabelle unten) wird angezeigt, wenn der aktive Schlüssel die Funktion zum Schutz von Netzwerkspeichern unterstützt.

Tabelle 8. Informationen zum Schutz von Netzwerkspeichern

BLOCK SCHUTZ VON NETZWERKSPEICHERN	INFORMATIONEN
Statusanzeige für den Schutz von Netzwerkspeichern	Der Indikator kann die folgende Form annehmen:  – In folgenden Fällen: • Mindestens eine der folgenden Aufgaben ist gestartet: **RPC: Schutz von Netzwerkspeichern** oder **ICAP: Schutz von Netzwerkspeichern** • Kaspersky Anti-Virus hat eine Verbindung zum Softwareprogramm der Firma EMC hergestellt, und in Kaspersky Anti-Virus wird die Aufgabe zum Echtzeitschutz von Dateien ausgeführt.  – in allen anderen Fällen.
EMC Celerra-Integrationsstatus	Folgende Werte sind möglich: • **Celerra Anti Virus Agent wurde nicht gefunden** – Kaspersky Anti-Virus konnte keine Software der Firma EMC finden oder es ist ein Fehler im Integrationscode aufgetreten. • **Der Schutz ist aktiviert** – Kaspersky Anti-Virus hat eine Verbindung zum Softwareprogramm der Firma EMC installiert, aber in Kaspersky Anti-Virus wird die Aufgabe zum Echtzeitschutz von Dateien nicht ausgeführt. • **Der Schutz ist aktiviert** – Kaspersky Anti-Virus hat eine Verbindung zum Softwareprogramm der Firma EMC hergestellt, und in Kaspersky Anti-Virus wird die Aufgabe zum Echtzeitschutz von Dateien ausgeführt.

Detaillierte Informationen und Anweisungen zum Schutz von Netzwerkspeichern mithilfe von Kaspersky Anti-Virus finden Sie im *Handbuch für die Implementierung von Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition zum Schutz von Netzwerkspeichern*.

ANPASSEN DER ALLGEMEINEN EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS IN DER KONSOLE VON KASPERSKY ANTI-VIRUS

Die allgemeinen Einstellungen von Kaspersky Anti-Virus legen die generellen Bedingungen für die Ausführung von Kaspersky Anti-Virus fest. Dazu gehören folgende Einstellungen: Anzahl der aktiven Prozesse, die von Kaspersky Anti-Virus verwendet werden; Wiederherstellung von Anti-Virus-Aufgaben nach einem Absturz von Aufgaben aktivieren; Führen eines Berichts zur Ablaufverfolgung; Anlegen von Speicher-Dumps für Prozesse von Kaspersky Anti-Virus bei deren Absturz; Anzeige des Anti-Virus-Symbol, wenn Kaspersky Anti-Virus nach dem Neustart des Servers automatisch neu gestartet wird; sowie andere allgemeine Einstellungen.

IN DIESEM ABSCHNITT

ANPASSEN DER ALLGEMEINEN EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS IN DER KONSOLE VON KASPERSKY ANTI-VIRUS

Um die allgemeine Einstellungen von Kaspersky Anti-Virus anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü des Knotens **Kaspersky Anti-Virus** und wählen Sie den Befehl **Eigenschaften**.

   Das Fenster **Eigenschaften: Kaspersky Anti-Virus** wird geöffnet.

2. Legen Sie im nächsten Fenster die allgemeinen Einstellungen von Kaspersky Anti-Virus gemäß Ihren Anforderungen fest.

   - Auf der Registerkarte **Allgemein** können Sie folgende Einstellungen anpassen:

     Im Block **Skalierbarkeits-Einstellungen**:

     - Maximale Anzahl der aktiven Prozesse, die von Kaspersky Anti-Virus gestartet werden können
     - Festgelegte Anzahl der Prozesse für Echtzeitschutz-Aufgaben
     - Anzahl der aktiven Prozesse für im Hintergrund laufende Aufgaben zur Untersuchung auf Befehl

     Im Block **Einstellungen für Zuverlässigkeit**:

     - Anzahl der Versuche zur Wiederherstellung von Aufgaben nach deren Absturz
   - Auf der Registerkarte **Erweitert** können Sie folgende Einstellungen anpassen:

     Im Block **Interaktion mit dem Benutzer**:

     - Anzeige des Kaspersky Anti-Virus-Symbols im Infobereich der Taskleiste (s. S. 32) bei jedem Start des Programms

     Im Block **Verwendung einer unterbrechungsfreien Stromversorgungsquelle**:

     - Aktionen von Kaspersky Anti-Virus bei der Nutzung einer unterbrechungsfreien Stromversorgungsquelle

Im Block **Grenzwerte für Ereignisdarstellung**:

- Anzahl der Tage fest, nach deren Ablauf die Ereignisse *Datenbanken sind veraltet*, *Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche des Computers liegt lange zurück* eintreten sollen

- Auf der Registerkarte **Crash-Diagnose** gehen Sie wie folgt vor:
  - Aktivieren oder deaktivieren Sie die Protokollierung von Debug-Informationen in einer Datei. Passen Sie die Einstellungen des Berichts erforderlichenfalls an.
  - Aktivieren oder deaktivieren Sie die Erstellung von Dump-Dateien für Kaspersky Anti-Virus-Prozesse.

Informationen in Speicherdump- und Protokolldateien werden von Kaspersky Anti-Virus im Klartext aufgezeichnet.

3. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Änderungen zu speichern.

AUFGABENVERWALTUNG

Dieser Abschnitt enthält Informationen über die Aufgaben von Kaspersky Anti-Virus, ihre Erstellung, die Festlegung der Einstellungen für ihre Ausführung, den Start und das Beenden von Aufgaben sowie die Anpassung der Einstellungen für den automatischen Start und das automatische Anhalten von Aufgaben nach Zeitplan.

IN DIESEM ABSCHNITT

ERSTELLEN EINER AUFGABE ZUR VIRENSUCHE

Sie können im Knoten **Untersuchung auf Befehl** benutzerdefinierte Aufgaben erstellen. In den anderen funktionellen Kaspersky Anti-Virus-Komponenten ist das Erstellen von benutzerdefinierten Aufgaben nicht vorgesehen.

Um eine neue Aufgabe zur Virensuche zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü des Knotens **Untersuchung auf Befehl** und wählen Sie den Befehl **Aufgabe hinzufügen** aus.

   Das Fenster **Aufgabe hinzufügen** wird geöffnet.

2. Tragen Sie folgende Informationen über die Aufgabe ein:

   - **Name** – Aufgabenname, maximal 100 Zeichen, kann aus beliebigen Zeichen bestehen, mit Ausnahme von **% ? I \ | / : * < >.**
   - **Beschreibung** – beliebige Zusatzinformationen über die Aufgabe, maximal 2000 Zeichen. Diese Informationen werden im Fenster Eigenschaften der Aufgabe angezeigt.

3. Bei Bedarf können Sie folgende Parameter anpassen:

   - Verwendung der heuristischen Analyse In neu erstellten Aufgaben zur Untersuchung auf Befehl wird die heuristische Analyse standardmäßig verwendet. Um die Analysetiefe zu ändern, vergewissern Sie sich, dass das Häkchen im Kontrollkästchen **Heuristische Analyse verwenden** gesetzt ist und verschieben Sie den Schieberegler in die gewünschte Stellung. Um die heuristische Analyse auszuschalten, entfernen Sie das Häkchen im Kontrollkästchen **Heuristische Analyse verwenden**.
   - Vertrauenswürdige Zone übernehmen (s. S. 77). In neu erstellten Aufgaben zum On-Demand-Scan wird die vertrauenswürdige Zone standardmäßig verwendet. Um ihre Verwendung zu deaktivieren, entfernen Sie das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.
   - Ausführung einer Aufgabe im Hintergrundmodus (s. S. 75). Damit eine Aufgabe in einem Prozess mit niedriger Priorität ausgeführt wird, aktivieren Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**.

4. Klicken Sie auf **OK**. Die Aufgabe wird angelegt. Im Fenster der Konsole erscheint eine Zeile mit den entsprechenden Angaben. Der Vorgang wird im Bericht zum System-Audit (s. S. 95) festgehalten.

SPEICHERN EINER AUFGABE NACH DEM ÄNDERN VON PARAMETERN

Sie können die Parameter einer laufenden und beendeten (angehaltenen) Aufgabe ändern. Die neuen Parameterwerte treten unter folgenden Bedingungen in Kraft:

- Wenn Sie die Einstellungen einer laufenden Aufgabe geändert haben: Die neuen Einstellungswerte werden sofort nach dem Speichern wirksam. In den übrigen Aufgaben werden Änderungen beim nächsten Aufgabenstart übernommen.
- Wenn Sie die Parameter einer beendeten Aufgabe geändert haben: Dann werden die neuen Parameterwerte wirksam, nachdem Sie die Änderungen gespeichert und die Aufgabe gestartet haben.

Um geänderte Aufgabenparameter zu speichern, öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**.

Wenn Sie die Parameter einer Aufgabe geändert haben und einen anderen Knoten der Konsolenstruktur wählen, ohne vorher den Befehl **Aufgabe speichern** gegeben zu haben, erscheint ein Fenster zum Speichern von Parametern. Klicken Sie dort auf die Schaltfläche **Ja**, um die Aufgabenparameter zu Speichern, oder auf **Nein**, und den Knoten ohne Speichern zu verlassen.

Sie können die Parameter für jede der folgenden Aufgaben konfigurieren: Echtzeitschutz für Dateien (s. Abschnitt "Anpassen der Aufgabe "Echtzeitschutz für Dateien" auf S. 52), Schutz von Netzwerkspeichern, Virensuche ("Anpassen von Aufgaben zur Virensuche" auf S. 66), Update (s. S. 47).

UMBENENNEN EINER AUFGABE

In der Konsole von Kaspersky Anti-Virus können nur benutzerdefinierte Aufgaben umbenannt werden. System- oder Gruppenaufgaben können nicht umbenannt werden.

Um eine Aufgabe umzubenennen, gehen Sie wie folgt vor:

1. Öffnen Sie das Kontextmenü durch Rechtsklick auf einen Aufgabenname und wählen Sie den Befehl **Eigenschaften**.
2. Geben Sie im Fenster **Eigenschaften: <Aufgabenname>** im Feld **Name** einen neuen Aufgabennamen an und klicken Sie auf **OK** oder **Übernehmen**.

   Die Aufgabe wird umbenannt. Der Vorgang wird im Bericht zum System-Audit (s. S. 95) festgehalten.

LÖSCHEN EINER AUFGABE

Sie können in der Konsole von Kaspersky Anti-Virus nur benutzerdefinierte Aufgaben löschen, Systemaufgaben und Gruppenaufgaben lassen sich nicht löschen.

Um eine Aufgabe zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie das Kontextmenü durch Rechtsklick auf einen Aufgabennamen und wählen Sie den Befehl **Aufgabe löschen**.
2. Klicken Sie im folgenden Fenster auf die Schaltfläche **Ja**, um die Operation zu bestätigen.

Die Aufgabe wird gelöscht und der Löschvorgang wird im Bericht zum System-Audit (s. S. 95) festgehalten.

MANUELLES STARTEN / ANHALTEN / FORTSETZEN / BEENDEN EINER AUFGABE

Sie können alle Aufgaben anhalten und fortsetzen, ausgenommen sind Update-Aufgaben.

Um eine Aufgabe zu starten / anzuhalten / fortzusetzen / zu beenden,

öffnen Sie das Kontextmenü durch Rechtsklick auf einen Aufgabenamen und wählen Sie den entsprechenden Befehl: **Starten**, **Anhalten**, **Fortsetzen** oder **Beenden**.

Die Operation wird ausgeführt. Im Ergebnisfenster ändert sich der Status der Aufgabe. Der Vorgang wird im Bericht zum System-Audit (s. S. 95) festgehalten.

Wenn Sie eine Untersuchungsaufgabe anhalten und später fortsetzen, setzt Kaspersky Anti-Virus die Untersuchung bei dem Objekt fort, bei dem die Aufgabe angehalten wurde.

ARBEIT MIT DEM AUFGABENZEITPLAN

Sie können den Zeitplan für den Start von Aufgaben von Kaspersky Anti-Virus ändern.

IN DIESEM ABSCHNITT

START NACH ZEITPLAN AKTIVIEREN UND DEAKTIVIEREN

Nachdem Sie den Zeitplan für den Start von Aufgaben angepasst haben, können Sie ihn aktivieren oder deaktivieren. Wenn Sie einen Zeitplan deaktivieren, werden seine Werte (Startintervall, Startzeit usw.) nicht gelöscht, und Sie können den Zeitplan bei Bedarf erneut aktivieren.

➧ *Um die den Zeitplan für den Start von Aufgaben zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Kontextmenü für den Namen der Aufgabe, deren Startzeitplan angepasst werden soll, und wählen Sie **Eigenschaften**.
2. Gehen Sie im Fenster **Eigenschaften: <Aufgabenname>** auf der Registerkarte **Zeitplan** nach einer der folgenden Methoden vor:
   - Um den Zeitplan zu aktivieren, kreuzen Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten** an.
   - Um den Zeitplan zu deaktivieren, entfernen Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.
3. Klicken Sie auf **OK** oder **Übernehmen**.

ZEITPLANEINSTELLUNGEN FÜR DEN START VON AUFGABEN IN DER KONSOLE VON KASPERSKY ANTI-VIRUS ANPASSEN

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

Beachten Sie auch die Beschreibung der Zeitplaneinstellungen für Aufgaben.

➧ *Um die Zeitplaneinstellungen für den Start von Aufgaben zu konfigurieren,* gehen Sie wie folgt vor*:*

1. Öffnen Sie das Kontextmenü für den Namen der Aufgabe, deren Zeitplan angepasst werden soll, und wählen Sie **Eigenschaften**.
2. Aktivieren Sie im Fenster **Eigenschaften: <Aufgabenname>** auf der Registerkarte **Zeitplan** den geplanten Aufgabenstart: Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.

   Die Felder mit den Zeitplaneinstellungen der Aufgabe zum On-Demand-Scan und der Update-Aufgabe stehen nicht zur Verfügung, wenn deren Start durch eine Richtlinie des Programms Kaspersky Security Center untersagt ist (s. Abschnitt "Zeitgesteuerten Start für lokale Systemaufgaben deaktivieren" auf S. 145).
3. Passen Sie die Zeitplaneinstellungen entsprechend an. Gehen Sie hierzu wie folgt vor*:*
   a. Legen Sie eine Frequenz für den Aufgabenstart fest: Wählen Sie aus der Liste **Startintervall** einen der folgenden Werte aus: **Stündlich**, **Täglich**, **Wöchentlich**, **Bei Programmstart**, **Nach dem Update der Programm-Datenbanken**: Geben sie die folgenden Parameter an:
      - 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 werden soll (Standardmäßig wird eine Aufgabe montags gestartet).

b. Legen Sie im Feld **Start** 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 **Eigenschaften: <Aufgabenname>** 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 geltenden Richtlinie des Programms Kaspersky Security Center (s. Abschnitt "Zeitgesteuerten Start für lokale Systemaufgaben deaktivieren" auf S. 145) verboten ist.

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

a. Um eine maximale Dauer für die Aufgabenausführung anzugeben, legen Sie in der Gruppe **Einstellungen für das Anhalten der Aufgabe** im Feld **Dauer** die entsprechende Dauer in Stunden und Minuten fest.

b. Um einen Zeitraum innerhalb von 24 Stunden anzugeben, während dem die Aufgabe angehalten wird, geben Sie in der Gruppe **Einstellungen für das Anhalten der Aufgabe** im Feld **Anhalten von... bis** den Beginn und das Ende des Zeitintervalls an.

c. Um ein Datum anzugeben, ab dem der Zeitplan ungültig wird, aktivieren Sie das Kontrollkästchen **Zeitplan deaktivieren ab** und wählen Sie mithilfe des Fensters **Kalender** das Datum aus, ab dem der Zeitplan ungültig werden soll.

d. Um den Start von übersprungenen Aufgaben zu aktivieren, aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

e. Damit der Parameter "Startzeit für Aufgaben verteilen auf ein Intervall von ... Min" verwendet wird, aktivieren Sie das Kontrollkästchen **Startzeit verteilen auf ein Intervall von** und geben Sie den Wert des Parameters in Minuten an.

5. Klicken Sie auf **Übernehmen**, um die Änderungen im Fenster **Eigenschaften:<Aufgabenname>** zu speichern.

VERWENDUNG VON BENUTZERKONTEN FÜR DEN AUFGABENSTART

Sie können Aufgaben starten, indem Sie Systembenutzerkonto verwenden oder ein anderes Benutzerkonto angeben.

IN DIESEM ABSCHNITT

VERWENDUNG EINES BENUTZERKONTOS FÜR DEN AUFGABENSTART

Sie können ein Benutzerkonto angeben, mit dessen Berechtigungen eine bestimmte Aufgabe gestartet werden soll. Dies gilt für alle funktionellen Komponenten von Kaspersky Anti-Virus mit Ausnahme der Komponenten **Echtzeitschutz für Dateien**, **Skript-Untersuchung** und **Schutz von Netzwerkspeichern**.

In der Standardeinstellung werden alle Aufgaben, mit Ausnahme von Aufgaben des Echtzeitschutzes für Dateien und der Skript-Untersuchung sowie des Schutzes von Netzwerkspeichern, unter dem Benutzerkonto **Lokales System** (**SYSTEM**) ausgeführt. Bei den Aufgaben des Echtzeitschutzes fängt Kaspersky Anti-Virus das zu untersuchende Objekt ab, wenn eine Anwendung darauf zugreift, und verwendet für den Zugriff auf das Objekt die Rechte dieser Anwendung.

In folgenden Fällen müssen Sie ein anderes Benutzerkonto mit ausreichenden Zugriffsrechten angeben:

- in der Update-Aufgabe, wenn Sie als Update-Quelle einen gemeinsamen Ordner auf einem anderen Netzwerkcomputer angegeben haben.
- in der Update-Aufgabe, wenn für Zugriff auf die Update-Quelle ein Proxyserver mit integrierter Authentizitätsprüfung von Microsoft Windows verwendet wird (NTLM-authentication).
- in Aufgaben zur Virensuche, wenn das Benutzerkonto **Lokales System** (**SYSTEM**) keine Zugriffsrechte für die zu untersuchenden Objekte besitzt (zum Beispiel für die Dateien in gemeinsamen Netzwerkordnern).

Sie können unter dem Benutzerkonto **Lokales System** (**SYSTEM**) Update- und Untersuchungsaufgaben starten, in denen Kaspersky Anti-Virus auf gemeinsame Ordner eines anderen Netzwerkcomputers zugreift, wenn dieser Computer in der gleichen Domäne angemeldet ist wie der geschützte Server. In diesem Fall muss das Benutzerkonto **Lokales System** (**SYSTEM**) Zugriffsrechte für diese Ordner besitzen. Kaspersky Anti-Virus wird mit den Rechten des Benutzerkontos **Domänennamen\Computername$** auf den Computer zugreifen.

FESTLEGEN EINES BENUTZERKONTOS FÜR DEN AUFGABENSTART

Um ein Benutzerkonto für den Aufgabenstart festzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie das Kontextmenü durch Rechtsklick auf einen Aufgabenname und wählen Sie den Befehl **Eigenschaften**.
2. Öffnen Sie im Fenster **Eigenschaften: <Aufgabenname>** die Registerkarte **Mit folgenden Rechten starten**.
3. Führen Sie auf der Registerkarte **Mit folgenden Rechten starten** folgende Aktionen aus:
   a. Wählen Sie den Punkt **Benutzername** aus.
   b. Geben Sie den Namen und das Kennwort des Benutzers an, dessen Konto Sie verwenden möchten.

   Der von Ihnen ausgewählte Benutzer muss auf dem geschützten Server oder in der gleichen Domäne angemeldet sein.

   c. Bestätigen Sie das eingegebene Kennwort.
4. Klicken Sie auf **OK**.

UPDATE DER DATENBANKEN UND MODULE FÜR KASPERSKY ANTI-VIRUS

Dieser Abschnitt enthält Informationen über die Aufgaben zum Update der Datenbanken und Module von Kaspersky Anti-Virus, über die Verteilung der Updates und das Rollback eines Datenbanken-Updates in Kaspersky Security, sowie Anweisungen zum Anpassen der Aufgabeneinstellungen für Updates von Datenbanken und Programm-Modulen.

In diesem Abschnitt

Update der Datenbanken von Kaspersky Anti-Virus

Die auf einem geschützten Server gespeicherten Datenbanken von Kaspersky Anti-Virus veralten schnell. Die Virenanalytiker von Kaspersky Lab entdecken täglich Hunderte neuer Bedrohungen, erstellen entsprechende Einträge und nehmen sie in die Datenbank-Updates des Programms auf. (Ein Datenbank-Update besteht aus einer oder mehreren Dateien mit Einträgen, durch die sich Bedrohungen identifizieren lassen, die seit dem vorhergehenden Update erkannt wurden). Um das Infektionsrisiko für den Server auf ein Minimum zu reduzieren, aktualisieren Sie die Datenbanken regelmäßig.

Wenn seit dem Erscheinen des zuletzt installierten Datenbank-Updates über eine Woche vergangen ist, tritt das Ereignis *Datenbanken sind veraltet* ein. Werden die Datenbanken länger als zwei Wochen nicht aktualisiert, so tritt das Ereignis *Datenbanken sind stark veraltet* ein). Informationen über die Aktualität der Datenbanken werden im Node **Kaspersky Anti-Virus** der Konsolenstruktur angezeigt (s. Abschnitt "**Schutzstatus und Informationen über Kaspersky Anti-Virus anzeigen**" auf S. 33). Sie können mit Hilfe der allgemeinen Einstellungen von Kaspersky Anti-Virus eine andere Anzahl von Tagen vor dem Eintritt dieser Ereignisse einstellen (s. S. 36), sowie Benachrichtigung des Administrators über diese Ereignisse einstellen (s. S. 106).

Für den Download von Updates für die Datenbanken und Programm-Module verwendet Kaspersky Anti-Virus die FTP- oder HTTP-Update-Server von Kaspersky Lab, den Administrationsserver von Kaspersky Security Center oder andere Update-Quellen.

Sie können die Updates auf jeden der geschützten Server downloaden oder einen Computer als Verteiler einrichten, so dass die Updates auf ihn kopiert und anschließend an die Server verteilt werden. Wenn Sie die Anwendung Kaspersky Administration für die zentralisierte Verwaltung des Computerschutzes im Unternehmen verwenden, können Sie den Administrationsserver von Kaspersky Security Center als Verteiler für die Updates einsetzen.

Update-Aufgaben können manuell oder nach Zeitplan gestartet werden (s. S. 40).

Wenn der Update-Download unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Anti-Virus automatisch zu den Datenbanken mit den zuletzt installierten Updates zurück. Sollten die Datenbanken von Kaspersky Anti-Virus beschädigt sein, können Sie selbst ein Rollback zu den zuvor installierten Updates ausführen (s. Abschnitt "Rollback von Updates der Kaspersky Anti-Virus-Datenbanken" auf S. 51).

UPDATE DER MODULE VON KASPERSKY ANTI-VIRUS

Kaspersky Lab stellt Updatepakete für die Module von Kaspersky Anti-Virus zur Verfügung. Es gibt *dringende* (oder *kritische*) und *geplante* Updates. Dringende Update-Pakete beheben Schwachstellen und Fehler. Geplante Updates fügen neue Funktionen hinzu oder verbessern vorhandene.

Dringende Updatepakete werden auf den Updateservern von Kaspersky Lab veröffentlicht. Sie können festlegen, dass sie mit Hilfe der Aufgabe **Update der Programm-Module** automatisch installiert werden.

Geplante Updatepakete werden von Kaspersky Lab nicht auf den Updateservern veröffentlicht, um sie automatisch zu installieren. Sie können solche Updatepakete von der Kaspersky-Lab-Webseite downloaden. Mit Hilfe der Aufgabe **Update der Programm-Module** können Sie sich über das erscheinen von geplanten Updates für Kaspersky Anti-Virus informieren.

Sie können dringende Updates entweder auf jeden einzelnen geschützten Server aus dem Internet herunterladen oder einen Computer als Verteiler einrichten. In diesem Fall werden Updates auf den Verteiler heruntergeladen, ohne sie zu installieren, und anschließend an die Server verteilt. Um Datenbank-Updates zu kopieren und zu speichern, ohne Sie zu installieren, verwenden Sie die Aufgabe **Update-Verteilung**.

Bevor Updates für die Module installiert werden, kann Kaspersky Anti-Virus Sicherungskopien der zuvor installierten Module anlegen. Wenn das Update der Programm-Module unterbrochen oder fehlerhaft abgeschlossen wird, kehrt Kaspersky Anti-Virus automatisch zu den zuvor installierten Programm-Modulen zurück. Außerdem können Sie manuell ein Rollback des Updates der Module zu den zuvor installierten Updates ausführen.

Während der Installation von heruntergeladenen Updates wird der Dienst von Kaspersky Anti-Virus automatisch beendet und anschließend neu gestartet.

SCHEMATA FÜR DAS UPDATE DER DATENBANKEN UND MODULE VON ANTIVIREN-ANWENDUNGEN IN EINEM UNTERNEHMEN

Die Auswahl der Update-Quelle in Update-Aufgaben ist davon abhängig, nach welchem Schema die Datenbanken und Programm-Module der Antiviren-Anwendungen in Ihrem Unternehmen aktualisiert werden.

Sie können die Datenbanken und Module von Kaspersky Anti-Virus auf den geschützten Servern nach folgenden Schemata aktualisieren:

- Download von Updates direkt aus dem Internet auf jeden der geschützten Server (Schema 1).
- Download von Updates aus dem Internet auf einen Computer (Verteiler) und anschließende Verteilung auf die übrigen Server.

Als Verteiler kann ein beliebiger Computer dienen, auf dem eine der folgenden Anwendungen installiert ist:

- Kaspersky Anti-Virus (einer der geschützten Server) (Schema 2)
- Administrationsserver von Kaspersky Security Center (Schema 3).

Das Update über einen Computer, der als Verteiler funktioniert, erlaubt nicht nur die Einsparung von Internet-Datenverkehr, sondern bietet den Servern auch zusätzliche Sicherheit.

Im Folgenden werden die genannten Update-Schemata beschrieben.

Schema 1. Schema für das Update direkt aus dem Internet

Legen Sie auf jedem geschützten Server die Aufgabe **Update der Programm-Datenbanken** (**Update der Programm-Module**) an (s. Abbildung unten). Geben Sie als Update-Quelle die Kaspersky-Lab-Update-Server an. Stellen Sie den Aufgabenzeitplan ein.

Als Update-Quelle können auch andere HTTP- oder FTP-Server gewählt werden, auf denen ein Ordner mit den Update-Dateien vorhanden ist.

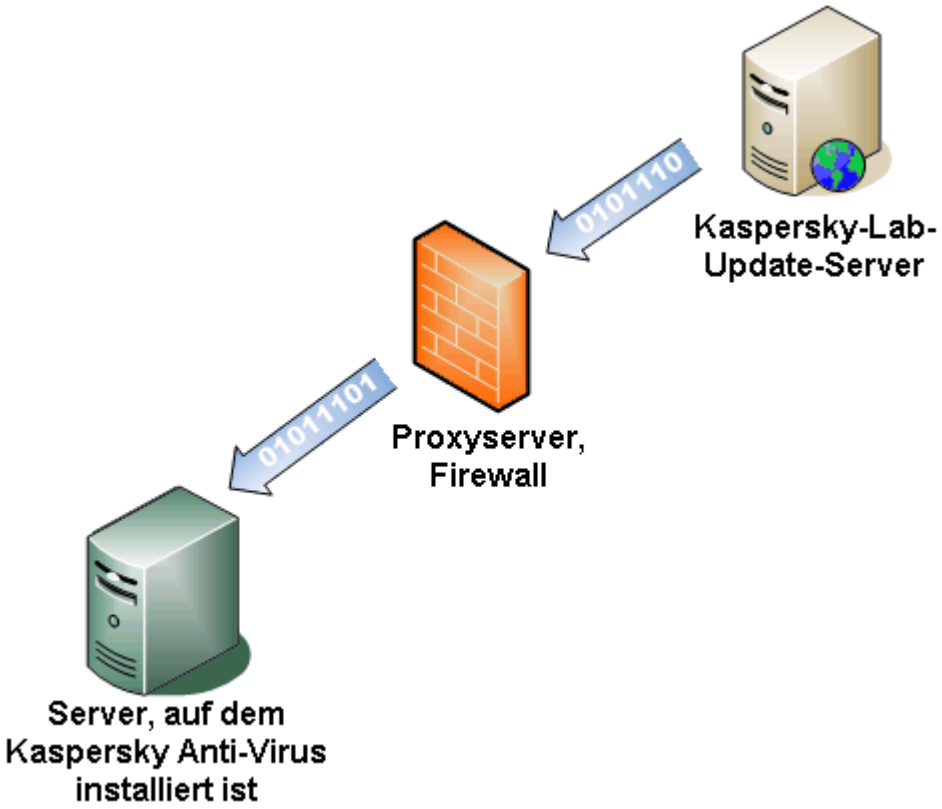


Abbildung 1: Schema für das Update der Datenbanken und Programm-Module

Schema 2. Update über einen der geschützten Server

Um ein Update nach diesem Schema durchzuführen, gehen Sie wie folgt vor:

1. **Kopieren Sie die Updates auf den ausgewählten geschützten Server.**

   Passen Sie auf dem als Verteiler ausgewählten Server die Aufgabe **Update-Verteilung** an. Geben Sie als Update-Quelle die Kaspersky-Lab-Update-Server an. Geben Sie einen Ordner an, in dem die Updates gespeichert werden sollen: Dabei muss es sich um einen gemeinsamen Ordner handeln..

   Unter Verwendung dieser Aufgabe können Sie nicht nur Updates für die geschützten Server empfangen, sondern auch für Rechner im lokalen Netzwerk, auf denen andere Korporativanwendungen von Kaspersky Lab der Versionen 6.0 und 8.0 installiert sind.

2. **Verteilen Sie die Updates auf die übrigen geschützten Server.**

   Erstellen Sie auf jedem der geschützten Server die Aufgabe **Update der Programm-Datenbanken** (**Update der Programm-Module**) (s. Abbildung unten). Geben Sie als Update-Quelle den Ordner auf dem Laufwerk des ausgewählten Rechners an, in den die Updates kopiert werden.

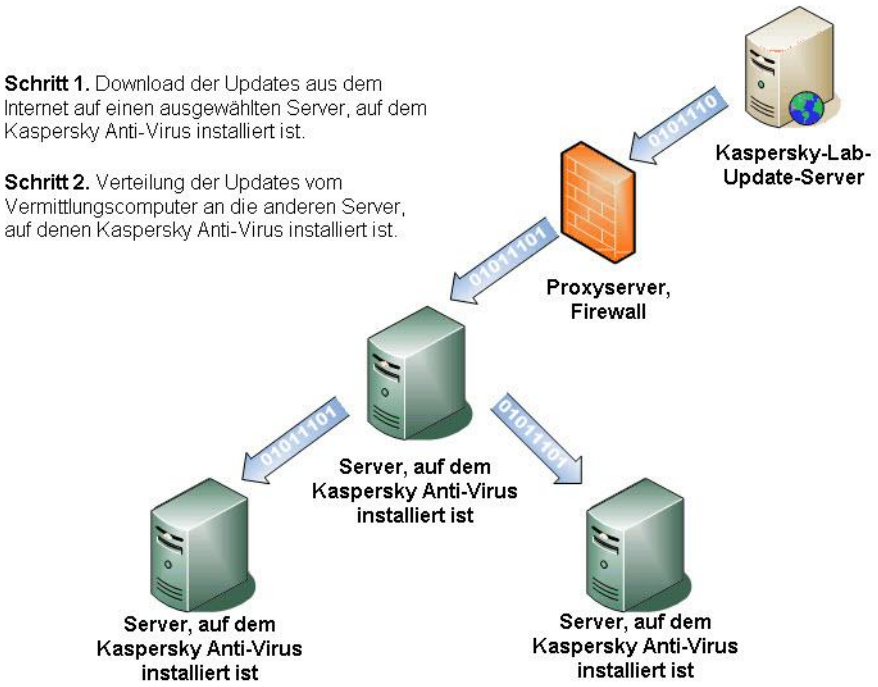


Abbildung 2:Update über einen der geschützten Server

Schema 3. Aktualisieren Sie über den Administrationsserver von Kaspersky Security Center

Wenn Sie das Programm Kaspersky Security Center für die zentrale Verwaltung des Schutzes von Computern einsetzen, können Sie Updates über den Administrationsserver für Kaspersky Security Center downloaden (s. Abbildung unten).

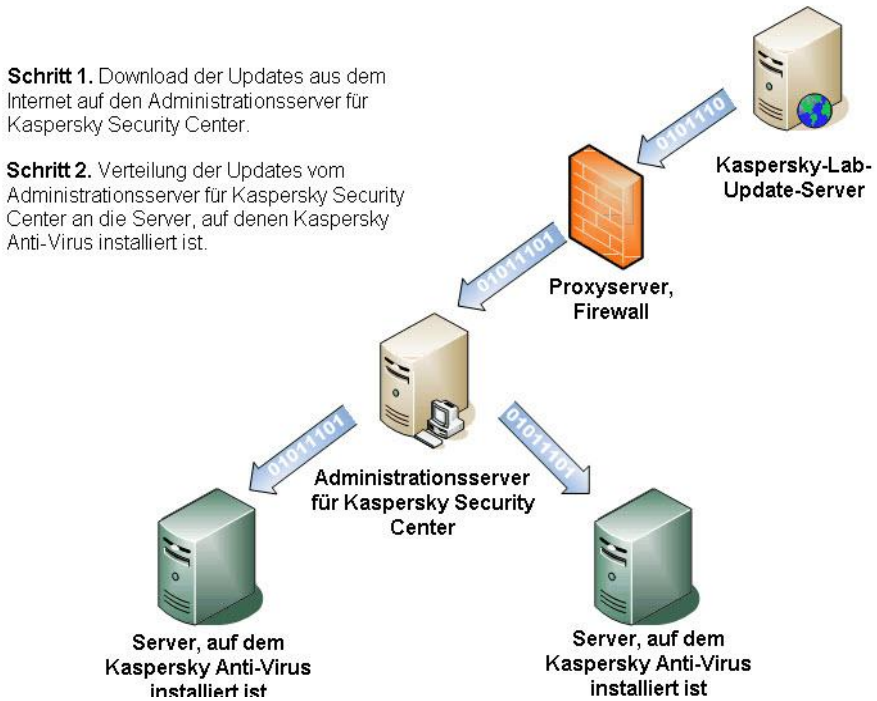


Abbildung 3:Update über den Administrationsserver von Kaspersky Security Center

Um ein Update nach diesem Schema durchzuführen, gehen Sie wie folgt vor:

1. Laden Sie die Updates von einem Kaspersky-Lab-Updateserver auf den Administrationsserver von Kaspersky Security Center herunter

   Passen Sie die globale Aufgabe **Update-Download durch Administrationsserver** für die angegebene Zusammenstellungen von Computern an. Geben Sie als Update-Quelle die Kaspersky-Lab-Update-Server an.

   Sie können nicht nur Updates für die geschützten Server empfangen, sondern auch für andere Rechner im lokalen Netzwerk, auf denen andere Korporativanwendungen von Kaspersky Lab der Versionen 6.0 und 8.0 installiert sind.

2. **Verteilen Sie die Updates auf die geschützten Server**

   Für die Update-Verteilung auf die geschützten Server stehen folgende Varianten zur Verfügung:

   - Passen Sie auf dem Administrationsserver von Kaspersky Security Center eine Gruppenaufgabe zum Update an, die der Update-Verteilung an die geschützten Server dienen soll.

     Wählen Sie im Aufgabenzeitplan das Startintervall **Nach Update-Download durch den Administrationsserver**. Der Administrationsserver startet die Aufgabe jedes Mal, wenn er Updates empfängt (Diese Variante gilt als empfohlen).

     Das Startintervall **Nach Update-Download durch den Administrationsserver** kann in der Konsole von Kaspersky Anti-Virus nicht angegeben werden.

   - Passen Sie auf jedem geschützten Server die Aufgabe **Update der Programm-Datenbanken** (**Update der Programm-Module**) an. Geben Sie dabei als Update-Quelle den Administrationsserver von Kaspersky Security Center an. Stellen Sie den Aufgabenzeitplan ein.

Wenn Sie zur Update-Verteilung den Einsatz des Administrationsservers von Kaspersky Security Center planen, installieren Sie zuerst auf jedem geschützten Server die Programmkomponente Administrationsagent, die zum Lieferumfang der Anwendung Kaspersky Security Center gehört. Er gewährleistet die Interaktion zwischen dem Administrationsserver und dem Kaspersky Anti-Virus auf einem geschützten Server. Ausführliche Informationen zum Administrationsagenten und seiner Konfiguration mit der Anwendung Kaspersky Security Center finden Sie im Dokument *Kaspersky Security Center. Administratorhandbuch*.

EINSTELLUNG VON AUFGABEN ZUM UPDATE

IN DIESEM ABSCHNITT

UPDATE-QUELLE AUSWÄHLEN, VERBINDUNG ZUR UPDATE-QUELLE ANPASSEN

In jeder Update-Aufgabe können Sie eine oder mehrere Update-Quellen angeben und die Verbindung mit den Update-Quellen anpassen.

Beachten Sie, dass geänderte Parameter von Update-Aufgaben nicht in laufenden Update-Aufgaben übernommen werden, sondern erst nach dem nächsten Aufgabenstart.

Um die Parameter der Update-Aufgabe zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Update** und wählen Sie eine der Update-Aufgaben aus.
2. Klicken Sie im Ergebnisfenster zur Konfiguration der Parameter auf den Link **Eigenschaften**.

   Passen Sie auf den Registerkarten des Fensters **Eigenschaften: <Aufgabenname>** die Update-Einstellungen gemäß Ihren Anforderungen an.

3. Wählen Sie auf der Registerkarte **Allgemein** die Update-Quelle, von der Kaspersky Anti-Virus die Updates herunterladen soll.
4. Wenn Sie die Option **Andere HTTP-, FTP-Server oder Netzwerkressourcen** gewählt haben, fügen Sie eine oder mehrere benutzerdefinierte Update-Quellen hinzu. Um eine Quelle anzugeben klicken Sie auf den Link **Andere HTTP-, FTP-Server oder Netzwerkressourcen und im Fenster** Update-Server **auf die Schaltfläche** Hinzufügen. Geben Sie im Eingabefeld die Adresse des Ordners mit den Update-Dateien auf einem FTP- oder HTTP-Server an; geben Sie einen lokalen oder einen Netzwerkordner im UNC-Format (Universal Naming Convention) an. Klicken Sie auf **OK**.

   Sie können hinzugefügte benutzerdefinierte Quellen aktivieren oder deaktivieren: Um eine hinzugefügte Quelle zu deaktivieren, entfernen Sie in der Liste das entsprechende Kontrollkästchen. Um eine Quelle zu aktivieren, kreuzen Sie das entsprechende Kontrollkästchen an.

   Um die Reihenfolge zu ändern, in der Kaspersky Anti-Virus auf benutzerdefinierte Quellen zugreift, verschieben Sie die gewünschte Quelle mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Stelle der Liste, je nachdem, wann auf die Quelle zugegriffen werden soll.

   Um den Pfad einer Quelle zu ändern, markieren Sie die Quelle in der Liste und klicken auf die Schaltfläche **Ändern**. Nehmen Sie dann im Eingabefeld die erforderlichen Änderungen vor und klicken Sie die **EINGABE**-Taste.

   Um eine Vorlage zu löschen, markieren Sie sie in der Liste und klicken Sie auf die Schaltfläche **Löschen**. Die Quelle wird aus der Liste entfernt.
5. Damit für den Download die Update-Server von Kaspersky Lab verwendet werden, falls die benutzerdefinierten Quellen nicht verfügbar sind, aktivieren Sie das Kontrollkästchen **Kaspersky-Lab-Update-Server verwenden**, wenn vom Benutzer angegebene Server nicht verfügbar sind.
6. Konfigurieren Sie auf der Registerkarte **Verbindungseinstellungen anpassen** die Verbindung mit der Update-Quelle.

   Führen Sie folgende Aktionen aus:

   - Geben Sie den Modus des FTP-Servers für die Verbindung mit einem geschützten Server an
   - Ändern Sie gegebenenfalls die Wartezeit bei einer Verbindung mit der Update-Quelle eines FTP- oder HTTP-Servers
   - Wenn der Update-Download von einer angegebenen Quelle über einen Proxyserver erfolgt, geben Sie die Parameter für den Zugriff auf den Proxyserver an:
     - Zugriff auf Proxyserver bei Verbindung mit verschiedenen Update-Quellen
     - Einstellungen des Proxyservers
     - Authentifizierungsmethode beim Zugriff auf einen Proxyserver
7. Nachdem Sie die erforderlichen Parameter angepasst haben, klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

OPTIMIERUNG DER NUTZUNG DES FESTPLATTEN-SUBSYSTEMS BEI DER AUSFÜHRUNG DER AUFGABE ZUM UPDATE DER PROGRAMM-DATENBANKEN

Bei Ausführung der Aufgabe **Update der Programm-Datenbanken** legt Kaspersky Anti-Virus die Update-Dateien auf einer lokalen Festplatte des Computers ab. Sie können die Belastung des Festplatten-Subsystems des Computers verringern, indem Sie die Update-Dateien während der Ausführung der Update-Aufgabe auf einer virtuellen Festplatte im Arbeitsspeicher ablegen.

Diese Funktion ist unter Microsoft Windows Server 2008 und späteren Versionen des Betriebssystems verfügbar.

Bei Nutzung dieser Funktion kann während der Ausführung der Aufgabe **Update der Programm-Datenbanken** eine zusätzliche logische Festplatte im Betriebssystem erscheinen. Nach Abschluss der Aufgabe verschwindet diese logische Festplatte wieder aus dem Betriebssystem.

Gehen Sie wie folgt vor, um die Belastung des Festplatten-Subsystems bei der Ausführung der Aufgabe Update der Programm-Datenbanken zu verringern:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Update** und wählen Sie die Aufgabe **Update der Programm-Datenbanken**.
2. Klicken Sie im Ergebnisfenster zur Konfiguration der Parameter auf den Link **Eigenschaften**.
3. Nehmen Sie auf der Registerkarte **Allgemein** im Block **Optimierung der Nutzung des Festplatten-Subsystems** folgende Einstellungen vor:
   - Aktivieren Sie das Kontrollkästchen **Belastung des Festplatten-Subsystems verringern**.
   - Geben Sie im Feld **Für die Optimierung zur Verfügung stehender Arbeitsspeicher** das Arbeitsspeichervolumen in Megabyte an. Das Betriebssystem stellt dieses Arbeitsspeichervolumen temporär für die Speicherung der Update-Dateien während der Aufgabenausführung zur Verfügung.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

EINSTELLUNGEN FÜR DIE AUFGABE UPDATE-VERTEILUNG ANPASSEN

*Um die Parameter der Aufgabe **Update-Verteilung** zu konfigurieren, gehen Sie wie folgt vor*:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Update** und wählen Sie die Aufgabe **Update-Verteilung**.
2. Klicken Sie im Ergebnisfenster auf den Link **Eigenschaften**.
3. Geben Sie im Fenster **Eigenschaften: Update-Verteilung** eine Update-Quelle und die entsprechenden Verbindungseinstellungen an. Beachten Sie die Anweisungen im Pkt. "Updatequelle auswählen, Verbindung zur Updatequelle und Regionsoptionen anpassen" (s. S. 47).
4. Geben Sie auf der Registerkarte **Allgemein** die Zusammensetzung der Updates an.
5. Geben Sie einen lokalen Ordner oder einen Netzwerkordner an, in dem Kaspersky Anti-Virus die heruntergeladenen Update-Dateien speichern soll.
6. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

PARAMETER DER AUFGABE UPDATE DER PROGRAMM-MODULE ANPASSEN

*Um die Parameter der Aufgabe **Update der Programm-Module** zu konfigurieren, gehen Sie wie folgt vor*:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Update** und wählen Sie die Aufgabe **Update der Programm-Module**.
2. Klicken Sie im Ergebnisfenster auf den Link **Eigenschaften**.
3. Geben Sie im Fenster **Eigenschaften: Update der Programm-Module** eine Update-Quelle und die entsprechenden Verbindungseinstellungen an. Beachten Sie die Anweisungen im Pkt. "Update-Quelle auswählen, Verbindung zur Update-Quelle und Regionsoptionen anpassen" (s. S. 47).
4. Geben Sie auf der Registerkarte **Allgemein** an, welche Aktionen ausgeführt werden sollen: Updates kopieren und installieren, oder nur prüfen, ob Updates vorhanden sind.
5. Damit Kaspersky Anti-Virus nach dem Abschluss der Aufgabe den Server automatisch neu startet, wenn zum Übernehmen von installierten Programm-Modulen ein Neustart erforderlich ist, aktivieren Sie das Kontrollkästchen **Neustart des Computers zulassen**.
6. Wenn Sie Informationen über die Veröffentlichung von geplanten Updates für Module von Kaspersky Anti-Virus, erhalten möchten, aktivieren Sie das Kontrollkästchen **Über verfügbare planmäßige Updates für die Programm-Module benachrichtigen**.

   Kaspersky Lab veröffentlicht geplante Updatepakete nicht auf den Update-Servern, um sie beim Update automatisch herunterzuladen. Sie können solche Updatepakete manuell von der Kaspersky-Lab-Webseite downloaden. Sie können festlegen, dass der Administrator über das Ereignis *Geplante Update für Anti-Virus-Module sind verfügbar* benachrichtigt wird. Die Benachrichtigung enthält die Adresse unserer Webseite, von der Sie geplante Updates herunterladen können. Details finden Sie im Abschnitt "Benachrichtigungen an Administrator und Benutzer anpassen" (s. S. 106).
7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

AUFGABEN ZUM UPDATE

In Kaspersky Anti-Virus sind vier Systemaufgaben zum Update vorgesehen: **Update der Programm-Datenbanken**, **Update der Programm-Module**, **Update-Verteilung** und **Rollback des Datenbank-Updates**.

Standardmäßig stellt Kaspersky Anti-Virus eine Verbindung zur Update-Quelle her (zu einem Update-Server von Kaspersky Lab), wobei automatisch die Proxyserver-Einstellungen im Netzwerk ermittelt und beim Zugriff auf den Proxyserver keine die Authentifizierung verwendet.

Sie können Aufgabe zum Update anpassen (s. S. 47). Nachdem Sie die Aufgabenparameter geändert haben, übernimmt Kaspersky Anti-Virus die neuen Werte beim nächsten Aufgabenstart.

Update-Aufgaben können beendet, aber nicht vorübergehend angehalten werden.

Informationen darüber, wie Kaspersky Anti-Virus-Aufgaben verwaltet werden, finden Sie im Pkt. "Aufgabenverwaltung" (s. S. 38).

Update der Programm-Datenbanken

Kaspersky Anti-Virus kopiert die Datenbanken aus der Update-Quelle auf den geschützten Server und verwendet in laufenden Aufgaben zum **Echtzeitschutz** sofort die aktualisierten Datenbanken. Die Aufgaben **Untersuchung auf Befehl** und **Schutz von Netzwerkspeichern** verwenden beim nächsten Aufgabenstart die aktualisierten Programm-Datenbanken.

In der Grundeinstellung wird die Aufgabe **Update der Programm-Datenbanken** jede Stunde gestartet.

Update der Programm-Module

Kaspersky Anti-Virus kopiert die Updates seiner Programm-Module aus der Update-Quelle auf den geschützten Server und installiert die Module. Zur Übernahme der installierten Programm-Module muss der Computer und/oder Kaspersky Anti-Virus eventuell neu gestartet werden.

Kaspersky Anti-Virus startet jede Woche am Freitag um 16.00 Uhr (Der Zeitpunkt hängt von den Regionsoptionen des geschützten Servers ab) die Aufgabe **Update der Programm-Module**. Dabei wird nur geprüft, ob kritische und geplante Updates für die Anti-Virus-Module vorhanden sind. Updates werden nicht kopiert.

Update-Verteilung

Kaspersky Anti-Virus lädt die Dateien für das Update der Datenbanken und Programm-Module herunter und speichert sie im angegebenen Netzwerkordner oder lokalen Ordner, ohne sie zu installieren.

Rollback des Datenbank-Updates

Kaspersky Anti-Virus kehrt zu den Datenbanken mit den zuvor installierten Updates zurück.

STATISTIK VON UPDATE-AUFGABEN

Während eine Update-Aufgabe ausgeführt wird, können Sie in Echtzeit Informationen über das Volumen der Daten anzeigen lassen, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt empfangen wurden, sowie weitere Informationen zur Aufgabenausführung.

Nachdem eine Aufgabe abgeschlossen oder beendet wurde, können Sie diese Informationen im Bericht über die Aufgabenausführung anzeigen (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99).

Um die Statistik der Update-Aufgabe anzuzeigen, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Update** auf.
2. Wählen Sie die Aufgabe, deren Statistik Sie anzeigen möchten.

Im Ergebnisfenster wird im Block **Statistik** eine Statistik der Aufgabe angezeigt.

Wenn Sie die Aufgabe **Update der Programm-Datenbanken** oder die Aufgabe **Update-Verteilung** zur Anzeige gewählt haben, wird das Volumen der Daten im Ergebnisfenster anzeigt, die bis zum jetztigen Zeitpunkt von Kaspersky Anti-Virus empfangen wurden (**Empfangene Daten**).

Bei Anzeige der Aufgabe **Update der Programm-Module** werden die in nachfolgender Tabelle beschriebenen Informationen dargestellt:

Tabelle 9. Informationen über die Aufgabe Update der Programm-Module

FELD	BESCHREIBUNG
Empfangene Daten	Gesamtvolumen der empfangenen Daten
Wichtige Updates sind verfügbar	Anzahl der kritischen Updates, die zur Installation bereitstehen.
Planmäßige Updates sind verfügbar	Anzahl der geplanten Updates, die zur Installation bereitstehen.
Fehler beim Übernehmen von Updates	Wenn dieser Wert ungleich Null ist, wurde das Update nicht übernommen. Den Namen des Updates, bei dessen Übernahme ein Fehler aufgetreten ist, können Sie im Bericht über Aufgabenausführung feststellen (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99).

ROLLBACK DES UPDATES FÜR DIE DATENBANKEN VON KASPERSKY ANTI-VIRUS

Bevor Updates für die Datenbanken installiert werden, legt Kaspersky Anti-Virus Sicherungskopien der bisher verwendeten Datenbanken an. Wenn die Aktualisierung unterbrochen oder fehlerhaft abgeschlossen wurde, kehrt Kaspersky Anti-Virus automatisch zu den Datenbanken mit den zuletzt installierten Updates zurück.

Wenn nach einem Datenbank-Update Probleme auftreten, können Sie die Datenbanken mit den zuvor installierten Updates wiederherstellen. Starten Sie dazu die Aufgabe **Rollback des Datenbank-Updates**.

ROLLBACK DES UPDATES FÜR PROGRAMM-MODULE

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

Bevor Updates für die Programm-Module installiert werden, legt Kaspersky Anti-Virus Sicherungskopien der bisher verwendeten Module an. Wenn die Aktualisierung von Modulen unterbrochen oder fehlerhaft abgeschlossen wurde, kehrt Kaspersky Anti-Virus automatisch zu den Modulen mit den zuletzt installierten Updates zurück.

Um ein Rollback der Programm-Module auszuführen, verwenden Sie die Verwaltungskomponente von Microsoft Windows **Programme ändern und löschen**.

Außerdem können Sie ein Rollback der Programm-Module zu den zuvor installierten Updates manuell ausführen.

ECHTZEITSCHUTZ

Dieser Abschnitt informiert über folgende Echtzeitschutzaufgaben: **Echtzeitschutz für Dateien** und **Skript-Untersuchung**. Darüber hinaus enthält dieser Abschnitt Anweisungen zum Anpassen der Einstellungen für Aufgaben zum Echtzeitschutz sowie zum Anpassen der Sicherheitseinstellungen des geschützten Servers.

IN DIESEM ABSCHNITT

AUFGABEN DES ECHTZEITSCHUTZES

In Kaspersky Anti-Virus sind zwei Systemaufgaben für den Echtzeitschutz vorgesehen: **Echtzeitschutz für Dateien** und **Skript-Untersuchung**.

Wenn die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird, untersucht Kaspersky Anti-Virus folgende Objekte des geschützten Servers, wenn darauf zugegriffen wird:

- Dateien
- alternative Datenströme der Dateisysteme (NTFS-Streams)
- MBR und Bootsektoren von lokalen Festplatten und Wechseldatenträgern

Wenn ein Programm eine Datei auf den Server schreibt oder vom Server ausliest, fängt Kaspersky Anti-Virus diese Datei ab und untersucht sie auf Bedrohungen. Beim Fund einer Bedrohung werden die von Ihnen festgelegten Aktionen ausgeführt: Es wird versucht, die Datei zu desinfizieren, die Datei wird in die Quarantäne verschoben oder einfach gelöscht. Kaspersky Anti-Virus gibt die Datei dem Programm erst zurück, wenn sie nicht infiziert ist oder erfolgreich desinfiziert wurde.

Standardmäßig werden Echtzeitschutz-Aufgaben automatisch beim Start von Kaspersky Anti-Virus gestartet. Sie können diese Aufgaben beenden und erneut starten und/oder ihren Zeitplan anpassen. Außerdem können Sie Echtzeitschutz-Aufgaben anhalten und fortsetzen, wenn die Objektuntersuchung für einen vorübergehenden Zeitraum unterbrochen werden soll (z.B. während einer Daten-Replikation).

Sie können die Aufgabe **Echtzeitschutz für Dateien** (s. Pkt "**Aufgabe Echtzeitschutz für Dateien anpassen**" auf S. 52) anpassen – Schutzbereich festlegen und Sicherheitseinstellungen für die gewählten Knoten wählen, vertrauenswürdige Zone übernehmen, Verwendung der heuristischen Analyse einstellen.

Wenn die Aufgabe **Skript-Untersuchung** ausgeführt wird, kontrolliert Kaspersky Anti-Virus die Ausführung von Skripts, die mit Microsoft Windows Script Technologies (oder Active Scripting) erstellt worden sind (z. B. VBScript- oder JScript®-Skripts). Die Ausführung von Skripts wird nur erlaubt, wenn das betreffende Skript von Kaspersky Anti-Virus als sicher eingestuft wurde. Kaspersky Anti-Virus verbietet die Ausführung von Skripts, die als gefährlich eingestuft wurden. Wenn Kaspersky Anti-Virus ein Skript als potenziell gefährlich eingestuft hat, führt er die von Ihnen festgelegte Aktion aus: Die Ausführung des Skripts wird verboten oder erlaubt. Informationen darüber, wie die Ausführung potenziell gefährlichen Skripts erlaubt oder verboten wird, finden Sie im Abschnitt "Anpassen der Aufgabe **Skript-Untersuchung**" (s. S. 62).

AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN ANPASSEN

Die Systemaufgabe **Echtzeitschutz für Dateien** besitzt die in der Tabelle unten beschriebenen Parameter. Sie können die Werte dieser Parameter ändern und die Aufgabe anpassen.

Nachdem Sie die Aufgabenparameter geändert haben, z.B. einen anderen Schutzbereich angegeben haben, übernimmt Kaspersky Anti-Virus die neuen Parameterwerte sofort in der laufenden Aufgabe. Im Bericht über die Aufgabenausführung werden Datum und Uhrzeit der Parameteränderung sowie Informationen über die Aufgabenparameter vor und nach der Änderung gespeichert.

*Um die Aufgabe **Echtzeitschutz für Dateien** zu konfigurieren,* gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.

   Im Ergebnisfenster auf der Registerkarte **Schutzbereich anpassen** werden die Dateistruktur des Servers und das Fenster **Sicherheitsstufe** für den ausgewählten Knoten der Dateiressourcen angezeigt (Standardmodus).
3. Passen Sie die entsprechenden Aufgabenparameter an (s. Tabelle unten).
4. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

*Tabelle 10. Standardparameter der Aufgabe **Echtzeitschutz für Dateien***

EINSTELLUNGEN	STANDARDWERT	BESCHREIBUNG
Schutzbereich	Gesamter Server	Sie können den Schutzbereich beschränken.
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, entspricht der Sicherheitsstufe **Empfohlen** (s. S. 56).	Sie können für die ausgewählten Knoten in der Dateistruktur des Servers *folgende Aktionen ausführen:* • eine andere vordefinierte Sicherheitsstufe auswählen (s. S. 56); • Sicherheitseinstellungen manuelll ändern (s. S. 73) • Sie können die Sicherheitseinstellungen des ausgewählten Knotens in einer Vorlage speichern, um sie später für andere Knoten zu übernehmen (s. S. 59).
Schutzmodus für Objekte	Beim Öffnen und Ändern	Sie können den Schutzmodus für Objekte festlegen – also angeben, bei welchen Zugriffsarten auf Objekte Kaspersky Anti-Virus diese überprüfen wird.
Heuristische Analyse	Wählen Sie die Sicherheitsstufe **Mittel** aus.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
Vertrauenswürdige Zone	Wird verwendet **Ausgeschlossen werden Programme zur Remote-Administration** RemoteAdmin und Dateien, die von Microsoft empfohlen werden, falls Sie bei der Installation von Kaspersky Anti-Virus die Optionen **Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen** und **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**gewählt haben.	Einheitliche Liste der Ausnahmen, die Sie in ausgewählten Untersuchungsaufgaben und in der Aufgabe **Echtzeitschutz für Dateien** verwenden können. Anlegen und Übernehmen von Ausnahmen der vertrauenswürdigen Zone (s. S. 77).

IN DIESEM ABSCHNITT

SCHUTZBEREICH DER AUFGABE "ECHTZEITSCHUTZ FÜR DATEIEN"

IN DIESEM ABSCHNITT

SCHUTZBEREICH DER AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN FESTLEGEN

Wenn die Aufgabe **Echtzeitschutz für Dateien** mit den standardmäßigen Parametern ausgeführt wird, untersucht Kaspersky Anti-Virus alle Objekte des Serverdateisystems. Wenn es aus Sicherheitsgründen nicht nötig ist, alle Objekte zu untersuchen, können Sie den Schutzbereich beschränken.

In der Konsole von Kaspersky Anti-Virus wird der Schutzbereich als Baumstruktur jener Dateien des Servers dargestellt, die von Kaspersky Anti-Virus untersucht werden können.

Die Knoten der Dateistruktur des Servers werden auf folgende Weise dargestellt:

☑ Der Knoten ist im Schutzbereich.

☐ Der Knoten ist nicht im Schutzbereich.

☑ Mindestens ein diesem Knoten untergeordneter Knoten gehört nicht zum Schutzbereich oder die Sicherheitseinstellungen des oder der untergeordneten Knoten unterscheiden sich von den Sicherheitseinstellungen dieses Knotens.

Beachten Sie, dass das Symbol ☑ angezeigt wird, wenn Sie alle untergeordneten Knoten auswählen, aber nicht den übergeordneten Knoten selbst. In diesem Fall werden Dateien und Ordner, die in diesem Knoten eingebettet sind, nicht automatisch in den Schutzbereich aufgenommen. Um sie zu übernehmen, können Sie die ihnen übergeordneten Knoten in den Schutzbereich aufnehmen. Oder Sie können in der Konsole von Kaspersky Anti-Virus "virtuelle Kopien" von ihnen anlegen und diese Objekte dem Schutzbereich hinzufügen.

Die Namen von virtuellen Knoten des Schutzbereichs werden blauer Schrift dargestellt.

VORDEFINIERTE SCHUTZBEREICHE

Wenn Sie die Aufgabe **Echtzeitschutz für Dateien** öffnen, wird im Ergebnisfenster auf der Registerkarte **Schutzbereich anpassen** die Dateistruktur des Servers angezeigt.

Die Dateistruktur des Servers enthält die Knoten, für die Sie nach den Sicherheitseinstellungen in Microsoft Windows über Leserechte verfügen.

Die Dateistruktur des Servers enthält folgende vordefinierte Schutzbereiche:

- **Lokale Festplatten**. Kaspersky Anti-Virus untersucht Dateien auf den Festplatten des Servers.
- **Wechseldatenträger**. Kaspersky Anti-Virus untersucht die Dateien auf Wechseldatenträgern, z.B. auf CDs oder USB-Sticks.
- **Netzwerkumgebung**. Kaspersky Anti-Virus untersucht die Dateien, die in Netzwerkordnern gespeichert sind oder von auf dem Server laufenden Anwendungen abgefragt werden. Kaspersky Anti-Virus untersucht 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 gemountet werden (z.B. gemeinsame Cluster-Laufwerke (Anlegen eines virtuellen Schutzbereichs).

Pseudo-Laufwerke, die mit dem Befehl SUBST erzeugt wurden, werden nicht in der Dateistruktur des Servers in der Konsole von Kaspersky Anti-Virus angezeigt. Um Objekte auf einem Pseudo-Laufwerk in den Schutzbereich aufzunehmen, schließen Sie den Ordner auf dem Server, mit dem dieses Pseudo-Laufwerk 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 Netzwerk-Laufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

FESTLEGEN DES SCHUTZBEREICHS

Um einen Schutzbereich anzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie die Aufgabe **Echtzeitschutz für Dateien**.
2. Auf der Registerkarte **Schutzbereich anpassen** des Ergebnisfensters, in der Dateistruktur des Servers, führen Sie folgende Aktionen aus:
   - Zum Ausschließen eines einzelnen Knotens aus dem Schutzbereich öffnen Sie die Dateistruktur des Servers, um den gewünschten Knoten anzuzeigen, und entfernen das entsprechende Kontrollkästchen.
   - Um nur jene Knoten auszuwählen, die dem Schutzbereich hinzugefügt werden sollen, deaktivieren Sie das Kontrollkästchen **Arbeitsplatz** und führen Sie dann eine der folgenden Aktionen aus:
     - um alle Laufwerke eines bestimmten Typs in den Schutzbereich aufzunehmen, aktivieren Sie das Kontrollkästchen für den entsprechenden Laufwerkstyp (z. B. um alle Wechseldatenträger auf dem Server einzuschließen, aktivieren Sie das Kontrollkästchen **Wechseldatenträger**).
     - um ein einzelnes Laufwerk eines bestimmten Typs in den Schutzbereich aufzunehmen, öffnen Sie den Knoten, der die Liste dieses Laufwerkstyps enthält, und aktivieren Sie das Kontrollkästchen für das entsprechende Laufwerk. Um z.B. den Wechseldatenträger **F:** auszuwählen, öffnen Sie den Knoten **Wechseldatenträger** und aktivieren Sie das Kontrollkästchen für Laufwerk **F:**.
     - um nur einen bestimmten Ordner eines Laufwerks in den Schutzbereich aufzunehmen, öffnen Sie die Dateistruktur des Servers, um den betreffenden Ordner anzuzeigen, und aktivieren Sie das entsprechende Kontrollkästchen. Auf gleiche Weise können auch Dateien in den Schutzbereich aufgenommen werden.
3. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Die Aufgabe **Echtzeitschutz für Dateien** kann nur gestartet werden, wenn mindestens ein Knoten der Dateistruktur des Servers in den Schutzbereich aufgenommen wurde.

Wenn Sie einen komplexen Schutzbereich festlegen, d. h. Sie geben beispielsweise unterschiedliche Sicherheitseinstellungswerte für mehrere separate Knoten in der Dateistruktur des Servers an, so kann dadurch die Untersuchung der Objekte bei Zugriff verlangsamt werden.

VIRTUELLE SCHUTZBEREICHE

Kaspersky Anti-Virus kann nicht nur vorhandene Ordner und Dateien auf Festplatten und Wechseldatenträgern untersuchen, sondern auch Datenträger, die vom Server temporär überwacht werden, beispielsweise allgemeine Datenträger eines Clusters sowie Ordner und Dateien, die von verschiedenen Anwendungen und Diensten dynamisch auf dem Server angelegt werden.

Wenn Sie alle Serverobjekte in den Schutzbereich aufgenommen haben, gehören automatisch auch diese dynamischen Knoten zum Schutzbereich. Wenn Sie allerdings spezielle Werte für die Sicherheitseinstellungen dieser dynamischen Knoten festlegen möchten oder den Echtzeitschutz nicht für den gesamten Server, sondern nur für einzelne Bereiche aktiviert haben, dann muss, um dynamische Laufwerke, Ordner oder Dateien in den Schutzbereich aufzunehmen, zuvor in der Konsole von Kaspersky Anti-Virus ein virtueller Schutzbereich angelegt werden. Die von Ihnen angelegten Laufwerke, Ordner und Dateien existieren nur in der Konsole von Kaspersky Anti-Virus, nicht aber in der Dateisystemstruktur des geschützten Servers.

Wenn Sie einen Schutzbereich anlegen und alle untergeordneten Ordner oder Dateien auswählen, nicht aber den übergeordneten Ordner, dann werden die dynamischen Ordner oder Dateien, die sich darin befinden, nicht automatisch in den Schutzbereich aufgenommen. Es ist erforderlich, in der Konsole von Kaspersky Anti-Virus "virtuelle Kopien" von ihnen anlegen und sie dem Schutzbereich hinzuzufügen.

Das Erstellen eines virtuellen Schutzbereiches in der Aufgabe "Echtzeitschutz für Dateien" finden Sie auf S. 56.

Informationen darüber, wie in Aufgaben zur Untersuchung auf Befehl ein virtueller Schutzbereich erstellt wird (s. S.71).

VIRTUELLE SCHUTZBEREICHE ERSTELLEN: DYNAMISCHE DATENTRÄGER, ORDNER UND DATEIEN IN SCHUTZBEREICH ÜBERNEHMEN

Sie können einzelne virtuelle Laufwerke, Ordner oder Dateien nur dann zum Schutzbereich bzw. Untersuchungsbereich hinzufügen, wenn der Schutzbereich bzw. Untersuchungsbereich als Dateistruktur dargestellt wird.

Um ein virtuelles Laufwerk zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.
2. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Schutzbereich anpassen** in der Dateistruktur des Servers das Kontextmenü für den Knoten **Virtuelle Festplatten** und wählen Sie in der Liste der verfügbaren Namen einen Namen für die anzulegende virtuelle Festplatte.
3. Setzen Sie das Häkchen neben dem hinzugefügten Datenträger, um diesen Datenträger in den Schutzbereich zu übernehmen.
4. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Um einen virtuellen Ordner oder eine virtuelle Datei zum Schutzbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.
2. Öffnen Sie das Kontextmenü für den Knoten, zu dem Sie einen Ordner oder eine Datei hinzufügen möchten. Klicken Sie dazu mit der rechten Maustaste auf der Registerkarte **Schutzbereich anpassen** des Ergebnisfensters in der Dateistruktur des Servers auf den betreffenden Knoten und wählen Sie einen der folgenden Punkte aus: **Virtuellen Ordner hinzufügen** oder **Virtuelle Datei hinzufügen**.
3. Tragen Sie im Eingabefeld den Namen für den Ordner (die Datei) ein. Bei der Angabe eines Dateinamens können Sie mit Hilfe der Sonderzeichen * und ? eine Maske angeben.
4. In der Zeile mit dem Namen der erstellten Ordners (Datei) setzen Sie das Häkchen, um den Ordner (die Datei) in den Schutzbereich zu übernehmen.
5. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

ANPASSEN DER SICHERHEITSPARAMETER FÜR EINEN BESTIMMTEN KNOTEN

IN DIESEM ABSCHNITT

VORDEFINIERTE SICHERHEITSSTUFEN IN DER AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN WÄHLEN

Für Knoten, die in der Dateistruktur des Servers 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 für den Server empfohlen, wenn in Ihrem Netzwerk neben Kaspersky Anti-Virus auf Servern und Workstations noch zusätzliche Maßnahmen für die Computersicherheit getroffen werden. Dazu zählen beispielsweise der Einsatz von Firewalls und von Sicherheitsrichtlinien für die Netzwerkbenutzer.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Server. Diese Stufe ist laut Empfehlung der Kaspersky-Lab-Experten für den Schutz von Dateiservern in den meisten Unternehmensnetzwerken ausreichend. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximale Sicherheit

Die Anwendung der Sicherheitsstufe **Maximale Sicherheit** wird empfohlen, wenn Sie erhöhten Wert auf die Computersicherheit des Unternehmensnetzwerks legen.

Tabelle 11. Vordefinierte Sicherheitsstufen und entsprechende Werte für die Sicherheitseinstellungen

EINSTELLUNGEN	SICHERHEITSSTUFE		
	MAXIMALE LEISTUNG	EMPFOHLEN	MAXIMALE SICHERHEIT
Schutz von Objekten	Nach Erweiterung	Nach Format	Nach Format
Optimierung	Aktiviert	Aktiviert	Deaktiviert
Aktion für infizierte Objekte	Desinfizieren. Irreparable Objekte löschen	Desinfizieren. Irreparable Objekte löschen	Desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte.	In Quarantäne verschieben	In Quarantäne verschieben	In Quarantäne verschieben
Objekte 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 festgelegt
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

Beachten Sie, dass die Einstellungen **Schutz von Objekten**, **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden** und **Heuristische Analyse verwenden** nicht zum Einstellungssatz der vordefinierten Sicherheitsstufen gehören. Wenn Sie nach der Auswahl einer der vordefinierten Sicherheitsstufen den Status 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. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.
2. Auf der Registerkarte **Schutzbereich anpassen** des Ergebnisfensters, in der Dateistruktur des Servers, wählen Sie den Knoten, für den Sie eine vordefinierte Sicherheitsstufe auswählen möchten.
3. Vergewissern Sie sich, dass dieser Knoten zum Schutzbereich gehört (s. Pkt "Schutzbereich erstellen" auf S. 55).
4. Wählen Sie die entsprechende Sicherheitsstufe aus der Liste im Fenster **Sicherheitsstufe** aus.
5. Im Fenster wird eine Liste mit Werten der Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
6. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

MANUELLES ANPASSEN VON SICHERHEITSEINSTELLUNGEN IN DER AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN

Standardmäßig werden in der Aufgabe **Echtzeitschutz für Dateien** die gleichen Sicherheitseinstellungen wie für den gesamten Schutzbereich verwendet. Ihre Werte entsprechen den Werten der vordefinierten Sicherheitsstufe **Empfohlen** (s. S. 56).

Sie können die Werte der standardmäßigen Sicherheitseinstellungen ändern. Dabei können Sie entweder einheitliche Werte für den gesamten Schutzbereich oder individuelle Werte für bestimmte Knoten der Dateistruktur des Servers festlegen.

Die Sicherheitseinstellungen, die Sie für einen ausgewählten Knoten festlegen, werden automatisch für alle untergeordneten Knoten übernommen. Wenn Sie die Sicherheitseinstellungen eines untergeordneten Knotens jedoch separat anpassen, werden die Sicherheitseinstellungen des übergeordneten Knotens nicht für ihn übernommen.

Um die Sicherheitseinstellungen eines bestimmten Knotens manuell anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.
2. Auf der Registerkarte **Schutzbereich anpassen** des Ergebnisfensters, in der Dateistruktur des Servers, wählen Sie den Knoten, dessen Sicherheitseinstellungen Sie anpassen möchten.
3. Klicken Sie im unteren Bereich des Fensters auf die Schaltfläche **Einstellungen**.

   Das Fenster **Sicherheitseinstellungen** wird geöffnet.

   Sie können für einen ausgewählten Knoten des Schutzbereichs eine zuvor erstellte Vorlage mit bestimmten Sicherheitseinstellungen übernehmen (s. S. 59).
4. Passen Sie die Sicherheitsparameter entsprechend an: Gehen Sie hierzu wie folgt vor:
   - Führen Sie bei Bedarf auf der Registerkarte **Allgemein** folgende Aktionen aus:
     - Geben Sie im Abschnitt **Schutz von Objekten** an, ob Kaspersky Anti-Virus alle Objekte des Schutzbereichs oder nur Objekte mit bestimmten Formaten oder bestimmten Erweiterungen untersuchen soll, ob Kaspersky Anti-Virus Laufwerksbootsektoren, MBR und alternative NTFS-Datenströme untersuchen soll, ob Kaspersky Anti-Virus Objekte, die eine Microsoft-Signatur besitzen, überspringen soll – Untersuchungsobjekte.
     - Legen Sie im Abschnitt **Optimierung** fest, ob Kaspersky Anti-Virus im ausgewählten Bereich alle Objekte untersuchen soll oder nur neue und veränderte Objekte.
     - Geben Sie im Abschnitt **Schutz von zusammengesetzten Objekten** an, welche zusammengesetzten Objekte von Kaspersky Anti-Virus untersucht werden sollen.
   - Führen Sie bei Bedarf auf der Registerkarte **Aktionen** folgende Aktionen aus:
     - Wählen Sie eine Aktion für infizierte Objekte
     - Wählen Sie eine Aktion für möglicherweise infizierte Objekte
     - Passen Sie die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an.
   - Führen Sie bei Bedarf auf der Registerkarte **Leistung** folgende Aktionen aus:
     - Schließen Sie Dateien nach Name oder Namensmaske aus
     - Schließen Sie gefundene Objekte nach Name oder Namensmaske aus
     - Geben Sie die maximale Untersuchungsdauer für ein Objekt an
     - Geben Sie die maximale Größe für ein zu untersuchendes zusammengesetztes Objekt an
     - Aktivieren oder deaktivieren Sie die Übernahme der iChecker-Technologie
     - Aktivieren oder deaktivieren Sie die Übernahme der iSwift-Technologie
5. Nachdem Sie die gewünschten Sicherheitseinstellungen angepasst haben, öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

ARBEIT MIT VORLAGEN IN DER AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN

IN DIESEM ABSCHNITT

SICHERHEITSEINSTELLUNGEN IN EINER VORLAGE SPEICHERN

In der Aufgabe **Echtzeitschutz für Dateien** können Sie, nachdem die Sicherheitsparameter eines bestimmten Knotens in der Dateistruktur des Servers angepasst wurden, diese Werte in einer Vorlage speichern, um die Vorlage später auf einen anderen Knoten zu übertragen.

Um einen Satz von Sicherheitsparametern in einer Vorlage zu speichern, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.
2. Auf der Registerkarte **Schutzbereich anpassen** des Ergebnisfensters, in der Dateistruktur des Servers, wählen Sie den Knoten, dessen Sicherheitseinstellungen Sie speichern möchten.
3. Klicken Sie im unteren Bereich des Fensters auf die Schaltfläche **Einstellungen**.
4. Klicken Sie im Fenster Parameter für Schutzbereich auf der Registerkarte **Allgemein** auf die Schaltfläche **Als Vorlage speichern**.
5. Geben Sie im Fenster **Eigenschaften der Vorlage** im Feld **Vorlagenname** den Namen der Vorlage ein.
6. Tragen Sie im Feld **Beschreibung** beliebige Zusatzinformationen über die Vorlage ein.
7. Klicken Sie auf **OK**. Die Vorlage mit dem Satz der Sicherheitseinstellungen wird gespeichert.

SICHERHEITSEINSTELLUNGEN IN EINER VORLAGE ANZEIGEN

Um die Werte der Sicherheitseinstellungen in einer vorhandenen Vorlage anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und wählen Sie den Befehl **Vorlagen für Einstellungen**.
3. Im Fenster **Vorlagen** wird eine Liste der Vorlagen angezeigt, die Sie in der Aufgabe **Echtzeitschutz für Dateien** übernehmen können.
4. Um Informationen über eine Vorlage und die entsprechenden Sicherheitseinstellungen anzuzeigen, wählen Sie die gewünschte Vorlage in der Liste und klicken Sie auf **Anzeigen**.

   Auf der Registerkarte **Allgemein** werden der Name der Vorlage und Zusatzinformationen über die Vorlage angezeigt. Die Registerkarte **Einstellungen** enthält eine Liste mit den Werten der Sicherheitseinstellungen, die in der Vorlage gespeichert sind.

VORLAGE ÜBERNEHMEN

Wenn Sie eine Vorlage für einen übergeordneten Knoten übernehmen, werden die Sicherheitseinstellungen der Vorlage auch für alle untergeordneten Knoten übernommen, mit Ausnahme der folgenden:

- Die Vorlage gilt nicht für Elemente, deren Sicherheitseinstellungen Sie separat konfiguriert haben. Um die Sicherheitseinstellungen aus einer Vorlage für alle untergeordneten Knoten zu übernehmen, deaktivieren Sie vor dem Übernehmen der Vorlage in der Dateistruktur des Servers das Kontrollkästchen des übergeordneten Knotens, und aktivieren Sie es anschließend wieder. Übernehmen Sie die Vorlage für den übergeordneten Knoten. Alle untergeordneten Knoten erhalten nun die gleichen Sicherheitseinstellungen wie der übergeordnete Knoten.
- Die Vorlage gilt nicht für untergeordnete virtuelle Elemente. Wenn Sie die Parameter eines untergeordneten virtuellen Elementes genauso wie die Parameter des übergeordneten Elementes konfigurieren wollen, müssen Sie das virtuelle Element markieren und die Vorlage separat darauf anwenden.

Um eine Vorlage mit einem Satz von Sicherheitsparametern für einen ausgewählten Knoten zu übernehmen, gehen Sie wie folgt vor:

1. Speichern Sie den Satz mit Sicherheitsparameterwerten vorher in einer Vorlage (s. S. 69).
2. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie den untergeordneten Knoten **Echtzeitschutz für Dateien**.
3. Öffnen Sie im Ergebnisfenster der Dateistruktur des Servers auf der Registerkarte **Schutzbereich anpassen** das Kontextmenü, indem Sie mit der rechten Maustaste auf den Knoten klicken, für den Sie die Vorlage übernehmen möchten, wählen Sie den Punkt **Vorlage übernehmen → <Vorlagenname>**.
4. öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl Aufgabe speichern, um die Änderungen in der Aufgabe zu speichern.

VORLAGE LÖSCHEN

Um eine Vorlage zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und wählen Sie den Befehl **Vorlagen für Einstellungen**.
3. Wählen Sie in der Vorlagenliste im Fenster **Vorlagen** die zu löschende Vorlage aus und klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**. Die gewählte Vorlage wird gelöscht.

SCHUTZMODUS FÜR OBJEKTE AUSWÄHLEN

Sie können den Schutzmodus für Objekte in der Aufgabe **Echtzeitschutz für Dateien** auswählen.

Um den Schutzmodus für Objekte auszuwählen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und wählen Sie den Punkt **Eigenschaften**.
3. Wählen Sie im Fenster **Eigenschaften: Echtzeitschutz für Dateien** auf der Registerkarte **Allgemein** einen Schutzmodus für Objekte aus und klicken Sie auf **OK**.

ÜBERNAHME VON DER HEURISTISCHE ANALYSE IN DER AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN.

In den Aufgabe **Echtzeitschutz für Dateien** können Sie die heuristische Analyse anwenden und das Analyseniveau konfigurieren.

Um die heuristische Analyse zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Öffnen Sie das Kontextmenü für die Aufgabe **Echtzeitschutz für Dateien** und gehen Sie auf **Eigenschaften**.
3. Aktivieren Sie im Fenster **Eigenschaften: Echtzeitschutz für Dateien** auf der Registerkarte **Allgemein** das Kontrollkästchen **Heuristische Analyse verwenden** und passen Sie die Analysestufe an.

   Um die heuristische Analysemethode auszuschalten, entfernen Sie das Häkchen im Kontrollkästchen **Heuristische Analyse verwenden**.
4. Klicken Sie auf **OK**.

STATISTIK FÜR DIE AUFGABE ECHTZEITSCHUTZ FÜR DATEIEN

Während die Aufgabe **Echtzeitschutz für Dateien** ausgeführt wird, können Sie in Echtzeit Informationen über die Anzahl der Objekte, die Kaspersky Anti-Virus seit seinem Start bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen lassen: Aufgabenstatistik.

*Um die Statistik der Aufgabe **Echtzeitschutz für Dateien** anzusehen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Wählen Sie die Aufgabe **Echtzeitschutz für Dateien**.
3. Klicken Sie auf der Registerkarte **Übersicht und Verwaltung** des Ergebnisfensters im Abschnitt **Statistik** auf den Link **Vollständige Statistik**.

Sie können folgende Informationen über Objekte anzeigen, die Kaspersky Anti-Virus seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat (s. Tabelle unten).

*Tabelle 12. Einstellungen der Aufgabe **Echtzeitschutz für Dateien**, **Vollständige Statistik***

FELD	BESCHREIBUNG
Gefunden	Anzahl der Objekte, die Kaspersky Anti-Virus gefunden hat. Findet Kaspersky Anti-Virus beispielsweise in fünf Dateien ein und dasselbe Schadprogramm, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Gefundene infizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus als infiziert eingestuft wurden.
Gefundene möglicherweise infizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft wurden.
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus aus folgenden Gründen nicht desinfiziert wurden: • Eine Desinfektion ist aufgrund des Typs des gefundenen Objekts nicht erforderlich. • Bei der Desinfektion ist eine Störung aufgetreten.
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Kaspersky Anti-Virus versucht hat, in die Quarantäne zu verschieben, was aber fehlgeschlagen ist, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Nicht gelöschte Objekte	Anzahl der Objekte, die Kaspersky Anti-Virus zu löschen versucht hat, was aber fehlgeschlagen ist, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht untersuchte Objekte	Anzahl der zum Schutzbereich gehörenden Objekte, die Kaspersky Anti-Virus nicht untersuchen konnte, da beispielsweise der Zugriff auf ein Objekt durch ein anders Programm gesperrt war.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Anti-Virus ins Backup zu kopieren versucht hat, was aber fehlgeschlagen ist, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Verarbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus desinfiziert wurden.

FELD	BESCHREIBUNG
In die Quarantäne verschoben	Anzahl der Objekte, die von Kaspersky Anti-Virus in die Quarantäne verschoben wurden.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Anti-Virus im Backup gespeichert wurden.
Gelöschte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus gelöscht wurden.
Kennwortgeschützte Objekte	Anzahl der Objekte (z.B. Archive), die von Kaspersky Anti-Virus übersprungen wurden, weil diese Objekte kennwortgeschützt sind.
Beschädigte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus übersprungen wurden, da ihr Format nicht ermittelt werden konnte.
Verarbeitete Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus verarbeitet wurden.

ANPASSEN DER AUFGABE SKRIPT-UNTERSUCHUNG

Die Systemaufgabe **Skript-Untersuchung** besitzt standardmäßig die in der Tabelle beschriebenen Parameter. Sie können die Werte dieser Parameter ändern und die Aufgabe anpassen.

*Tabelle 13. Standardmäßige Parameter der Aufgabe **Skript-Untersuchung***

EINSTELLUNGEN	STANDARDWERT	BESCHREIBUNG
Ausführung gefährlicher Skripts	Verboten	Die Ausführung von Skripts, die als gefährlich erkannt werden, wird von Kaspersky Anti-Virus immer verboten.
Ausführung potenziell gefährlicher Skripts	Verboten	Sie können die Aktionen festlegen, die Kaspersky Anti-Virus mit Skripten ausführen soll, die als potentiell gefährlich eingestuft werden: Ausführung verbieten oder erlauben.
Heuristische Analyse	Wählen Sie die Sicherheitsstufe **Mittel** aus.	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. Anlegen und Verwendung der vertrauenswürdigen Zone (s. S. 77)

➧ *Um die Aufgabe **Skript-Untersuchung** anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz** und wählen Sie die Aufgabe **Skript-Untersuchung**.

   Klicken Sie auf den Link **Eigenschaften**, um das Fenster **Eigenschaften: Skript-Untersuchung** zu öffnen.

2. Erlauben oder verbieten Sie in der Optionsgruppe **Aktionen für potentiell gefährliche Skripte** die Ausführung verdächtiger Skripts. Gehen Sie hierzu wie folgt vor:

   - Um die Ausführung potenziell gefährlicher Skripts zu erlauben, wählen Sie **Ausführung erlauben**.
   - Um die Ausführung potenziell gefährlicher Skripts zu verbieten, wählen Sie **Ausführung sperren**.

3. Nehmen Sie in der Optionsgruppe **Heuristische Analyse** folgende Einstellungen vor:

   - Um die heuristische Analyse einzuschalten, aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**. Um die Analysegenauigkeit zu ändern, wählen Sie die gewünschte Stufe mit dem Schieberegler.
   - Um die heuristische Analyse auszuschalten, entfernen Sie das Häkchen im Kontrollkästchen **Heuristische Analyse verwenden**.

4. Aktivieren oder deaktivieren Sie in der Optionsgruppe **Vertrauenswürdige Zone** die Verwendung der vertrauenswürdigen Zone wie folgt:

   - Um die Verwendung der vertrauenswürdigen Zone zu aktivieren, kreuzen Sie das Kontrollkästchen **Vertrauenswürdige Zone übernehmen** an.
   - Um die Verwendung der vertrauenswürdigen Zone zu deaktivieren, entfernen Sie das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.

   Informationen über das Hinzufügen von Skripts zur Liste der Ausnahmen für die vertrauenswürdige Zone (s. S. 80)

5. Klicken Sie im Fenster **Eigenschaften: Skript-Untersuchung** auf die Schaltfläche **OK**, um die Änderungen zu speichern.

STATISTIK FÜR DIE AUFGABE SKRIPT-UNTERSUCHUNG

Während die Aufgabe **Skript-Untersuchung** ausgeführt wird, können Sie in Echtzeit Informationen über Anzahl der Skripts, die Kaspersky Anti-Virus seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen: Aufgabenstatistik.

Um die Aufgabenstatistik anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur den Knoten **Echtzeitschutz**.
2. Wählen Sie die Aufgabe **Skript-Untersuchung**.

   Sie können sich die Parameter der Aufgabe **Skript-Untersuchung** anzeigen lassen (s. Tabelle unten).

Tabelle 14. Parameter der Aufgabe Skript-Untersuchung, Vollständige Statistik

FELD	BESCHREIBUNG
Gesperrte Skripts	Anzahl der Skripts, deren Ausführung von Kaspersky Anti-Virus verboten wurde
Erkannten gefährliche Skripts	Anzahl der erkannten gefährlichen Skripts
Erkennen potenziell gefährlicher Skripts	Anzahl der erkannten potenziell gefährlichen Skripts
Verarbeitete Skripts	Anzahl der verarbeiteten Skripts

LISTE DER ERWEITERUNGEN VON DATEIEN, DIE STANDARDMÄßIG UNTERSUCHT WERDEN

ECHTZEITSCHUTZ FÜR DATEIEN

In der Grundeinstellung untersucht Kaspersky Anti-Virus Dateien, die die folgenden Erweiterungen besitzen:

386; *acm*; *ade*, *adp*; *asp*; *asx*; *ax*; *bas*; *bat*; *bin*; *chm*; *cla*, *clas**; *cmd*; *com*; *cpl*; *crt*; *dll*; *dpl*; *drv*; *dvb*; *dwg*; *efi*; *emf*; *eml*; *exe*; *fon*; *fpm*; *hlp*; *hta*; *htm*, *html**; *htt*; *ico*; *inf*; *ini*; *ins*; *isp*; *jpg*, *jpe*;

js, *jse*;
lnk;
mbx;
msc;
msg;
msi;
msp;
mst;
nws;
ocx;
oft;
otm;
pcd;
pdf;
php;
pht;
*phtm**;
pif;
plg;
png;
pot;
prf;
prg;
reg;
rsc;
rtf;
scf;
scr;
sct;
shb;
shs;
sht;
*shtm**;
swf;
sys;
the;
*them**;
tsp;
url;
vb;
vbe;
vbs;
vxd;
wma;
wmf;
wmv;
wsc;
wsf;
wsh;
do?;
md?;
mp?;
ov?;
pp?;
vs?;
xl?.

VIRENSUCHE

Dieser Abschnitt enthält Informationen über die Aufgaben zur Untersuchung auf Befehl und Anweisungen zum Anpassen der Einstellungen der Aufgaben zur Untersuchung auf Befehl sowie zum Anpassen der Sicherheitseinstellungen für Aufgaben zur Untersuchung auf Befehl.

IN DIESEM ABSCHNITT

AUFGABEN ZUR VIRENSUCHE

Kaspersky Anti-Virus überprüft den angegebenen Bereich einmalig auf Viren und andere Bedrohungen der Computersicherheit. Kaspersky Anti-Virus überprüft Daten, den Arbeitsspeicher des Servers sowie Autostart-Objekte.

In Kaspersky Anti-Virus sind vier Systemaufgaben zur Untersuchung auf Befehl vorgesehen:

- Die Aufgabe **Untersuchung kritischer Bereiche** wird standardmäßig wöchentlich nach Zeitplan ausgeführt. Kaspersky Anti-Virus untersucht Objekte, die sich in kritischen Bereichen des Betriebssystems befinden: Autostart-Objekte, Bootsektoren und Master-Bootsektoren von Festplatten und Wechseldatenträgern, Arbeitsspeicher und Prozessspeicher. Er untersucht Dateien, die sich in Systemordnern befinden, z.B. im Ordner %windir%\system32. Anti-Virus verwendet Sicherheitsparameter, deren Werte der Stufe **Empfohlen** (s. S. 72) entsprechen. Sie können die Parameter für die Aufgabe **Untersuchung kritischer Bereiche ändern**.
- Die Aufgabe **Untersuchung von Quarantäne-Objekten** wird standardmäßig jedes Mal nach dem Update der Datenbanken nach Zeitplan ausgeführt. Sie können die Einstellungen für die Aufgabe **Untersuchung von Quarantäne-Objekten** (s. S. 84) ändern.
- Die Aufgabe **Untersuchung beim Hochfahren des Betriebssystems** wird jedes Mal ausgeführt, wenn Kaspersky Anti-Virus gestartet wird. Kaspersky Anti-Virus untersucht die Bootsektoren und Master-Bootsektoren der Festplatten und Wechseldatenträger, sowie den Arbeits- und Prozessspeicher. Jedes Mal, wenn die Aufgabe ausgeführt wird, legt Kaspersky Anti-Virus eine Kopie der virenfreien Bootsektoren an. Wenn bei der nächsten Untersuchung eine Bedrohung darin gefunden wird, werden infizierte Bootsektoren durch die Sicherungskopien ersetzt.
- Die Aufgabe **Programmintegrität prüfen** wird bei jedem Start von Kaspersky Anti-Virus ausgeführt. Sie gewährleistet die Untersuchung der Module von Kaspersky Anti-Virus auf Beschädigungen oder Änderungen. Es wird der Installationsordner des Programms geprüft. Die Statistik über die Aufgabenausführung enthält Angaben über die Anzahl der untersuchten und beschädigten Module. Die Parameterwerte einer Aufgabe werden vom Programm vorgegeben und lassen sich nicht ändern. Die Parameterwerte für einen Zeitplan lassen sich dagegen für so eine Aufgabe ändern.

Sie können benutzerdefinierte Untersuchungsaufgaben erstellen. Beispielweise können Sie eine Aufgabe zur Untersuchung der gemeinsamen Ordner auf dem Server erstellen.

Kaspersky Anti-Virus kann gleichzeitig mehrere Untersuchungsaufgaben ausführen.

Kategorien der Anti-Virus-Aufgaben nach Erstellungs- und Ausführungsort

Funktionen "Echtzeitschutz" und "Virensuche"

Aufgabenverwaltung in der Anti-Virus-Konsole (s. S. 38)

ANPASSEN VON AUFGABEN ZUR VIRENSUCHE

Die Systemaufgabe **Untersuchung kritischer Bereiche** und benutzerdefinierte Untersuchungsaufgaben können angepasst werden (s. Tabelle unten).

Informationen darüber, wie eine benutzerdefinierte Aufgabe erstellt wird, finden Sie im Pkt. "Aufgabe zur Virensuche erstellen" (s. S 38).

Tabelle 15. Standardparameter für eine neu erstellte Untersuchungsaufgabe

EINSTELLUNGEN	BEDEUTUNG	EINSTELLUNGSMÖGLICHKEITEN
Untersuchungsbereich	Gesamter Server	Sie können den Schutzbereich ändern (s. S. 68).
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, entspricht der Sicherheitsstufe **Empfohlen**.	Sie können für die ausgewählten Knoten in der Dateistruktur des Servers folgende Aktionen ausführen: • eine andere vordefinierte Sicherheitsstufe auswählen (s. S. 72); • Sicherheitseinstellungen manuelll ändern (s. S. 73) Sie können die Sicherheitseinstellungen des ausgewählten Knotens in einer Vorlage speichern, um sie später für andere Knoten zu übernehmen (s. S. 69).
Heuristische Analyse	Die Analysestufe **Mittel** wird verwendet.	Sie können die Verwendung der heuristischen Analyse aktivieren und deaktivieren und die Analysegenauigkeit einstellen.
Vertrauenswürdige Zone	Wird verwendet Das Programme zur Remote-Administration **RemoteAdmin** wird ausgeschlossen, wenn Sie bei der Installation von Kaspersky Anti-Virus **Objekte nach der Maske not-a-virusRemoteAdmin* zu Ausnahmen hinzufügen** ausgewählt haben.	Einheitliche Liste der Ausnahmen, die Sie für die ausgewählten Aufgaben zur Untersuchung auf Befehl sowie für die Aufgaben **Echtzeitschutz für Dateien**, **Skript-Untersuchung** und **RPC: Schutz von Netzwerkspeichern** anwenden können. Beachten Sie auch die Informationen darüber, wie die vertrauenswürdige Zone angelegt und verwendet wird (s. S. 77)

Um eine neue Aufgabe zur Virensuche zu konfigurieren, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Wählen Sie die Aufgabe aus, die Sie anpassen möchten.
3. Auf der Registerkarte **Untersuchungsbereich anpassen** passen Sie die Aufgabenparameter an: legen Sie den Untersuchungsbereich fest. Ändern Sie bei Bedarf die Sicherheitseinstellungen des gesamten Untersuchungsbereichs oder der einzelnen Knoten. Neu erstellte benutzerdefinierte Aufgaben besitzen standardmäßig die in der obigen Tabelle genannten Einstellungen.
4. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

IN DIESEM ABSCHNITT

UNTERSUCHUNGSBEREICH IN DEN AUFGABEN ZUR UNTERSUCHUNG AUF BEFEHL

IN DIESEM ABSCHNITT

IN AUFGABEN ZUR VIRENSUCHE EINEN UNTERSUCHUNGSBEREICH FESTLEGEN

In neu erstellten Aufgaben zur Untersuchung auf Befehl ist standardmäßig der gesamte Server im Untersuchungsbereich enthalten. Wenn es aus Sicherheitsgründen nicht nötig ist, alle Objekte zu untersuchen, können Sie den Untersuchungsbereich auf bestimmte Serverbereiche beschränken.

In der Konsole von Kaspersky Anti-Virus wird der Untersuchungsbereich als Baumstruktur jener Dateien des Servers dargestellt, die von Kaspersky Anti-Virus untersucht werden können.

Die Knoten der Dateistruktur des Servers werden auf folgende Weise dargestellt:

☑ Der Knoten gehört zum Untersuchungsbereich.

☐ Der Knoten gehört nicht zum Untersuchungsbereich.

☑ Mindestens ein diesem Knoten untergeordneter Knoten gehört nicht zum Untersuchungsbereich oder die Sicherheitsparameter des untergeordneten Knotens unterscheiden sich von den Sicherheitsparametern dieses Knotens.

Die Namen von virtuellen Knoten eines Untersuchungsbereichs werden mit blauer Schrift angezeigt.

VORDEFINIERTE UNTERSUCHUNGSBEREICHE

➧ *Um die Dateistruktur des Servers anzusehen, gehen Sie wie folgt vor:*

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Um eine Aufgabe zu öffnen, wählen Sie die Aufgabe zur Untersuchung auf Befehl, dessen Untersuchungsbereich Sie anzeigen möchten.

   Im Ergebnisfenster, auf der Registerkarte **Untersuchungsbereich anpassen** wird die Dateistruktur des Servers angezeigt, aus deren Objekten Sie einen Untersuchungsbereich erstellen können.

Die Dateistruktur des Servers enthält die folgenden vordefinierten Bereiche:

- **Arbeitsplatz**. Kaspersky Anti-Virus untersucht den gesamten Server.
- **Lokale Festplatten**. Kaspersky Anti-Virus untersucht Objekte auf den Festplatten des Servers. Sie können alle Festplatten sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.
- **Wechseldatenträger**. Kaspersky Anti-Virus untersucht die Objekte auf Wechseldatenträgern, z.B. auf CDs oder USB-Sticks. Sie können alle Wechseldatenträger sowie einzelne Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen oder daraus ausschließen.
- **Netzwerkumgebung**. Sie können dem Untersuchungsbereich Netzwerkordner oder Dateien hinzufügen, indem Sie die Netzwerkpfade im UNC-Format (Universal Naming Convention) angeben. Das für den Aufgabenstart verwendete Benutzerkonto muss über Zugriffsrechte für die hinzugefügten Netzwerkordner oder Dateien verfügen. In der Grundeinstellung werden alle Untersuchungsaufgaben mit dem Benutzerkonto **Lokales System** (**SYSTEM**) ausgeführt. Details finden Sie im Pkt. "Netzlaufwerke, Ordner oder Dateien in den Untersuchungsbereich aufnehmen" (s. S. 70).

- **Systemspeicher**. Kaspersky Anti-Virus untersucht ausführbare Dateien und Module von Prozessen, die während der Untersuchung im Betriebssystem ausgeführt werden.
- **Autostart-Objekte**. Kaspersky Anti-Virus untersucht Objekte, auf die durch Registrierungsschlüssel und Konfigurationsdateien verwiesen wird, z.B. WIN.INI oder SYSTEM.INI, sowie Programm-Module von Anwendungen, die beim Hochfahren des Computers automatisch gestartet werden.
- **Freigegebene Ordner**. Kaspersky Anti-Virus untersucht alle gemeinsamen Ordner auf dem geschützten Server.
- **Virtuelle Festplatten**. Sie können in den Schutzbereich dynamische Ordner und Dateien sowie Datenträger aufnehmen, die temporär vom Server überwacht werden, beispielsweise allgemeine Datenträger eines Clusters (Anlegen eines virtuellen Schutzbereiches). Details finden Sie im Abschnitt "Virtuellen Untersuchungsbereich erstellen: Dynamische Datenträger, Ordner oder Dateien in den Untersuchungsbereich aufnehmen" (s. S. 71).

Pseudo-Laufwerke, die mit dem Befehl SUBST erzeugt wurden, werden nicht in der Dateistruktur des Servers in der Konsole von Kaspersky Anti-Virus angezeigt. Um Objekte auf einem Pseudo-Laufwerk zu untersuchen, nehmen Sie den Ordner auf dem Server, mit dem dieses Pseudo-Laufwerk verbunden ist, in den Schutzbereich auf.

Verbundene Netzlaufwerke werden nicht in der Dateistruktur des Servers angezeigt. Um Objekte auf einem Netzlaufwerk in den Untersuchungsbereich aufzunehmen, geben Sie den Pfad des Ordners an, der diesem Netzlaufwerk entspricht. Verwenden Sie das UNC-Format (Universal Naming Convention).

UNTERSUCHUNGSBEREICH FESTLEGEN

Wenn Sie Kaspersky Anti-Virus auf dem geschützten Server im Remote-Betrieb über die Konsole von Kaspersky Anti-Virus verwalten, die am Remote-Arbeitsplatz des Administrators installiert ist, müssen Sie zur Gruppe der Administratoren auf dem geschützten Server gehören, um die dort befindlichen Ordner zu sehen.

Wenn Sie den Untersuchungsbereich in den Aufgaben **Untersuchung beim Hochfahren des Betriebssystems** und **Untersuchung kritischer Bereiche** geändert haben, können Sie in diesen Aufgaben den standardmäßigen Untersuchungsbereich wiederherstellen. Führen Sie dazu die Wiederherstellung von Kaspersky Anti-Virus aus (**Start → Programme → Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Ändern oder Löschen**). Aktivieren Sie im Assistenten das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**.

Um einen Untersuchungsbereich anzulegen, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Wählen Sie die Untersuchungsaufgabe, deren Untersuchungsbereich Sie anpassen möchten.
3. Im Ergebnisfenster auf der Registerkarte **Untersuchungsbereich anpassen** wird die Dateistruktur des Servers angezeigt. In neu erstellten Untersuchungsaufgaben sind standardmäßig alle Bereiche des geschützten Servers im Untersuchungsbereich enthalten.
4. Führen Sie folgende Aktionen aus:
   - Um die Knoten auszuwählen, die Sie dem Untersuchungsbereich hinzufügen möchten, deaktivieren Sie das Kontrollkästchen **Arbeitsplatz** und gehen Sie folgendermaßen vor:
     - Wenn Sie alle Datenträger eines bestimmten Typs in den Untersuchungsbereich aufnehmen möchten, aktivieren Sie das Kontrollkästchen für den entsprechenden Datenträgertyp.
     - Wenn Sie einen einzelnen Datenträger in den Untersuchungsbereich aufnehmen möchten, öffnen Sie den Knoten, der eine Liste der Datenträger dieses Typs enthält, und aktivieren Sie das Kontrollkästchen für den entsprechenden Datenträger. Um z.B. den Wechseldatenträger **F:** auszuwählen, öffnen Sie den Knoten **Wechseldatenträger** und aktivieren Sie das Kontrollkästchen für Laufwerk **F**:.
     - Wenn Sie einen bestimmten Ordner auf einem Datenträger in den Untersuchungsbereich aufnehmen möchten, öffnen Sie die Dateistruktur des Servers und aktivieren Sie das Kontrollkästchen für den betreffenden Ordner. Auf gleiche Weise können auch Dateien in den Untersuchungsbereich aufgenommen werden.
   - Um einen einzelnen Knoten aus dem Untersuchungsbereich auszuschließen, öffnen Sie die Dateistruktur des Servers und deaktivieren Sie das Kontrollkästchen für den betreffenden Knoten.
5. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Sehen Sie sich die folgenden Abschnitte an, wenn Sie Informationen benötigen, wie Sie Folgendes in den Untersuchungsbereich einschließen können:

- Netzwerk-Datenträger, Ordner oder Datei (s. S. 70).
- Dynamische Datenträger, Ordner oder Datei (s. S. 70).

IN UNTERSUCHUNGSAUFGABEN MIT VORLAGEN ARBEITEN

IN DIESEM ABSCHNITT

SICHERHEITSEINSTELLUNGEN IN EINER VORLAGE SPEICHERN

In der Aufgabe zur Untersuchung auf Befehl können Sie, nachdem die Sicherheitseinstellungen eines bestimmten Knotens in der Dateistruktur des Servers angepasst wurden, diesen Parametersatz in einer Vorlage speichern. Sie können diese Vorlage später zur Konfiguration der Sicherheitseinstellungen anderer Knoten in dieser Aufgabe oder in anderen Aufgaben zur Untersuchung auf Befehl übernehmen.

Sie können Vorlagen, die in der Aufgabe zur **Untersuchung auf Befehl** angelegt wurden, zur Konfiguration der Sicherheitseinstellungen in den Aufgaben **Echtzeitschutz für Dateien** und **RPC: Schutz von Netzwerkspeichern** verwenden.

Um einen Satz von Sicherheitseinstellungenn in einer Vorlage zu speichern, gehen Sie wie folgt vor:

1. In der Konsolenstruktur markieren Sie den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie die Aufgabe zur Virensuche, deren Sicherheitseinstellungen Sie in einer Vorlage speichern möchten.
3. Auf der Registerkarte **Untersuchungsbereich anpassen**, in der Dateistruktur des Servers, wählen Sie den Knoten, dessen Sicherheitseinstellungen Sie speichern möchten.
4. Klicken Sie im Fenster **Sicherheitseinstellungen** auf der Registerkarte **Allgemein** auf die Schaltfläche **Als Vorlage speichern**.
5. Geben Sie im Fenster **Eigenschaften der Vorlage** im Feld **Vorlagenname** den Namen der Vorlage ein.
6. Tragen Sie im Feld **Beschreibung** beliebige Zusatzinformationen über die Vorlage ein.
7. Klicken Sie auf **OK**. Die Vorlage wird mit den entsprechenden Parameterwerten gespeichert.

SICHERHEITSEINSTELLUNGEN IN EINER VORLAGE ANZEIGEN

Um die Werte der Sicherheitseinstellungen in einer vorhandenen Vorlage anzuzeigen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Untersuchung auf Befehl** und wählen Sie den Befehl **Vorlagen für Einstellungen** aus.

   Im Fenster **Vorlagen** wird eine Liste der Vorlagen angezeigt, die Sie in den Aufgaben zur Untersuchung auf Befehl übernehmen können.
2. Um Informationen über eine Vorlage und die entsprechenden Werte für die Sicherheitseinstellungen anzuzeigen, wählen Sie die gewünschte Vorlage in der Liste und klicken Sie auf die Schaltfläche **Anzeigen**.

   Auf der Registerkarte **Allgemein** werden der Name der Vorlage und Zusatzinformationen über die Vorlage angezeigt. Die Registerkarte **Einstellungen** enthält eine Liste mit den in der Vorlage gespeicherten Werten der Sicherheitseinstellungen.

VORLAGE ÜBERNEHMEN

Wenn Sie eine Vorlage für einen übergeordneten Knoten übernehmen, werden die Sicherheitseinstellungen der Vorlage auch für alle untergeordneten Knoten übernommen, mit Ausnahme der folgenden Situationen:

- Die Vorlage gilt nicht für Elemente, deren Sicherheitseinstellungen Sie separat konfiguriert haben. Um die Sicherheitseinstellungen aus einer Vorlage für alle untergeordneten Knoten zu übernehmen, deaktivieren Sie vor dem Übernehmen der Vorlage in der Dateistruktur des Servers das Kontrollkästchen des übergeordneten Knotens, und aktivieren Sie es anschließend wieder. Übernehmen Sie die Vorlage für den übergeordneten Knoten. Alle untergeordneten Knoten erhalten nun die gleichen Sicherheitseinstellungen wie der übergeordnete Knoten.
- Die Vorlage wird nicht auf die angepassten Netzlaufwerke, Ordner und Dateien angewendet.

Um eine Vorlage mit Sicherheitsparametern zu übernehmen, gehen Sie wie folgt vor:

1. Speichern Sie den Satz mit Sicherheitseinstellungen vorher in einer Vorlage (s. Seite 59).
2. In der Konsolenstruktur markieren Sie den Knoten **Untersuchung auf Befehl**.
3. Wählen Sie die Aufgabe zur Virensuche, in der Sie die die Sicherheitseinstellungen übernehmen möchten.
4. Öffnen Sie in der Dateistruktur des Servers auf der Registerkarte **Untersuchungsbereich anpassen** das Kontextmenü für den Knoten, für den Sie eine Vorlage übernehmen möchten, und wählen Sie den Punkt **Vorlage übernehmen** → **<Vorlagenname>** aus.
5. Klicken Sie im Fenster **Sicherheitseinstellungen** auf **OK**, um die Änderungen zu speichern.

VORLAGE LÖSCHEN

Um eine Vorlage zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Untersuchung auf Befehl** und wählen Sie den Befehl **Vorlagen für Einstellungen** aus.
2. Wählen Sie in der Vorlagenliste im Fenster **Vorlagen** die zu löschende Vorlage aus und klicken Sie auf die Schaltfläche **Löschen**.
3. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**. Die gewählte Vorlage wird gelöscht.

NETZLAUFWERKE, ORDNER ODER DATEIEN IN DEN UNTERSUCHUNGSBEREICH AUFNEHMEN

Sie können Netzlaufwerke, Ordner und Dateien in den Untersuchungsbereich aufnehmen. Geben Sie dazu die Netzwerkpfade im UNC-Format (Universal Naming Convention) an.

Bei der Arbeit mit dem Benutzerkonto **Lokales System** (**Local System**) besitzt der Benutzer keine Möglichkeit, Netzwerkordner zu scannen.

Um ein Netzwerkobjekt zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Wählen Sie die Untersuchungsaufgabe, zu deren Untersuchungsbereich Sie einen Netzwerkpfad hinzufügen möchten.
3. Auf der Registerkarte **Untersuchungsbereich anpassen** öffnen Sie das Kontextmenü für den Knoten **Netzwerkumgebung** und wählen Sie den Befehl **Netzwerkordner hinzufügen** oder **Netzwerkordner hinzufügen**.
4. Geben Sie den Pfad des Netzwerkordners oder der Netzwerkdatei im UNC-Format (Universal Naming Convention) an und drücken Sie die **EINGABE**-Taste.
5. Aktivieren Sie das Kontrollkästchen für das hinzugefügte Netzwerkobjekt, um es in den Untersuchungsbereich aufzunehmen.
6. Ändern Sie bei Bedarf die Sicherheitseinstellungen für das hinzugefügte Netzwerkobjekt (s. Pkt "Anpassen von Sicherheitseinstellungen in Aufgaben zur Virensuche" auf S. 71).
7. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

VIRTUELLE UNTERSUCHUNGSBEREICHE ERSTELLEN: DYNAMISCHE DATENTRÄGER, ORDNER UND DATEIEN IN UNTERSUCHUNGSBEREICH ÜBERNEHMEN

In den Untersuchungsbereich können folgende Elemente aufgenommen werden: dynamische Festplatten, Ordner und Dateien, sowie Festplatten, die in den Server eingebunden werden, beispielsweise gemeinsame Cluster-Datenträger. So wird ein virtueller Untersuchungsbereich angelegt.

Sie können einzelne virtuelle Laufwerke, Ordner oder Dateien nur dann zum Schutzbereich bzw. Untersuchungsbereich hinzufügen, wenn der Schutzbereich bzw. Untersuchungsbereich als Dateistruktur dargestellt wird.

Um ein virtuelles Laufwerk zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Um eine Aufgabe zu öffnen, markieren Sie die Untersuchungsaufgabe, in der Sie einen virtuellen Untersuchungsbereich erstellen möchten.
3. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Untersuchungsbereich anpassen** in der Dateistruktur des Servers das Kontextmenü für den Knoten **Virtuelle Festplatten** und wählen Sie in der Liste der verfügbaren Namen einen Namen für die anzulegende virtuelle Festplatte.
4. Aktivieren Sie das Kontrollkästchen für den hinzugefügten Datenträger, um den Datenträger in den Untersuchungsbereich aufzunehmen.
5. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

Um einen virtuellen Ordner oder eine virtuelle Datei zum Untersuchungsbereich hinzuzufügen, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Um eine Aufgabe zu öffnen, markieren Sie die Untersuchungsaufgabe, in der Sie einen virtuellen Untersuchungsbereich erstellen möchten.
3. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Untersuchungsbereich anpassen** in der Dateistruktur des Servers, das Kontextmenü für den Knoten des virtuellen Laufwerks, zu dem Sie einen Ordner oder eine Datei hinzufügen möchten, und wählen Sie den Befehl **Virtuellen Ordner hinzufügen** oder **Virtuelle Datei hinzufügen**.
4. Tragen Sie im Eingabefeld den Namen für den Ordner (die Datei) ein. Sie können eine Maske für den Namen des Ordners (der Datei) angeben. Für Masken können die Sonderzeichen ***** und **?** verwendet werden.
5. Aktivieren Sie das Kontrollkästchen in der Zeile mit dem Namen des neuen Ordners (der neuen Datei), um den Ordner (die Datei) in den Untersuchungsbereich aufzunehmen.
6. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

ANPASSEN VON SICHERHEITSEINSTELLUNGEN IN AUFGABEN ZUR VIRENSUCHE

In einer ausgewählten Aufgabe zur Untersuchung auf Befehl können Sie die Sicherheitseinstellungen entweder durch Angabe einheitlicher Werte für den gesamten Untersuchungsbereich oder individuell für bestimmte Knoten in der Dateistruktur des Servers festlegen. Die Sicherheitseinstellungen, die Sie für einen ausgewählten Knoten festlegen, werden automatisch für alle untergeordneten Knoten übernommen. Wenn Sie für einen untergeordneten Knoten aber individuelle Sicherheitseinstellungen festlegen, gelten die Sicherheitseinstellungen des übergeordneten Knoten nicht für ihn.

Sie können die Parameter eines ausgewählten Untersuchungsbereichs auf eine der folgenden Weisen anpassen:

- Sie können eine der drei vordefinierten Sicherheitsstufen wählen (Maximale Leistung, Empfohlen oder Maximale Sicherheit).
- Sie können die Sicherheitseinstellungen ausgewählter Knoten in der Dateistruktur des Servers manuell anpassen.

Sie können den Parametersatz eines Knotens in einer Vorlage speichern, um diese Vorlage später für andere Knoten zu übernehmen.

IN DIESEM ABSCHNITT

VORDEFINIERTE SICHERHEITSSTUFEN IN AUFGABEN ZUR VIRENSUCHE AUSWÄHLEN

Für den ausgewählten Knoten in der Dateistruktur des Servers können Sie eine der drei folgenden vordefinierten Sicherheitsstufen festlegen: Maximale Leistung, Empfohlen und Maximale Sicherheit. Jede vordefinierte Sicherheitsstufe besitzt bestimmte Werte für die Sicherheitseinstellungen (s. Tabelle unten).

Maximale Leistung

Die Sicherheitsstufe **Maximale Leistung** wird für den Server empfohlen, wenn in Ihrem Netzwerk neben Kaspersky Anti-Virus auf Servern und Workstations noch zusätzliche Maßnahmen für die Computersicherheit getroffen werden. Dazu zählen beispielsweise der Einsatz von Firewalls und von Sicherheitsrichtlinien für die Netzwerkbenutzer.

Empfohlen

Die Sicherheitsstufe **Empfohlen** bietet ein optimales Gleichgewicht zwischen Schutzniveau und Ressourcenauslastung der geschützten Server. Diese Stufe ist laut Empfehlung der Kaspersky-Lab-Experten für den Schutz von Dateiservern in den meisten Unternehmensnetzwerken ausreichend. Die Sicherheitsstufe **Empfohlen** gilt als Standard.

Maximale Sicherheit

Die Anwendung der Sicherheitsstufe **Maximale Sicherheit** wird empfohlen, wenn Sie erhöhten Wert auf die Computersicherheit des Unternehmensnetzwerks legen.

Tabelle 16. Vordefinierte Sicherheitsstufen und entsprechende Werte für die Sicherheitseinstellungen

EINSTELLUNGEN	VORDEFINIERTE SICHERHEITSSTUFE		
	MAXIMALE LEISTUNG	EMPFOHLEN	MAXIMALE SICHERHEIT
Objekte untersuchen	Nach Format	Alle Objekte	Alle Objekte
Optimierung	Aktiviert	Deaktiviert	Deaktiviert
Aktionen für infizierte Objekte	Desinfizieren. Irreparable Objekte löschen	Desinfizieren. Irreparable Objekte löschen	Desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte.	In Quarantäne verschieben	In Quarantäne verschieben	In Quarantäne verschieben
Objekte ausschließen	Nein	Nein	Nein
Nicht erkennen	Nein	Nein	Nein
Untersuchung beenden, wenn sie länger dauert als (Sek.)	60 Sek.	Nein	Nein
Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	8 MB	Nein	Nein
Alternative NTFS-Ströme	Ja	Ja	Ja
Bootsektoren und MBR	Ja	Ja	Ja

EINSTELLUNGEN	VORDEFINIERTE SICHERHEITSSTUFE		
	MAXIMALE LEISTUNG	EMPFOHLEN	MAXIMALE SICHERHEIT
Zusammengesetzte Objekte untersuchen	• SFX-Archive* • Gepackte Objekte* • eingebettete OLE-Objekte* * Nur neue und veränderte	• Archive* • SFX-Archive* • Gepackte Objekte* • eingebettete OLE-Objekte* * Alle Objekte	• Archive* • SFX-Archive* • Mail-Datenbanken* • Dateien in Mail-Formaten* • Gepackte Objekte* • eingebettete OLE-Objekte* * Alle Objekte
Verarbeitung autonomer Dateien	Ja	Ja	Ja

Beachten Sie, dass die Sicherheitseinstellungen **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden**, **Heuristische Analyse verwenden und Dateien auf Microsoft-Signatur überprüfen** nicht zum Einstellungssatz der vordefinierten Sicherheitsstufen gehören. Wenn Sie den Status der Einstellungen **iChecker-Technologie verwenden**, **iSwift-Technologie verwenden**, **Heuristische Analyse verwenden** oder **Dateien auf Microsoft-Signatur prüfen** ändern, ändert sich die von Ihnen gewählte vordefinierte Sicherheitsstufe nicht.

Um eine vordefinierte Sicherheitsstufe auszuwählen, gehen Sie wie folgt vor:

1. In der Konsolenstruktur markieren Sie den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie eine Aufgabe zur Virensuche, in der Sie die Sicherheitseinstellungen anpassen möchten.
3. Wählen Sie im Ergebnisfenster auf der Registerkarte **Untersuchungsbereich anpassen** den Knoten für den Sie die vordefinierte Sicherheitsstufe auswählen möchten.
4. Vergewissern Sie sich, dass der gewählte Knoten zum Schutzbereich gehört (s. S. 68).
5. Wählen Sie im Fenster **Sicherheitsstufe** die Stufe aus, die Sie anwenden möchten.

   Im Fenster wird eine Liste der Werte für die Sicherheitseinstellungen angezeigt, die der von Ihnen ausgewählten Sicherheitsstufe entsprechen.
6. Öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

SICHERHEITSPARAMETER IN UNTERSUCHUNGSAUFGABEN MANUELL ANPASSEN

Um die Sicherheitseinstellungen eines bestimmten Knotens manuell anzupassen, gehen Sie wie folgt vor:

1. In der Konsolenstruktur markieren Sie den Knoten **Untersuchung auf Befehl**.
2. Wählen Sie eine Aufgabe zur Virensuche, in der Sie die Sicherheitseinstellungen anpassen möchten.
3. Im Ergebnisfenster auf der Registerkarte **Untersuchungsbereich anpassen** wählen Sie den Knoten, dessen Sicherheitseinstellungen Sie anpassen möchten. Vergewissern Sie sich, dass der gewählte Knoten zum Schutzbereich gehört (s. S. 68).
4. Im unteren Bereich des Ergebnisfensters wird das Fenster **Sicherheitsstufe** angezeigt.
5. Klicken Sie auf die Schaltfläche **Einstellungen**, um das Fenster **Sicherheitseinstellungen** zu öffnen.
6. Passen Sie im Fenster **Sicherheitseinstellungen** die Sicherheitseinstellungen für den gewählten Knoten entsprechend an. Gehen Sie hierzu wie folgt vor:
   - Gehen Sie auf der Registerkarte **Allgemein** wie folgt vor:
     - Geben Sie im Abschnitt **Untersuchung von Objekten** an, ob Kaspersky Anti-Virus alle Objekte des Untersuchungsbereichs oder nur Objekte mit bestimmten Formaten oder Erweiterungen untersuchen soll, ob Kaspersky Anti-Virus Laufwerksbootsektoren, MBR und alternative NTFS-Datenströme untersuchen soll.

- Legen Sie im Abschnitt **Optimierung** fest, ob Kaspersky Anti-Virus im ausgewählten Bereich alle Objekte oder nur neue und veränderte Dateien untersuchen soll.
- Geben Sie im Abschnitt **Zusammengesetzte Objekte untersuchen** an, welche zusammengesetzten Objekte von Kaspersky Anti-Virus untersucht werden sollen.

- Führen Sie bei Bedarf auf der Registerkarte **Aktionen** folgende Aktionen aus:
  - Wählen Sie eine Aktion für infizierte Objekte
  - Wählen Sie eine Aktion für möglicherweise infizierte Objekte
  - Passen Sie erforderlichenfalls die Aktionen für Objekte in Abhängigkeit vom Typ des gefundenen Objekts an.
- Führen Sie bei Bedarf auf der Registerkarte **Leistung** folgende Aktionen aus:
  - Schließen Sie Dateien nach Name oder Maske aus
  - Schließen Sie gefundene Objekte nach Name oder Namensmaske aus
  - Geben Sie die maximale Untersuchungsdauer für ein Objekt an
  - Geben Sie die maximale Größe für ein zu untersuchendes zusammengesetztes Objekt an
  - Aktivieren oder deaktivieren Sie die Übernahme der iChecker-Technologie
  - Aktivieren oder deaktivieren Sie die Übernahme der iSwift-Technologie
  - Geben Sie an, ob Kaspersky Anti-Virus bei den Dateien das Vorhandensein der Microsoft-Signatur prüfen soll
- Wählen Sie auf der Registerkarte **Hierarchischer Speicher** die Methode zur Verarbeitung von autonomen Dateien.

  Sie können die Methode zur Verarbeitung von autonomen Dateien nur dann angeben, wenn Sie vorher die Methode festgelegt haben, mit der das HSM-System den Speicherort der untersuchten Dateien bestimmt.

7. Nachdem Sie die gewünschten Sicherheitseinstellungen angepasst haben, öffnen Sie das Kontextmenü durch Rechtsklick auf den Aufgabennamen und wählen Sie den Befehl **Aufgabe speichern**, um die Änderungen in der Aufgabe zu speichern.

VERWENDEN DER HEURISTISCHEN ANALYSE IN DER AUFGABE VIRENSUCHE

In den Aufgaben zur Untersuchung auf Befehl können Sie die heuristische Analyse anwenden und das Analyseniveau konfigurieren.

Um die heuristische Analyse zu aktivieren, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Öffnen Sie das Kontextmenü in der Aufgabe zur Virensuche, in der Sie die heuristische Analysemethode verwenden wollen, und gehen Sie auf den Eintrag **Eigenschaften**.
3. Aktivieren Sie im Fenster **Eigenschaften: <Aufgabenname>** auf der Registerkarte **Allgemein** das Kontrollkästchen **Heuristische Analyse verwenden** und passen Sie die Analysestufe gemäß Ihren Anforderungen an.

   Um die heuristische Analysemethode auszuschalten, entfernen Sie das Häkchen im Kontrollkästchen **Heuristische Analyse verwenden**.
4. Klicken Sie auf **OK**.

AUSFÜHRUNG EINER UNTERSUCHUNGSAUFGABE IM HINTERGRUNDMODUS

Prozesse, in denen Aufgaben von Kaspersky Anti-Virus ausgeführt werden, besitzen die Basispriorität **Mittel** (**Normal**).

Sie können einem Prozess, in dem eine Untersuchungsaufgabe ausgeführt wird, die Basispriorität **Niedrig** (**Low**) zuweisen. Wenn die Priorität eines Prozesses gesenkt wird, erhöht sich dadurch die Ausführungsdauer der Aufgabe und die Ausführungsgeschwindigkeit der Prozesse anderer aktiver Anwendungen wird gesteigert.

In einem aktiven Prozess mit niedriger Priorität können mehrere Aufgaben im Hintergrundmodus ausgeführt werden. Sie können die maximale Anzahl der Prozesse von Aufgaben zur Untersuchung auf Befehl im Hintergrund angeben.

Die Priorität einer Aufgabe kann entweder beim Erstellen der Aufgabe oder später im Fenster **Eigenschaften: <Aufgabenname>** festgelegt werden.

Um die Priorität der Aufgabe zur Virensuche zu ändern, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Öffnen Sie das Kontextmenü durch Rechtsklick auf die Aufgabe, deren Priorität Sie ändern möchten, und wählen Sie den Befehl **Eigenschaften**.
3. Das Fenster **Eigenschaften: <Aufgabenname>** wird geöffnet.
4. Führen Sie auf der Registerkarte **Allgemein** eine der folgenden Aktionen aus:
   - Um den Hintergrundmodus für die Aufgabenausführung zu aktivieren, kreuzen Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen** an.
   - Um den Hintergrundmodus für die Aufgabenausführung zu deaktivieren, entfernen Sie das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**.

Wenn Sie den Hintergrundmodus für eine laufende Aufgaben aktivieren oder deaktivieren, wird die Priorität der Aufgabe nicht sofort geändert, sondern erst bei ihrem folgenden Start.

STATISTIK VON AUFGABEN ZUR VIRENSUCHE

Während eine Untersuchungsaufgabe ausgeführt wird, können Sie Informationen über Anzahl der Objekte, die Kaspersky Anti-Virus seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat, anzeigen.

Diese Informationen stehen auch zur Verfügung, wenn Sie eine Aufgabe anhalten. Sie können die Aufgabenstatistik im Bericht über die Aufgabenausführung anzeigen (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99).

Um die Statistik der Aufgabe zur Virensuche anzusehen, gehen Sie wie folgt vor:

1. Klappen Sie in der Konsolenstruktur den Knoten **Untersuchung auf Befehl** auf.
2. Wählen Sie die Untersuchungsaufgabe, deren Statistik Sie anzeigen möchten.
3. Klicken Sie auf der Registerkarte **Übersicht und Verwaltung** des Ergebnisfensters im Abschnitt **Statistik** auf den Link **Vollständige Statistik**.

Sie können folgende Informationen über Objekte anzeigen, die Kaspersky Anti-Virus seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet hat (s. Tabelle unten).

Tabelle 17. Statistik von Aufgaben zur Virensuche

FELD	BESCHREIBUNG
Gefunden	Anzahl der Objekte, die Kaspersky Anti-Virus gefunden hat. Findet Kaspersky Anti-Virus beispielsweise in fünf Dateien ein und dasselbe Schadprogramm, dann wird der Wert in diesem Feld um den Wert eins erhöht.
Gefundene infizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus als infiziert eingestuft wurden.
Gefundene möglicherweise infizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft wurden.

FELD	BESCHREIBUNG
Nicht desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus aus folgenden Gründen nicht desinfiziert wurden: • Eine Desinfektion ist aufgrund des Typs des gefundenen Objekts nicht erforderlich. • Bei der Desinfektion ist eine Störung aufgetreten.
Nicht in die Quarantäne verschobene Objekte	Anzahl der Objekte, die Kaspersky Anti-Virus versucht hat, in die Quarantäne zu verschieben, was aber fehlgeschlagen ist, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Nicht gelöschte Objekte	Anzahl der Objekte, die Kaspersky Anti-Virus zu löschen versucht hat, was aber fehlgeschlagen ist, da beispielsweise der Zugriff auf ein Objekt durch ein anderes Programm gesperrt war.
Nicht untersuchte Objekte	Anzahl der zum Schutzbereich gehörenden Objekte, die Kaspersky Anti-Virus nicht untersuchen konnte, da beispielsweise der Zugriff auf ein Objekt durch ein anders Programm gesperrt war.
Nicht ins Backup verschobene Objekte	Anzahl der Objekte, die Kaspersky Anti-Virus ins Backup zu kopieren versucht hat, was aber fehlgeschlagen ist, da beispielsweise zu wenig Speicherplatz auf der Festplatte verfügbar war.
Verarbeitungsfehler	Anzahl der Objekte, bei deren Verarbeitung ein Fehler in der Aufgabe aufgetreten ist.
Desinfizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus desinfiziert wurden.
In die Quarantäne verschoben	Anzahl der Objekte, die von Kaspersky Anti-Virus in die Quarantäne verschoben wurden.
Ins Backup verschoben	Anzahl der Objekte, deren Kopien von Kaspersky Anti-Virus im Backup gespeichert wurden.
Gelöschte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus gelöscht wurden.
Kennwortgeschützte Objekte	Anzahl der Objekte (z.B. Archive), die von Kaspersky Anti-Virus übersprungen wurden, weil diese Objekte kennwortgeschützt sind.
Beschädigte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus übersprungen wurden, da ihr Format nicht ermittelt werden konnte.
Verarbeitete Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus verarbeitet wurden.

VERTRAUENSWÜRDIGE ZONE

Dieser Abschnitt enthält Informationen über die vertrauenswürdige Zone für Kaspersky Anti-Virus, Anweisungen zum Hinzufügen von Objekten in die vertrauenswürdige Zone sowie zur Anwendung der vertrauenswürdigen Zone in den Aufgaben von Kaspersky Anti-Virus.

IN DIESEM ABSCHNITT

VERTRAUENSWÜRDIGE ZONE FÜR KASPERSKY ANTI-VIRUS

Sie können eine Liste mit Ausnahmen aus dem Schutzbereich bzw. Untersuchungsbereich erstellen und diese Ausnahmeliste in den Aufgaben zur Untersuchung auf Befehl, zum Echtzeitschutz, zur Skript-Untersuchung und zum Schutz von Netzwerkspeichern über das RPC-Protokoll verwenden. Diese Liste von Ausnahmen heißt *vertrauenswürdige Zone*.

Wenn Sie bei der Installation von Kaspersky Anti-Virus das Kontrollkästchen **Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen** aktiviert haben, fügt Kaspersky Anti-Virus der vertrauenswürdigen Zone eine Ausnahme für Objekte nach der Maske `not-a-virus:RemoteAdmin*` hinzu. Dies gilt für Aufgaben zum Schutz von Netzwerkspeichern über das RPC-Protokoll sowie zur Untersuchung auf Befehl.

Wenn Sie bei der Installation von Kaspersky Anti-Virus die Kontrollkästchen **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen** und **Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen** aktiviert haben, fügt Kaspersky Anti-Virus für die Aufgaben zum Echtzeitschutz für Dateien jene Dateien zur vertrauenswürdigen Zone hinzu, die von Microsoft und Kaspersky Lab empfohlen werden.

Zur vertrauenswürdigen Zone von Kaspersky Anti-Virus können folgende Objekte hinzugefügt werden:

- Objekte, auf die Prozesse von Programmen zugreifen, die sensibel auf das Abfangen von Dateien reagieren (vertrauenswürdige Prozesse).
- Objekte, auf die im Verlauf von Backup-Operationen zugegriffen wird (Backup-Operationen).
- Objekte, die durch den Speicherort und/oder durch das darin gefundene Objekt definiert sind (Ausnahmeregeln).

Die vertrauenswürdige Zone wird standardmäßig in folgenden Aufgaben verwendet: Echtzeitschutz für Dateien, Schutz von Netzwerkspeichern über das RPC-Protokoll und Skript-Untersuchung, vom Benutzer neu erstellte Aufgaben zur Untersuchung auf Befehl, sowie alle Systemaufgaben zur Untersuchung auf Befehl. Eine Ausnahme bildet die Aufgabe Untersuchung von Quarantäne-Objekten.

Sie können die Liste mit den Ausnahmen für die vertrauenswürdige Zone in eine Konfigurationsdatei exportieren, um sie später auf einem anderen Server in Kaspersky Anti-Virus zu importieren.

Vertrauenswürdige Prozesse

Ausnahmen dieses Typs werden in den Aufgaben Echtzeitschutz für Dateien und Schutz von Netzwerkspeichern über das RPC-Protokoll verwendet.

Bestimmte Programme auf dem Server können instabil werden, wenn Dateien, auf die das Programm zugreift, von Kaspersky Anti-Virus abgefangen werden. Zu diesen Anwendungen zählen beispielsweise Systemprogramme von Domain-Controllern.

Damit solche Programme nicht negativ beeinflusst werden, können Sie den Echtzeitschutz für jene Objekte deaktivieren, auf die die aktiven Prozesse dieser Programme zugreifen. Dazu wird in der vertrauenswürdigen Zone eine Liste mit vertrauenswürdigen Prozessen angelegt.

Die Firma Microsoft empfiehlt, bestimmte Dateien des Betriebssystems Microsoft Windows und Programmdateien der Firma Microsoft als nicht infizierbar vom Echtzeitschutz auszuschließen. Eine Auswahl der empfohlenen Ausnahmen finden Sie auf der Webseite der Firma Microsoft http://www.microsoft.com/de/ (Artikelcode: KB822158).

Sie können das Übernehmen von vertrauenswürdigen Prozessen in der vertrauenswürdigen Zone aktivieren und deaktivieren.

Wenn die ausführbare Datei eines Prozesses beispielsweise durch ein Update verändert wird, schließt Kaspersky Anti-Virus den Prozess aus der vertrauenswürdigen Liste aus.

Backup-Operationen

Ausnahmen dieses Typs werden in den Aufgaben zum Echtzeitschutz für Dateien übernommen.

Sie können den Echtzeitschutz für Objekte, auf die bei Backup-Operationen zugegriffen wird, während dem Anlegen von Sicherungskopien ausschalten. Objekte, die von einem Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden, werden von Kaspersky Anti-Virus nicht untersucht.

Ausnahmeregeln

Ausnahmen dieses Typs werden in den Aufgaben Echtzeitschutz für Dateien, Schutz von Netzwerkspeichern über das RPC-Protokoll, Skript-Untersuchung und in Aufgaben zur Untersuchung auf Befehl verwendet.

Sie können die Liste der Ausnahmen für die vertrauenswürdige Zone in den Aufgaben Echtzeitschutz für Dateien, Schutz von Netzwerkspeichern über das RPC-Protokoll, Skript-Untersuchung und in Aufgaben zur Untersuchung auf Befehl anwenden. Sie können die Aufgaben auswählen, für die Sie jede zur vertrauenswürdigen Zone hinzugefügte Ausnahmeregel anwenden möchten. Darüber hinaus können Sie in den Einstellungen für die Sicherheitsstufe jeder Aufgabe in Kaspersky Anti-Virus Objekte einzeln von der Untersuchung ausschließen.

Sie können Objekte nach ihrem Speicherort auf dem Server oder nach dem Namen bzw. der Namensmaske der in ihnen gefundenen Objekte zur vertrauenswürdigen Zone hinzufügen oder beide Einstellungen verwenden.

Auf der Grundlage der Ausnahmeregel kann Kaspersky Anti-Virus in den festgelegten Aufgaben Objekte gemäß der folgenden Einstellungen überspringen:

- angegebene erkannte Objekte nach Name oder Namensmaske in den angegebenen Bereichen des Servers oder des Netzwerkspeichers
- alle erkannten Objekte in den angegebenen Bereichen des Servers oder des Netzwerkspeichers
- Festgelegte gefundene Objekte nach Name oder Namensmaske in allen Schutzbereichen bzw. Untersuchungsbereichen

AUSNAHMEN ZUR VERTRAUENSWÜRDIGEN ZONE HINZUFÜGEN

Dieser Abschnitt enthält Informationen zum Hinzufügen von vertrauenswürdigen Prozessen und Ausnahmeregeln in die vertrauenswürdige Zone von Kaspersky Anti-Virus.

IN DIESEM ABSCHNITT

PROZESSE ZUR LISTE DER VERTRAUENSWÜRDIGEN PROZESSE HINZUFÜGEN

Ein Prozess kann der Liste der vertrauenswürdigen Prozesse auf zwei Arten hinzugefügt werden:

- Den Prozess aus der Liste der Prozesse auswählen, die auf dem geschützten Server aktiv sind.
- Die ausführbare Datei des Prozesses auswählen, unabhängig davon, ob der Prozess gerade aktiv ist oder nicht.

Wenn die ausführbare Datei eines Prozesses verändert wird, löscht Kaspersky Anti-Virus den Prozess aus der Liste der vertrauenswürdigen Prozesse.

Um einen Prozess zur Liste vertrauenswürdigen Prozesse hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten Kaspersky Anti-Virus und wählen Sie den Punkt **Einstellungen für vertrauenswürdige Zone anpassen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

2. Aktivieren Sie im Fenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**.

3. Fügen Sie den vertrauenswürdigen Prozess auf eine der folgenden Arten hinzu:

   - Wenn Sie einen Prozess aus der Liste der aktiven Prozesse hinzufügen möchten, gehen Sie wie folgt vor:

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

        Das Fenster **Vertrauenswürdigen Prozess hinzufügen** wird geöffnet.

     b. Klicken Sie im Fenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **Prozesse**.

        Das Fenster **Aktive Prozesse** wird geöffnet.

     c. Wählen Sie im Fenster **Aktive Prozesse** den gewünschten Prozess aus der Liste der ausgeführten Prozesse und klicken Sie auf die Schaltfläche **OK**.

        Das Benutzerkonto, mit dessen Berechtigungen die Aufgabe zum Echtzeitschutz von Dateien gestartet wird, muss auf dem Server mit installiertem Kaspersky Anti-Virus über Administratorrechte verfügen, damit die Liste der aktiven Prozesse angezeigt werden kann. Sie können die Prozesse in der Liste der aktiven Prozesse nach Dateinamen, PID oder Pfad der ausführbaren Prozessdatei auf dem lokalen Computer sortieren.

     d. Klicken Sie im Fenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **OK**.

        Der gewählte Prozess wird im Fenster **Vertrauenswürdige Zone** zur Liste der vertrauenswürdigen Prozesse hinzugefügt.

   - Wenn Sie eine ausführbare Prozessdatei angeben möchten, gehen Sie wie folgt vor:

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

        Das Fenster **Vertrauenswürdigen Prozess hinzufügen** wird geöffnet.

     b. Klicken Sie im Fenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **Durchsuchen**, wählen Sie die ausführbare Datei des Prozesses aus, und klicken Sie auf die Schaltfläche **OK**.

        Im Fenster **Vertrauenswürdigen Prozess hinzufügen** werden Name und Pfad der ausführbaren Prozessdatei angezeigt.

        Wenn Sie die Pfade angeben, können Sie die Umgebungsvariablen des Systems verwenden. Dagegen können Sie die benutzerdefinierten Umgebungsvariablen nicht verwenden.

        Kaspersky Anti-Virus betrachtet einen Prozess nicht als vertrauenswürdig, wenn sich der Pfad der ausführbaren Prozessdatei von dem Pfad unterscheidet, den Sie im Feld **Ordner der Datei auf dem geschützten Computer** angegeben haben.

     c. Klicken Sie im Fenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **OK**.

        Der gewählte Prozess wird im Fenster **Vertrauenswürdige Zone** zur Liste der vertrauenswürdigen Prozesse hinzugefügt.

4. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern und das Fenster zu schließen.

ANWENDUNG DES VERTRAUENSWÜRDIGEN PROZESSES IN DER VERTRAUENSWÜRDIGEN ZONE DEAKTIVIEREN

Gehen Sie folgendermaßen vor, um die Anwendung des vertrauenswürdigen Prozesses in der vertrauenswürdigen Zone deaktivieren:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten Kaspersky Anti-Virus und wählen Sie den Punkt **Einstellungen für vertrauenswürdige Zone anpassen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

2. Deaktivieren Sie im Fenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** in der Liste der vertrauenswürdigen Prozesse das Kontrollkästchen neben dem Namen der ausführbaren Prozessdatei, die Sie vorübergehend nicht in der vertrauenswürdigen Zone anwenden möchten.

3. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern und das Fenster zu schließen.

FUNKTION ECHTZEITSCHUTZ FÜR DATEIEN UND NETZWERKSPEICHER WÄHREND DER ERSTELLUNG DER SICHERUNGSKOPIE DEAKTIVIEREN. VERTRAUENSWÜRDIGE ZONE AUSSCHLIEßEN

Um den Echtzeitschutz für Dateien während des Anlegens von Sicherungskopien zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten Kaspersky Anti-Virus und wählen Sie den Punkt **Einstellungen für vertrauenswürdige Zone anpassen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

2. Aktivieren Sie im Fenster **Vertrauenswürdige Zone** auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Operationen beim Sicherungskopieren nicht untersuchen**.

3. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern und das Fenster zu schließen.

AUSNAHMEREGELN ZUR VERTRAUENSWÜRDIGEN ZONE HINZUFÜGEN

Gehen Sie folgendermaßen vor, um der vertrauenswürdigen Zone eine Ausnahmeregel hinzuzufügen:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten Kaspersky Anti-Virus und wählen Sie den Punkt **Einstellungen für vertrauenswürdige Zone anpassen**.

   Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

2. Klicken Sie im Fenster **Vertrauenswürdige Zone** auf der Registerkarte **Ausnahmeregeln** auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Ausnahmeregel** wird geöffnet.

3. Geben Sie im Block **Das Objekt wird unter folgenden Bedingungen nicht untersucht** die Objekte, die Sie aus dem Schutzbereich bzw. dem Untersuchungsbereich ausschließen möchten, sowie jene Objekte, die Sie nicht den zu erkennenden Objekten zurechnen möchten (beispielsweise Tools zur Remote-Verwaltung), an.

   - Wenn Sie ein Objekte aus dem Schutzbereich bzw. dem Untersuchungsbereich ausschließen möchten, aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt**, klicken Sie auf die Schaltfläche **Ändern** und geben Sie im Fenster **Objekt auswählen** das Objekt an, das von der Untersuchung ausgeschlossen werden soll.

     Sie können die Sonderzeichen ? und * verwenden, um Objekte anzugeben.

- Wenn Sie den Namen eines zu erkennenden Objekts angeben möchten, aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**, klicken auf **Ändern** und geben im Fenster **Liste der gefundenen Objekte** den Namen oder die Namensmaske des gefundenen Objekts gemäß der Klassifizierung der Viren-Enzyklopädie von Kaspersky Lab an (http://www.securelist.com/de/), z. B. `not-a-virus:RemoteAdmin*`.
- Aktivieren Sie im Block **Gültigkeitsbereich der Regel** die Kontrollkästchen neben den Namen der Aufgaben, in denen die Ausnahmeregel übernommen werden soll.

4. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern und das Fenster zu schließen.

   Die hinzugefügte Ausnahmeregel wird in der Liste auf der Registerkarte **Ausnahmeregeln** im Fenster **Vertrauenswürdige Zone** angezeigt.

IMPORT UND EXPORT VON PARAMETERN

Sie können die Einstellungen von Kaspersky Anti-Virus in eine Konfigurationsdatei im xml-Format exportieren und Einstellungen aus einer Konfigurationsdatei in Kaspersky Anti-Virus importieren. In einer Konfigurationsdatei können entweder alle Einstellungen für Kaspersky Anti-Virus oder nur die Einstellungen einzelner Komponenten gespeichert werden.

Wenn Sie alle Einstellungen für Kaspersky Anti-Virus exportieren, speichert Kaspersky Anti-Virus die allgemeinen Einstellungen für Kaspersky Anti-Virus und die Einstellungen der folgenden Komponenten und Funktionen von Kaspersky Anti-Virus in einer Datei:

- Echtzeitschutz für Dateien
- Skript-Untersuchung.
- Schutz von Netzwerkspeichern
- Untersuchung auf Befehl.
- Update der Datenbanken und Module für Kaspersky Anti-Virus.
- Quarantäne
- Backup.
- Berichte.
- Benachrichtigungen an den Administrator und die Benutzer.
- Vertrauenswürdige Zone.

Ferner können Sie die allgemeinen Einstellungen von Kaspersky Anti-Virus und die Berechtigungen des Benutzerkontos in einer Datei speichern.

Kaspersky Anti-Virus exportiert die Parameter von Gruppenaufgaben nicht.

Kaspersky Anti-Virus exportiert alle von ihm verwendeten Kennwörter, wie beispielsweise Daten von Benutzerkonten für den Aufgabenstart oder für die Proxyserver-Verbindung. Kennwörter werden vor dem Export in verschlüsselter Form in der Konfigurationsdatei gespeichert. Die Kennwörter können aber von Kaspersky Anti-Virus nur auf den gleichen Computer importiert werden, wenn Anti-Virus nicht neu installiert oder aktualisiert wurde. Die Kennwörter können von Kaspersky Anti-Virus nicht auf einen anderen Computer importiert werden. Nach dem Import von Parametern auf einen anderen Computer müssen alle Kennwörter manuell angegeben werden.

Wenn zum Zeitpunkt des Exports von Parametern eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert Kaspersky Anti-Virus die aus der Richtlinie übernommenen Werte.

Sie können Einstellungen aus einer Konfigurationsdatei importieren, die nur Einstellungen für bestimmte Kaspersky Anti-Virus-Komponenten enthält (z.B. eine Konfigurationsdatei, die für Kaspersky Anti-Virus erstellt wurde, als nicht alle Komponenten installiert waren). Nach dem Parameter-Import werden in Kaspersky Anti-Virus nur jene Parameter geändert, die in der Konfigurationsdatei vorhanden waren. Die übrigen Parameter bleiben unverändert.

Importierte Aufgabenparameter werden nicht in momentan laufende Aufgaben übernommen, sondern erst nach dem folgenden Start der Aufgabe.

Gesperrte Einstellungen der aktiven Richtlinie von Kaspersky Security Center werden beim Import von Einstellungen nicht verändert.

ANWENDUNG DER VERTRAUENSWÜRDIGEN ZONE IN DEN AUFGABEN VON KASPERSKY ANTI-VIRUS AKTIVIEREN BZW. DEAKTIVIEREN

Die vertrauenswürdige Zone wird standardmäßig in folgenden Aufgaben verwendet: **Echtzeitschutz für Dateien**, **RPC: Schutz von Netzwerkspeichern** und **Skript-Untersuchung**, vom Benutzer neu erstellte Aufgaben zur Untersuchung auf Befehl sowie alle Systemaufgaben zur Untersuchung auf Befehl. Eine Ausnahme bildet die Aufgabe **Untersuchung von Quarantäne-Objekten**.

Nachdem die vertrauenswürdige Zone aktiviert bzw. deaktiviert wurde, werden die Ausnahmen in den laufenden Aufgaben sofort wirksam bzw. unwirksam.

Um das Übernehmen der vertrauenswürdigen Zone für die Aufgaben von Kaspersky Lab zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für eine Aufgabe und wählen Sie den Punkt **Eigenschaften**.

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

2. Führen Sie im Fenster **Eigenschaften: <Aufgabenname>** auf der Registerkarte **Allgemein** im Abschnitt **Vertrauenswürdige Zone** eine der folgenden Aktionen aus:

   - Wenn Sie die vertrauenswürdige Zone in der Aufgabe übernehmen möchten, aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.
   - Wenn Sie die Übernahme der vertrauenswürdige Zone in der Aufgabe deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.

3. Wenn Sie die Einstellungen für die vertrauenswürdige Zone anpassen möchten, folgen Sie dem Link für die vertrauenswürdige Zone

4. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern und das Fenster zu schließen.

ISOLIERUNG MÖGLICHERWEISE INFIZIERTER OBJEKTE. VERWENDUNG DER QUARANTÄNE

Dieser Abschnitt enthält Informationen über die Isolierung von möglicherweise infizierten Objekten, also über die Verschiebung dieser Objekte in die Quarantäne sowie über die Anpassung der Quarantäne-Einstellungen.

IN DIESEM ABSCHNITT

MÖGLICHERWEISE INFIZIERTE OBJEKTE ISOLIEREN

Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft worden sind, werden in die Quarantäne verschoben, d. h. die Objekte werden von ihrem ursprünglichen Speicherort in den *Quarantäne-Ordner* verschoben. Aus Sicherheitsgründen werden die Objekte im Quarantäne-Ordner in verschlüsselter Form gespeichert.

QUARANTÄNE-OBJEKTE ANZEIGEN

Die unter Quarantäne stehenden Objekte können im Knoten **Quarantäne** der Konsole von Kaspersky Anti-Virus angezeigt werden.

Um die Objekte in der Quarantäne anzuzeigen, wählen Sie in der Konsolenstruktur den Knoten **Quarantäne** aus.

Um ein bestimmtes Objekt in der Quarantäneliste zu suchen, können Sie die Quarantäne-Objekte sortieren (s. S 83) Objekte sortieren oder filtern.

IN DIESEM ABSCHNITT

QUARANTÄNE-OBJEKTE SORTIEREN

Die Objekte in der Liste mit den Quarantäne-Objekten sind standardmäßig in umgekehrter chronologischer Reihenfolge nach dem Datum des Verschiebens angeordnet. Um ein bestimmtes Objekt zu finden, können Sie die Objekte nach dem Spalteninhalt und den Objektinformationen sortieren. Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Quarantäne** verlassen und erneut öffnen, oder wenn Sie die Konsole von Kaspersky Anti-Virus nach dem Speichern in der msc-Datei schließen und sie erneut aus dieser Datei öffnen.

- *Um die Objekte zu sortieren, gehen Sie wie folgt vor:*

  1. Wählen Sie in der Konsolenstruktur den Knoten **Quarantäne**.
  2. Klicken Sie im Ergebnisfenster auf den Titel der Spalte, nach deren Inhalt die Objekte in der Liste sortiert werden sollen.

QUARANTÄNE-OBJEKTE FILTERN

Um ein Objekt in der Quarantäne zu suchen, können Sie die Objekte in der Liste filtern. Das heißt, es werden nur Objekte angezeigt, die den von Ihnen definierten Filterkriterien (Filtern) entsprechen. Das Filterungsergebnis wird gespeichert, wenn Sie den Knoten Quarantäne verlassen und erneut öffnen, oder wenn Sie die Konsole von Kaspersky Anti-Virus nach dem Speichern in der msc-Datei schließen und sie erneut aus dieser Datei öffnen.

- *Um einen oder mehrere Filter einzustellen, gehen Sie wie folgt vor:*

  1. Öffnen Sie in der Konsolenstruktur das Kontextmenü des Knotens **Quarantäne** und wählen Sie den Befehl **Filter**.

     Das Fenster **Filtereinstellungen** wird geöffnet.

  2. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

     a. Wählen Sie in der Liste **Feldname** ein Feld aus, mit dem der Filterwert verglichen werden soll.

     b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterbedingungen in der Liste können unterschiedlich sein, je nachdem, welchen Wert Sie in der Liste **Feldname** gewählt haben.

     c. Geben Sie im Feld **Feldwert** einen Wert für den Filter an oder wählen Sie ihn in der Liste aus.

     d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

     Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt. Wiederholen Sie diese Aktionen für jeden Filter, den Sie hinzufügen möchten. Halten Sie sich bei der Arbeit mit Filtern an die folgenden Regeln:

     - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.
     - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.
     - Um einen Filter zu löschen, markieren Sie ihn in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.
     - Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Fensters **Filtereinstellungen**, ändern Sie dann die entsprechenden Werte in den Feldern **Feldname**, **Operator** oder **Feldwert**, und klicken Sie auf die Schaltfläche **Ersetzen**.

  3. Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**.

- *Damit wieder alle Objekte in der Liste der Quarantäne-Objekte angezeigt werden,*

  öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Quarantäne** und wählen Sie den Befehl **Filter entfernen**.

UNTERSUCHUNG VON QUARANTÄNE-OBJEKTEN. PARAMETER DER AUFGABE "UNTERSUCHUNG VON QUARANTÄNEOBJEKTEN"

Kaspersky Anti-Virus führt in der Grundeinstellung nach jedem Update der Datenbanken die Systemaufgabe **Untersuchung von Quarantäne-Objekten** aus. Die Aufgabenparameter werden in folgender Tabelle genannt. Die Werte können nicht verändert werden.

Sie können den Zeitplan für die Aufgabe **Untersuchung von Quarantäne-Objekten** ändern oder die Aufgabe manuell starten.

Wenn die Quarantäneobjekte nach einem Datenbank-Update untersucht wurden, kann Anti-Virus bestimmte Objekte als virenfrei einstufen: Der Status dieser Objekte ändert sich in der Liste in **Fehlalarm**. Kaspersky Anti-Virus kann andere Objekte als infiziert einstufen und für sie Aktionen ausführen, die in den Einstellungen für die Aufgabe zur Untersuchung auf Befehl **Untersuchung von Quarantäne-Objekten** vorgegeben sind: **Desinfizieren, irreparable Objekte löschen**.

*Tabelle 18. Einstellungen für die Aufgabe **Untersuchung von Quarantäne-Objekten***

EINSTELLUNG FÜR DIE AUFGABE "UNTERSUCHUNG VON QUARANTÄNE-OBJEKTEN"	BEDEUTUNG
Untersuchungsbereich	Quarantäne-Ordner
Parameter für Sicherheit	Einheitlich für den gesamten Untersuchungsbereich, Werte stehen in der folgenden Tabelle.

*Tabelle 19. Sicherheitseinstellungen für die Aufgabe **Untersuchung von Quarantäne-Objekten***

SICHERHEITSEINSTELLUNGEN	BEDEUTUNG
Objekte untersuchen	Alle Objekte
Optimierung	Deaktiviert
Aktion für infizierte Objekte	Desinfizieren. Irreparable Objekte löschen
Aktion für möglicherweise infizierte Objekte.	Überspringen
Objekte ausschließen	Nein
Nicht erkennen	Nein
Untersuchung beenden, wenn sie länger andauert als (Sek.)	Nicht festgelegt
Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	Nicht festgelegt
Alternative NTFS-Ströme	Aktiviert
Bootsektoren und MBR	Deaktiviert
iChecker-Technologie verwenden	Deaktiviert
iSwift-Technologie verwenden	Deaktiviert
Zusammengesetzte Objekte untersuchen	• Archive* • SFX-Archive* • Gepackte Objekte* • eingebettete OLE-Objekte* * Der Parameter "Nur neue und veränderte Dateien untersuchen" ist deaktiviert.
Microsoft-Signatur bei Dateien prüfen	Wird nicht ausgeführt.
Heuristische Analyse verwenden	Die Analysestufe **Tief** ist eingestellt.
Vertrauenswürdige Zone (s. S. 77)	Wird nicht verwendet

WIEDERHERSTELLUNG VON OBJEKTEN AUS DER QUARANTÄNE

Kaspersky Anti-Virus verschiebt möglicherweise infizierte Objekte verschlüsselt in den Quarantäne-Ordner, damit der geschützte Server vor schädlichen Wirkungen bewahrt wird.

Sie können jedes Objekt aus der Quarantäne wiederherstellen. Das kann in folgenden Fällen notwendig sein:

- Wenn nach der Quarantäne-Untersuchung anhand der aktualisierten Datenbanken der Status des Objektes in **Fehlalarm** oder **Desinfiziert** geändert worden ist.
- wenn Sie das Objekt für den Server als nicht gefährlich einschätzen und es benutzen wollen. Damit kaspersky Anti-Virus dieses Objekt bei künftigen Untersuchungen nicht isoliert, können Sie das Objekt von der Untersuchung in der Aufgabe **Echtzeitschutz für Dateien** und in die Aufgabe zur Untersuchung auf Befehl ausschließen. Geben Sie dazu das Objekt als Wert der Sicherheitseinstellung **Objekte ausschließen** (nach Dateiname) oder **Nicht erkennen** in diesen Aufgaben an oder fügen Sie es zur vertrauenswürdigen Zone hinzu (s. S. 77).

Beim Wiederherstellen eines Objektes können Sie entscheiden, wo das wiederhergestellte Objekt gespeichert werden soll: Am ursprünglichen Ort (gilt als Standard), in einem speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Server oder in einem benutzerdefinierten Ordner auf dem Rechner, auf dem die Anti-Virus-Konsole installiert ist, oder auf einem anderen Computer des Netzwerks.

Damit Kaspersky Anti-Virus bei der Wiederherstellung von Objekten aus der Quarantäne Objekte mit großem Umfang nicht untersucht, legen Sie eine Ausnahme für den Ordner %Temp%\wseeqbfiles\.

Der Wiederherstellungsordner dient zum Speichern von wiederhergestellten Objekten auf dem geschützten Server. Sie können für seine Untersuchung spezielle Sicherheitseinstellungen festlegen. Der Pfad dieses Ordners wird in den Quarantäne-Einstellungen angegeben.

Die Wiederherstellung von Objekten aus der Quarantäne kann den Computer infizieren.

Sie können ein Objekt wiederherstellen, nachdem dessen Kopie im Quarantäne-Ordner gespeichert worden ist, damit Sie es weiter benutzen können, beispielsweise, um das Objekt nach einem Update der Datenbanken noch einmal zu untersuchen.

Wenn ein in die Quarantäne verschobenes Objekt zu einem zusammengesetzten Objekt gehört (z. B. zu einem Archiv), fügt Kaspersky Anti-Virus es bei der Wiederherstellung nicht mehr in das zusammengesetzte Objekt ein, sondern speichert es separat im festgelegten Ordner.

Sie können ein Objekt oder mehrere Objekte wiederherstellen.

➧ *Um eine Datei aus der Quarantäne wiederherzustellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Knoten **Quarantäne**.
2. Im Ergebnisfenster führen Sie eine der folgenden Aktionen aus:
   - Um ein Objekt wiederherzustellen, öffnen Sie das Kontextmenü des Objekts, das Sie wiederherstellen wollen, und gehen Sie auf **Wiederherstellen**.
   - Um mehrere Objekte wiederherzustellen, wählen Sie in der Liste die entsprechenden Objekte mit Hilfe der Taste **Strg** oder **Umschalt** aus. Öffnen Sie anschließend das Kontextmenü eines der markierten Objekte, und wählen Sie den Punkt **Wiederherstellen**.

   Das Fenster **Objektwiederherstellung** wird geöffnet.
3. **Geben Sie im Fenster** Objektwiederherstellung **für jedes markierte Objekt den Ordner an, in den das wiederhergestellte Objekt gespeichert werden soll (Objektname wird im Feld** Objekt im oberen Teil des Fensters angezeigt; bei mehreren Objekten wird der Name des ersten Objektes in der Liste der markierten Objekte angezeigt).

   Führen Sie eine der Aktionen durch:
   - um ein Objekt am ursprünglichen Speicherplatz wiederherzustellen, gehen Sie auf **Im Ursprungsordner wiederherstellen**;
   - um ein Objekt in einem Ordner wiederherzustellen, den Sie als Ordner für wiederhergestellte Objekte in den Quarantäneparameter angegeben haben, wählen Sie **Im standardmäßigen Server-Ordner wiederherstellen**;
   - um ein Objekt in einem anderen Ordner auf dem Computer zu speichern, auf dem die Anti-Virus-Konsole installiert ist, oder in einem Netzwerkordner, gehen Sie auf **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen**, und danach wählen Sie den gewünschten Ordner aus oder Sie geben dessen Pfad ein.
4. Wenn Sie nach der Wiederherstellung eine Kopie des Objekts im Quarantäne-Ordner speichern möchten, entfernen Sie das Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Backup löschen**.

5. Um die eingegebenen Bedingungen für das Wiederherstellen auf die übrigen ausgewählten Objekte anzuwenden, setzen Sie das Häkchen im Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

   Alle ausgewählten Objekte werden am vorgegebenen Speicherort wiederhergestellt und gespeichert: Bei Auswahl der Variante **Im Ursprungsordner auf dem Server wiederherstellen** wird jedes Objekt an seinem ursprünglichen Speicherort gespeichert. Bei Auswahl der Variante **Im standardmäßigen Server-Ordner wiederherstellen** oder **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** werden alle Objekte im angegebenen Ordner gespeichert.

6. Klicken Sie auf **OK**.

   Kaspersky Anti-Virus beginnt damit, das erste von Ihnen ausgewählte Objekt wiederherzustellen.

7. Wenn am angegebenen Ort bereits ein Objekt mit diesem Namen vorhanden ist, wird das Fenster **Ein Objekt mit diesem Namen ist bereits vorhanden** geöffnet.

   a. Wählen Sie eine der folgenden Anti-Virus-Aktionen:

      - **Ersetzen**, um das wiederhergestellte Objekt anstelle des vorhandenen Objektes zu speichern
      - **Umbenennen**, um das wiederhergestellte Objekt unter einem anderen Namen zu speichern. Im Eingabefeld tragen Sie einen neuen Dateinamen für das Objekt und den vollständigen Pfad ein.
      - **Umbenennen und Suffix hinzufügen**, um das Objekt umzubenennen und der Datei einen Suffix hinzuzufügen. Tragen Sie im Eingabefeld das Suffix ein.

   b. Wenn Sie mehrere Dateien für die Wiederherstellung markiert haben und die gewählte Aktion **Ersetzen** oder **Umbenennen und Suffix hinzufügen** auch auf die übrigen markierten Objekte angewendet werden soll, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**. (Wenn Sie den Wert **Umbenennen** eingestellt haben, steht das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden** nicht zur Verfügung.)

   c. Klicken Sie auf **OK**.

      Das Objekt wird wiederhergestellt. Die Daten zum Wiederherstellungsvorgang werden im Systemaudit-Bericht registriert.

Wenn Sie im Fenster **Objektwiederherstellung** nicht die Variante **Auf alle ausgewählten Objekte anwenden** ausgewählt haben, öffnet sich das Fenster **Objektwiederherstellung** noch einmal. Sie können dort den Speicherort angeben, an dem das folgende ausgewählte Objekt wiederhergestellt werden soll (s. Schritt 3 dieser Anleitung).

DATEIEN NACH QUARANTÄNE VERSCHIEBEN

Sie können manuell Dateien in die Quarantäne verschieben.

Um eine Datei in die Quarantäne zu verschieben, gehen Sie wie folgt vor:

1. In der Konsolenstruktur öffnen Sie das Kontextmenü für den Knoten **Quarantäne** und gehen Sie auf den Eintrag **Hinzufügen**.
2. Geben Sie im Fenster **Öffnen** die Datei an, die Sie in die Quarantäne verschieben möchten, und klicken auf die Schaltfläche **OK**.

   Kaspersky Anti-Virus verschiebt die ausgewählte Datei in die Quarantäne.

OBJEKTE AUS QUARANTÄNE LÖSCHEN

Gemäß den Parametern der Aufgabe **Untersuchung von Quarantäne-Objekten** (s. S. 84) löscht Anti-Virus automatisch aus dem Quarantäne-Ordner diejenigen Objekte, deren Status sich bei der Quarantäne-Untersuchung anhand aktualisierter Datenbanken in **Infiziert** geändert hat und die Kaspersky Anti-Virus nicht reparieren konnte. Die übrigen Objekte werden von Kaspersky Anti-Virus nicht gelöscht.

Sie können ein oder mehrere Objekte manuell aus der Quarantäne löschen.

Um ein oder mehrere Objekte aus der Quarantäne zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Quarantäne**.
2. Führen Sie eine der Aktionen durch:

   - Um ein Objekt zu löschen, öffnen Sie das Kontextmenü durch Rechtsklick auf das Objekt, das gelöscht werden soll, und wählen Sie den Befehl **Löschen**.

- Um mehrere Objekte zu löschen, markieren Sie in der Liste die entsprechenden Objekte mit Hilfe der Taste **Strg** oder **Umschalt**. Öffnen Sie anschließend das Kontextmenü durch Rechtsklick auf eines der gewählten Objekte und wählen Sie den Befehl **Löschen**.

3. Klicken Sie im folgenden Fenster auf die Schaltfläche **Ja**, um die Operation zu bestätigen.

MÖGLICHERWEISE INFIZIERTE QUARANTÄNE-OBJEKTE ZUR ANALYSE AN KASPERSKY LAB EINSCHICKEN

Wenn das Verhalten einer bestimmten Datei den Verdacht nahe legt, dass sie eine Bedrohung enthält, Kaspersky Anti-Virus die Datei aber als virenfrei einstuft, handelt es sich möglicherweise um eine neue, unbekannte Bedrohung, deren Beschreibung noch nicht in den Datenbanken verzeichnet ist. Sie können diese Datei zur Analyse in das Virenlabor von Kaspersky Lab einschicken. Die Viren-Analytiker von Kaspersky Lab untersuchen die Datei. Wenn sie eine neue Bedrohung darin finden, wird den Datenbanken ein entsprechender Eintrag und ein Desinfektionsalgorithmus hinzugefügt. Es ist möglich, dass Kaspersky Anti-Virus, wenn Sie das Objekt nach einem Datenbank-Update erneut untersuchen, die Datei als infiziert einstuft und desinfizieren kann. Dadurch können Sie nicht nur das Objekt retten, sondern auch dabei helfen, eine Virenepidemie zu verhindern.

Nur Dateien aus der Quarantäne können zur Analyse eingeschickt werden. Die Dateien sind in verschlüsselter Form in der Quarantäne gespeichert und werden beim Verschicken nicht von der auf dem Mailserver installierten Antiviren-Anwendung gelöscht.

Nachdem die Gültigkeit der Lizenz abgelaufen ist, können keine Quarantäneobjekte an Kaspersky Lab geschickt werden.

Um eine Datei zur Analyse in das Virenlabor von Kaspersky Lab einzuschicken, gehen Sie wie folgt vor:

1. Wenn sich die Datei nicht in der Quarantäne befindet, verschieben Sie sie zuerst in die Quarantäne (s. S. 87).
2. Öffnen Sie im Knoten **Quarantäne** in der Liste der Quarantäneobjekte das Kontextmenü der Datei, die zur Analyse an Kaspersky Lab geschickt werden soll, und wählen Sie den Befehl **Objekt zur Analyse einschicken**.
3. Wenn auf dem Rechner, auf dem die Konsole von Kaspersky Anti-Virus installiert ist, ein Mail-Client eingerichtet ist, wird eine neue E-Mail erstellt. Prüfen Sie die Nachricht und klicken Sie anschließend auf die Schaltfläche **Senden**.

   Das Feld **Empfänger** enthält die E-Mail-Adresse von Kaspersky Lab newvirus@kaspersky.com. Im Feld **Betreff** steht der Text "Quarantäneobjekt".

   Der Nachrichtenkörper enthält den Text "Datei wurde zur Analyse an Kaspersky Lab geschickt". Sie können der Nachricht zusätzliche Informationen über die Datei hinzufügen: z. B. warum Sie die Datei für möglicherweise infiziert oder gefährlich halten, wie sich die Datei verhält und wie sie das System beeinflusst.

   Die Nachricht enthält als Anlage das Archiv <Objektname>.cab. Es enthält die Datei <uuid>.klq mit dem verschlüsselten Objekt (uuid – unikaler Objekt-ID in Kaspersky Anti-Virus), die Datei <uuid>.txt mit Daten, die Kaspersky Anti-Virus über das Objekt erhalten hat, sowie die Datei Sysinfo.txt, die folgende Informationen über Kaspersky Anti-Virus und das Betriebssystem des Servers enthält:

   - Name und Version des Betriebssystems
   - Name und Version von Kaspersky Anti-Virus
   - Erscheinungsdatum der zuletzt installierten Datenbank-Updates
   - Nummer des aktiven Schlüssels

   Diese Informationen benötigen die Virenanalytiker von Kaspersky Lab zur schnellen und effektiven Analyse einer Datei. Wenn Sie diese Daten nicht weitergeben möchten, können Sie die Datei Sysinfo.txt aus dem Archiv löschen.

   Wenn auf dem Rechner, auf dem die Konsole von Kaspersky Anti-Virus installiert ist, kein Mail-Client eingerichtet ist, wird der Verbindungsassistent von Microsoft Windows geöffnet. Sie können folgendermaßen vorgehen:

   - Folgen Sie den Anweisungen des Verbindungsassistenten, erstellen Sie ein neues Benutzerkonto und schicken Sie die Datei von diesem Rechner aus ab.
   - Verlassen Sie den Assistenten und speichern Sie das ausgewählte verschlüsselte Objekt in einer Datei. Schicken Sie die Datei manuell an Kaspersky Lab.

Um ein verschlüsseltes Objekt in einer Datei zu speichern, gehen Sie wie folgt vor:

1. Klicken Sie im folgenden Fenster zum Speichern des Objekts auf die Schaltfläche **Ja**.
2. Wählen Sie den Ordner auf einem Laufwerk des geschützten Servers oder den Netzwerkordner, in den Sie die Datei mit dem Objekt speichern möchten.

ANPASSEN DER QUARANTÄNE-EINSTELLUNGEN IN DER MMC

In diesem Abschnitt werden die Einstellungen der Quarantäne beschrieben. Neuen Werte für Quarantäne-Einstellungen werden sofort nach dem Speichern übernommen.

Um die Quarantäne-Einstellungen anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Quarantäne** und wählen Sie den Befehl **Eigenschaften**.
2. Passen Sie im Fenster **Eigenschaften: Quarantäne** die Quarantäne-Einstellungen entsprechend an:
   - Um einen vom Standardordner abweichenden Quarantäne-Ordner anzugeben, wählen Sie im Feld **Ordner für die Quarantäne** den entsprechenden Ordner auf einem Laufwerk des geschützten Servers aus oder geben Sie seinen Namen und vollständigen Pfad an.
   - Um die maximale Größe des Ordners für die Quarantäne festzulegen, aktivieren Sie das Kontrollkästchen **Maximale Größe der Quarantäne** und tragen Sie im Eingabefeld den entsprechenden Wert in MB ein.
   - Um die minimale Größe für den freien Speicherplatz im Ordner für die Quarantäne festzulegen, definieren Sie die Einstellung **Maximale Größe der Quarantäne**, aktivieren Sie das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz** und tragen Sie im Eingabefeld den entsprechenden Wert in MB ein.
   - Um einen anderen Wiederherstellungsordner anzugeben, wählen Sie in der Einstellungsgruppe **Einstellungen für die Wiederherstellung von Objekten** den entsprechenden Ordner auf einem lokalen Laufwerk des geschützten Servers aus oder geben Sie den Namen und vollständigen Pfad an.
3. Klicken Sie auf **OK**.

STATISTIK FÜR QUARANTÄNE

In der Statistik für die Quarantäne können Sie Informationen über die Anzahl der Quarantäne-Objekte erhalten.

Um eine Statistik für die Quarantäne anzuzeigen,

öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Quarantäne** und wählen Sie den Befehl **Statistik**.

Im Fenster **Statistik** werden Informationen über die aktuelle Anzahl der Quarantäne-Objekte angezeigt (s. Tabelle unten):

Tabelle 20. Informationen über Quarantäne-Objekte im Fenster Statistik für Quarantäne

FELD	BESCHREIBUNG
Möglicherweise infizierte Objekte	Anzahl der Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft wurden.
Aktuelle Größe der Quarantäne	Gesamtvolumen der Daten im Quarantäne-Ordner.
Fehlalarme	Anzahl der Objekte, die den Status **Fehlalarm** erhielten, weil sie bei der Quarantäne-Untersuchung unter Verwendung von aktualisierten Datenbanken virenfrei eingestuft wurden.
Desinfizierte Objekte	Anzahl der Objekte, denen nach der Quarantäne-Untersuchung der Status **Desinfiziert** zugewiesen wurde.
Objekte insgesamt	Anzahl der Quarantäne-Objekte.

SICHERUNGSKOPIEREN VON OBJEKTEN VOR DESINFEKTION / LÖSCHEN. VERWENDUNG DES BACKUPS

Dieser Abschnitt enthält Informationen über die Erstellung von Sicherungskopien für gefundene schädliche Objekte, bevor diese desinfiziert oder gelöscht werden, sowie über die Anpassung der Einstellungen des Backups.

IN DIESEM ABSCHNITT

SICHERUNGSKOPIEREN VON OBJEKTEN VOR DESINFEKTION / LÖSCHEN

Bevor ein Objekt mit dem Status *Infiziert* oder *Möglicherweise infiziert* desinfiziert oder gelöscht wird, speichert Kaspersky Anti-Virus eine verschlüsselte Sicherungskopie im *Backup*.

Wenn ein Objekt Bestandteil eines zusammengesetzten Objekts ist (z. B. zu einem Archiv gehört), wird das gesamte zusammengesetzte Objekt ins Backup kopiert. Wenn Kaspersky Anti-Virus z.B. ein Objekt aus einer Mail-Datenbank als infiziert einstuft, wird die komplette Mail-Datenbank gesichert.

Wenn ein Objekt, das von Kaspersky Anti-Virus ins Backup kopiert wird, umfangreich ist, kann sich das System verlangsamen und der freie Festplattenplatz auf Ihrem Computer kann sich verringern.

Sie können Dateien aus dem Backup entweder im ursprünglichen Ordner oder in einem anderen Ordner auf dem geschützten Server oder auf einem anderen Rechner des lokalen Unternehmensnetzwerks wiederherstellen. Sie können eine Datei aus dem Backup beispielsweise wiederherstellen, wenn die infizierte Originaldatei wichtige Informationen enthielt, die Integrität der Datei aber bei der Desinfektion durch Kaspersky Anti-Virus verletzt wurde und dadurch der Zugriff auf die Informationen nicht mehr möglich ist.

Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des Computers führen.

DATEIEN IM BACKUP ANZEIGEN

Die Dateien im Backup-Ordner können nur über die Konsole von Kaspersky Anti-Virus im Knoten **Backup** angezeigt werden. Sie können die Dateien nicht mit den Dateimanagern von Microsoft Windows anzeigen.

- *Um Dateien im Backup anzuzeigen,*

  Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.

- *Um ein bestimmtes Objekt in der Liste zu finden,*

  sortieren (s. S. 91) oder filtern (s. S. 91) Sie die Objekte.

IN DIESEM ABSCHNITT

DATEIEN IM BACKUP SORTIEREN

Standardmäßig werden die Dateien im Backup nach ihrem Speicherdatum in umgekehrter chronologischer Reihenfolge sortiert. Um eine bestimmte Datei zu suchen, können Sie die Dateien nach dem Inhalt einer beliebigen Spalte im Ergebnisfenster sortieren.

Das Sortierergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen oder wenn Sie die Konsole von Kaspersky Anti-Virus mit dem Speichern in der msc-Datei schließen und sie wieder aus dieser Datei öffnen.

Um die Dateien im Backup zu sortieren, gehen Sie wie folgt vor:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.
2. Wählen Sie In der Dateiliste des Backups den Titel der Spalte aus, nach deren Inhalt Sie die Objekte sortieren wollen.

DATEIEN IM BACKUP FILTERN

Um ein bestimmtes Objekt im Backup zu suchen, können Sie die Dateien filtern, das heißt, im Knoten **Backup** nur Dateien anzeigen, die den von Ihnen definierten Filterbedingungen (Filtern) entsprechen.

Das Filterergebnis wird gespeichert, wenn Sie den Knoten **Backup** verlassen oder wenn Sie die Konsole von Kaspersky Anti-Virus mit dem Speichern in der msc-Datei schließen und sie wieder aus dieser Datei öffnen.

Um die Dateien im Backup zu filtern, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Backup** und wählen Sie den Befehl **Filter** aus.
2. Das Fenster **Filtereinstellungen** wird geöffnet.
3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie in der Liste **Feldname** ein Feld aus, mit dessen Wert der von Ihnen angegebene Filterwert verglichen werden soll.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterbedingungen in der Liste können unterschiedlich sein, je nachdem, welchen Wert Sie im Feld **Feldname** gewählt haben.
   c. Geben Sie im Feld **Feldwert** einen Wert für den Filter an oder wählen Sie ihn aus.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt. Wiederholen Sie diese Aktionen für jeden Filter, den Sie hinzufügen möchten. Sie können die folgenden Regeln für die Arbeit mit Filtern verwenden:

   - Wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind** um einige Filter durch logisches UND zu verknüpfen.
   - Wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist** um einige Filter durch logisches ODER zu verknüpfen.
   - Um einen Filter zu löschen, markieren Sie ihn in der Filterliste und klicken Sie auf die Schaltfläche **Löschen**.
   - Um einen Filter zu bearbeiten, markieren Sie ihn in der Filterliste des Fensters **Filtereinstellungen**, ändern Sie die entsprechenden Werte in den Feldern **Feldname**, **Operator** oder **Feldwert** und klicken Sie auf die Schaltfläche **Ersetzen**.

   Nachdem Sie alle Filter hinzugefügt haben, klicken Sie auf die Schaltfläche **Übernehmen**. In der Liste werden nur die Dateien angezeigt, die den von Ihnen definierten Filtern entsprechen.

Damit wieder alle Dateien in der Liste der Backup-Dateien angezeigt werden,

öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Backup** und wählen Sie den Befehl **Filter entfernen**.

DATEIEN AUS BACKUP WIEDERHERSTELLEN

Kaspersky Anti-Virus speichert Dateien im Backup im verschlüsselten Format, damit der geschützte Server vor schädlichen Wirkungen bewahrt wird.

Sie können Dateien aus dem Backup wiederherstellen.

In den folgenden Fällen müssen Sie möglicherweise eine Datei wiederherstellen:

- Wenn die Ursprungsdatei, die sich als infiziert herausgestellt hat, wichtige Informationen enthalten hat, bei der Reparatur dieser Datei Kaspersky Anti-Virus deren Integrität nicht retten konnte und aufgrund dessen auf die Informationen nicht mehr zugegriffen werden kann.
- Wenn Sie die Datei für den Server als sicher einschätzen und sie benutzen möchten. Damit Kaspersky Anti-Virus diese Datei bei künftigen Untersuchungen nicht als infiziert oder möglicherweise infiziert einstuft, können Sie sie von der Untersuchung in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur Untersuchung auf Befehl ausschließen. Geben Sie dazu die Datei als Parameter **Objekte ausschließen** oder als Parameter **Nicht erkennen** für diese Aufgaben an.

Die Wiederherstellung von Dateien aus dem Backup kann zu einer Infektion des Computers führen.

Beim Wiederherstellen einer Datei können Sie entscheiden, wo sie gespeichert werden soll: Am ursprünglichen Speicherplatz (gilt als Standard), in einen speziellen Ordner für wiederhergestellte Objekte auf dem geschützten Server oder in einen von benutzerdefinierten Ordner auf dem Rechner, auf dem die Konsole von Kaspersky Anti-Virus installiert ist, oder auf einem anderen Computer des lokalen Netzwerks.

Damit Kaspersky Anti-Virus bei der Wiederherstellung von Dateien aus dem Backup Objekte mit großem Umfang nicht untersucht, legen Sie eine Ausnahme für den Ordner %Temp%\wseeqbfiles\ fest.

Der Wiederherstellungsordner dient zum Speichern von wiederhergestellten Objekten auf dem geschützten Server. Sie können für seine Untersuchung spezielle Sicherheitseinstellungen festlegen. Der Pfad dieses Ordners wird durch die Backup-Parameter angegeben. S. Pkt "Anpassen der Backup-Parameter" (s. S. 94).

Wenn Kaspersky Anti-Virus eine Datei wiederherstellt, wird standardmäßig eine Kopie im Backup angelegt. Nach der Wiederherstellung können Sie die Sicherungskopie aus dem Backup löschen.

Um Dateien aus dem Backup wiederherzustellen, gehen Sie wie folgt vor:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.
2. Führen Sie eine der Aktionen durch:
   - Um eine Datei wiederherzustellen, öffnen Sie das Kontextmenü in der Backup-Dateiliste durch Rechtsklick auf die betreffende Datei und wählen Sie den Befehl **Wiederherstellen**.
   - Um mehrere Dateien wiederherzustellen, wählen Sie in der Liste die entsprechenden Dateien mit Hilfe der Taste **Strg** oder **Umschalt** aus. Öffnen Sie anschließend das Kontextmenü durch Rechtsklick auf eine der markierten Dateien, und wählen Sie den Befehl **Wiederherstellen**.
3. Geben Sie im Fenster **Objektwiederherstellung** den Ordner an, in dem die wiederhergestellte Datei gespeichert werden soll.

   Der Dateiname wird im Feld **Objekt** im oberen Bereich des Fensters angezeigt. Wenn Sie mehrere Dateien markiert haben, wird der Name der ersten Datei in der Auswahlliste angezeigt.

   Führen Sie eine der Aktionen durch:

   - Um eine wiederhergestellte Datei auf dem geschützten Server zu speichern, wählen Sie eine der folgenden Optionen:
     - **Im Ursprungsordner wiederherstellen**, wenn Sie die Datei im ursprünglichen Ordner wiederherstellen möchten.
     - **Im standardmäßigen Server-Ordner wiederherstellen**, wenn Sie eine Datei in einem Ordner wiederherstellen wollen, den Sie in den Backup-Einstellungen als Ordner für wiederhergestellte Objekte angegeben haben.

- Um eine wiederhergestellte Datei in einem anderen Ordner zu speichern, wählen Sie **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** und wählen Sie den entsprechenden Ordner aus (auf dem Computer, auf dem die Konsole von Kaspersky Anti-Virus installiert ist, oder einen Netzwerkordner) oder geben Sie seinen Pfad an.

4. Wenn Sie nach der Wiederherstellung eine Kopie der Datei im Backup-Ordner speichern möchten, deaktivieren Sie das Kontrollkästchen **Objekte nach der Wiederherstellung aus dem Backup löschen**.
5. Wenn Sie mehrere Dateien für die Wiederherstellung markiert haben und die festgelegten Speicherbedingungen auch auf die übrigen markierten Dateien angewendet werden sollen, aktivieren Sie das Kontrollkästchen **Auf alle ausgewählten Objekte anwenden**.

   Alle ausgewählten Dateien werden im vorgegebenen Ordner wiederhergestellt und gespeichert: Bei Auswahl der Variante **Im Ursprungsordner auf dem Server wiederherstellen** wird jede Datei in ihrem ursprünglichen Ordner gespeichert. Bei Auswahl der Variante **Im standardmäßigen Server-Ordner wiederherstellen** oder **In einem Ordner auf lokalem Rechner oder in einer Netzwerkressource wiederherstellen** werden alle Dateien im angegebenen Ordner gespeichert.
6. Klicken Sie auf **OK**.

   Kaspersky Anti-Virus beginnt damit, das erste von Ihnen ausgewählte Objekt wiederherzustellen.

   Wenn im angegebenen Ordner bereits eine Datei mit diesem Namen vorhanden ist, wird das Fenster **Ein Objekt mit diesem Namen ist bereits vorhanden** geöffnet.
7. Führen Sie folgende Aktionen aus:

   a. Wählen Sie eine der folgenden Bedingungen für das Speichern einer wiederhergestellten Datei aus:

      - **Ersetzen**, um eine vorhandenen Datei durch die wiederhergestellte Datei zu ersetzen.
      - **Umbenennen**, um die wiederhergestellte Datei unter einem anderen Namen zu speichern. Tragen Sie im Eingabefeld einen neuen Dateinamen und den vollständigen Pfad ein.
      - **Umbenennen und Suffix hinzufügen**, um die Datei umzubenennen, indem ihrem Namen ein Suffix hinzugefügt wird. Tragen Sie im Eingabefeld das Suffix ein.

   b. Wenn Sie die ausgewählte Aktion **Ersetzen** oder **Umbenennen** und Suffix hinzufügen auf die übrigen markierten Dateien anwenden möchten, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**.

      (Wenn Sie die Option **Umbenennen** ausgewählt haben, steht das Kontrollkästchen **Auf alle Objekte anwenden** nicht zur Verfügung.

   c. Klicken Sie auf **OK**.

   Die Datei wird wiederhergestellt. Informationen über den Wiederherstellungsvorgang werden im Systemaudit-Bericht protokolliert.

   Wenn Sie mehrere Dateien zur Wiederherstellung ausgewählt und die Variante **Auf alle ausgewählten Objekte anwenden** im Fenster **Objektwiederherstellung** nicht ausgewählt haben, wird das Fenster **Objektwiederherstellung** erneut geöffnet. Dort können Sie den Ordner angeben, in dem die nächste ausgewählte Datei beim Wiederherstellen gespeichert werden soll (s. Schritt 3 in dieser Anweisung).

DATEIEN AUS BACKUP LÖSCHEN

Um eine oder mehrere Dateien aus dem Backup zu entfernen, gehen Sie wie folgt vor:

1. Gehen Sie in der Konsolenstruktur auf den Knoten **Backup**.
2. Führen Sie eine der Aktionen durch:

   - Um eine Datei zu löschen, öffnen Sie in der Objektliste das Kontextmenü durch Rechtsklick auf die entsprechende Datei und wählen Sie den Befehl **Löschen**.
   - Um mehrere Dateien zu löschen, markieren Sie in der Liste die entsprechenden Dateien mit Hilfe der Taste **Strg** oder **Umschalt**. Öffnen Sie anschließend das Kontextmenü durch Rechtsklick auf einen der gewählten Dateien, und wählen Sie den Befehl **Löschen**.
3. Klicken Sie im Fenster **Bestätigung** auf die Schaltfläche **Ja**, um die Operation zu bestätigen. Die ausgewählten Dateien werden gelöscht.

ANPASSEN DER BACKUP-PARAMETER IN DER MMC

In diesem Abschnitt wird beschrieben, wie die Backup-Einstellungen angepasst werden.

Neue Werte für die Backup-Parameter werden sofort nach dem Speichern übernommen.

Um die Backup-Parameter anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Backup** und wählen Sie den Befehl **Eigenschaften** aus.
2. Gehen Sie im Fenster **Eigenschaften: Backup** wie folgt vor:
   - 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 Namen und vollständigen Pfad an.
   - Um die maximale Größe des Backups festzulegen, aktivieren Sie das Kontrollkästchen **Maximale Größe des Backups** und tragen Sie im Eingabefeld den entsprechenden Wert in MB ein.
   - Um einen Grenzwert für freien Speicherplatz im Backup festzulegen, definieren Sie den Wert des Parameters **Maximale Größe des Backups**, aktivieren Sie das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz (MB)** und tragen Sie im Eingabefeld den entsprechenden Wert in MB ein.
   - Um einen anderen Wiederherstellungsordner anzugeben, wählen Sie in der Einstellungsgruppe **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 an.
3. Klicken Sie auf **OK**.

STATISTIK FÜR BACKUP

In der Statistik für das Backup können Sie Informationen über den aktuellen Status des Backups erhalten.

Um eine Statistik für das Backup anzuzeigen,

öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Backup** und wählen Sie den Befehl **Statistik**. Das Fenster **Backup-Statistik** wird geöffnet.

Im Fenster **Backup-Statistik** werden Informationen über den aktuellen Status des Backups angezeigt (s. Tabelle unten).

Tabelle 21. Informationen über den aktuellen Backup-Status

FELD	BESCHREIBUNG
Aktuelle Größe des Backups	Datenvolumen im Backup-Ordner. Die Größe bezieht sich auf die verschlüsselten Dateien.
Objekte insgesamt	Aktuelle Anzahl der Objekte im Backup

REGISTRIEREN VON EREIGNISSEN. BERICHTE VON KASPERSKY ANTI-VIRUS

Dieser Abschnitt informiert über die Verwendung folgender Berichte von Kaspersky Anti-Virus: Systemaudit-Bericht, Berichte über die Ausführung der Aufgaben von Kaspersky Anti-Virus und Ereignisbericht von Kaspersky Anti-Virus.

IN DIESEM ABSCHNITT

METHODEN ZUM REGISTRIEREN VON EREIGNISSEN IN KASPERSKY ANTI-VIRUS

In Kaspersky Anti-Virus werden Ereignisse in zwei Gruppen unterteilt:

- Ereignisse im Zusammenhang mit der Verarbeitung von Objekten in den Aufgaben von Kaspersky Anti-Virus
- Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Anti-Virus, beispielsweise Programmstart, Erstellen oder Löschen von Aufgaben, Aufgabenstart, Ändern der Aufgabeneinstellungen

Kaspersky nutzt folgende Methoden zum Registrieren von Ereignissen:

- **Berichte über Aufgabenausführung**. Ein Bericht über Aufgabenausführung enthält Informationen über die aktuellen Aufgabenparameter, den aktuellen Aufgabenstatus und Ereignisse, die während der Aufgabenausführung eingetreten sind.
- **Systemaudit-Bericht**. Der Systemaudit-Bericht enthält Informationen über Ereignisse im Zusammenhang mit der Verwaltung von Kaspersky Anti-Virus.
- **Ereignisbericht**. Das Ereignisjournal enthält Informationen über Ereignisse, die für die Crash-Diagnose von Kaspersky Anti-Virus erforderlich sind. Das Ereignisjournal ist in der Konsole "Event Viewer" von Microsoft Windows verfügbar.

Wenn bei der Arbeit von Kaspersky Anti-Virus ein Problem auftreten sollte (z.B. Kaspersky Anti-Virus oder eine bestimmte Aufgabe stürzen ab) und Sie möchten das Problem diagnostizieren, können Sie einen Ablaufverfolgungsbericht und Speicherauszüge für die Kaspersky Anti-Virus-Prozesse anlegen und diese Dateien zur Analyse an den Technischen Kundendienst von Kaspersky Lab einschicken. Nähere Informationen über das Erstellen von Ablaufverfolgungsberichten und Speicherauszügen finden Sie im Abschnitt "Anpassen der allgemeinen Einstellungen von Kaspersky Anti-Virus in der Konsole von Kaspersky Anti-Virus" (s. S. 36).

Informationen in Speicherdump- und Protokolldateien werden von Kaspersky Anti-Virus im Klartext aufgezeichnet.

SYSTEMAUDIT-BERICHT

In Kaspersky Anti-Virus wird ein Systemaudit von Ereignissen im Zusammenhang mit der Verwaltung von Kaspersky Anti-Virus geführt. Das Programm sammelt beispielsweise Informationen über den Programmstart, den Start und die Beendigung von Aufgaben in Kaspersky Anti-Virus, die Änderung von Aufgabeneinstellungen oder das Erstellen und Löschen von Aufgaben zur Untersuchung auf Befehl. Einträge zu diesen Ereignissen werden im Ergebnisfenster angezeigt, wenn Sie in der Konsole von Kaspersky Anti-Virus den Knoten **Systemaudit-Bericht** auswählen.

In der Grundeinstellung speichert Kaspersky Anti-Virus die Ereignisse des Systemaudit-Berichts für unbeschränkte Zeit. Sie können die Aufbewahrungsdauer der Einträge im Systemaudit-Bericht anpassen.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Anti-Virus die Dateien des Berichts zum System-Audit speichert.

IN DIESEM ABSCHNITT

EREIGNISSE IM SYSTEMAUDIT-BERICHT SORTIEREN

Standardmäßig werden die Ereignisse im Systemaudit-Bericht in umgekehrter chronologischer Reihenfolge dargestellt.

Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte außer der Spalte Ereignisse sortieren.

Um Ereignisse im Systemaudit-Bericht zu sortieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Wählen Sie den untergeordneten Knoten **Systemaudit-Bericht**.
3. Klicken Sie im Ergebnisfenster auf den Titel der Spalte, nach deren Inhalt die Ereignisse in der Ereignisliste sortiert werden sollen.

   Die Ergebnisse der Sortierung bleiben bis zur nächsten Anzeige des Systemaudit-Berichts erhalten.

EREIGNISSE IM SYSTEMAUDIT-BERICHT FILTERN

Sie können im Systemaudit-Bericht nur die Einträge jener Ereignisse anzeigen, die Ihren Filterkriterien (Filtern) entsprechen.

Um Ereignisse im Systemaudit-Bericht zu filtern, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Öffnen Sie das Kontextmenü des Knotens **Systemaudit-Bericht** und wählen Sie den Punkt **Filter**.

   Das Fenster **Filtereinstellungen** wird geöffnet.
3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:
   a. Wählen Sie aus der Liste **Feldname** die Spalte, nach der die Filterung erfolgen soll.
   b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.
   c. Wählen Sie in der Liste **Feldwert** den Filterwert.
   d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.
4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:
   - Wenn Sie mehrere Filter durch logisches "UND" verknüpfen möchten, wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind**.
   - Wenn Sie mehrere Filter durch logisches "ODER" verknüpfen möchten, wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist**.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Filterkriterien für Ereignisse im Systemaudit-Bericht zu speichern.

   In der Ereignisliste des Systemaudit-Berichts werden nur Ereignisse angezeigt, die den Filterkriterien entsprechen. Die Filterergebnisse bleiben bis zur nächsten Anzeige des Systemaudit-Berichts erhalten.

Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Öffnen Sie das Kontextmenü des Knotens **Systemaudit-Bericht** und wählen Sie den Punkt **Filter entfernen**.

   In der Ereignisliste des Systemaudit-Berichts werden alle Ereignisse angezeigt.

EREIGNISSE AUS DEM SYSTEMAUDIT-BERICHT LÖSCHEN

In der Grundeinstellung speichert Kaspersky Anti-Virus die Ereignisse des Systemaudit-Berichts für unbeschränkte Zeit. Sie können die Aufbewahrungsdauer der Einträge im Systemaudit-Bericht anpassen.

Sie können manuell alle Ereignisse aus dem Systemaudit-Bericht löschen.

Um Ereignisse aus dem Systemaudit-Bericht zu entfernen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Öffnen Sie das Kontextmenü des Knotens **Systemaudit-Bericht** und wählen Sie den Punkt **Leeren**.
3. Führen Sie eine der Aktionen durch:
   - Wenn Sie den Inhalt des Systemaudit-Berichts vor dem Löschen der Ereignisse aus dem Bericht in einer csv-Datei oder txt-Datei speichern möchten, klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Ja**. Geben Sie im folgenden Fenster den Namen und den Speicherort der Datei an.
   - Wenn Sie den Inhalt des Berichts nicht in einer Datei speichern möchten, klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Nein**.

Der Systemaudit-Bericht wird gelöscht.

BERICHTE ÜBER AUFGABENAUSFÜHRUNG

Dieser Abschnitt enthält Informationen zu den Berichten über die Aufgabenausführung in Kaspersky Anti-Virus sowie Anweisungen für deren Ausführung.

IN DIESEM ABSCHNITT

BERICHTE ÜBER AUFGABENAUSFÜHRUNG

Informationen über die Ausführung von Aufgaben in Kaspersky Anti-Virus werden im Ergebnisfenster angezeigt, wenn in der Konsole von Kaspersky Anti-Virus der Knoten **Berichte über Aufgabenausführung** ausgewählt ist.

Im Bericht über die Aufgabenausführung können Sie eine Statistik über die Aufgabenausführung, Informationen für alle Objekte, die seit den Start dem Aufgabenstart bis zum aktuellen Zeitpunkt vom Programm verarbeitet wurden sowie die Aufgabeneinstellungen anzeigen.

Standardmäßig werden Einträge in den Berichten über die Aufgabenausführung von Kaspersky Anti-Virus 30 Tage lang ab der Beendigung der Aufgabe aufbewahrt. Sie können die Aufbewahrungsdauer der Einträge in den Berichten über die Aufgabenausführung ändern.

Sie können einen vom Standardordner abweichenden Ordner angeben, in dem Kaspersky Anti-Virus die Dateien der Berichte über die Aufgabenausführung speichert. Ferner können Sie die Ereignisse auswählen, über die Kaspersky Anti-Virus Einträge in den Berichten über die Aufgabenausführung speichert.

EREIGNISLISTE IN DEN BERICHTEN ÜBER DIE AUSGABENAUSFÜHRUNG ANZEIGEN

- *Um in den Berichten über die Aufgabenausführung eine Ereignisliste anzuzeigen, gehen Sie wie folgt vor:*

  1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
  2. Wählen Sie den untergeordneten Knoten **Berichte über Aufgabenausführung**.

     Die Ereignisliste, die in den Berichten über die Ausführung von Aufgaben in Kaspersky Anti-Virus gespeichert ist, wird im Ergebnisfenster angezeigt.

  Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte sortieren oder einen Filter anwenden.

EREIGNISLISTE IN DEN BERICHTEN ÜBER DIE AUSGABENAUSFÜHRUNG SORTIEREN

Standardmäßig werden die Ereignisse in den Berichten über die Aufgabenausführung in umgekehrter chronologischer Reihenfolge dargestellt. Sie können die Ereignisse nach dem Inhalt einer beliebigen Spalte sortieren.

- *Um die Ereignisse in den Berichten über die Aufgabenausführung zu sortieren, gehen Sie wie folgt vor:*

  1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
  2. Wählen Sie den untergeordneten Knoten **Berichte über Aufgabenausführung**.
  3. Klicken Sie im Ergebnisfenster auf den Titel der Spalte, nach deren Inhalt die Ereignisse in den Berichten über die Ausführung von Aufgaben in Kaspersky Anti-Virus sortiert werden sollen.

     Die Ergebnisse der Sortierung bleiben bis zur nächsten Anzeige der Berichte über die Aufgabenausführung erhalten.

EREIGNISLISTE IN DEN BERICHTEN ÜBER DIE AUSGABENAUSFÜHRUNG FILTERN

Sie können in der Ereignisliste der Berichte über die Aufgabenausführung nur die Einträge jener Ereignisse anzeigen, die Ihren Filterkriterien (Filtern) entsprechen.

- *Um die Ereignisse in den Berichten über die Aufgabenausführung zu filtern, gehen Sie wie folgt vor:*

  1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
  2. Öffnen Sie das Kontextmenü des Knotens **Berichte über Aufgabenausführung** und wählen Sie den Punkt **Filter**.

     Das Fenster **Filtereinstellungen** wird geöffnet.
  3. Um einen Filter hinzufügen, führen Sie folgende Aktionen durch:

     a. Wählen Sie aus der Liste **Feldname** die Spalte, nach der die Filterung erfolgen soll.

     b. Wählen Sie in der Liste **Operator** die Filterbedingungen. Die Filterkriterien unterscheiden sich in Abhängigkeit der in der Liste **Feldname** ausgewählten Option.

     c. Wählen Sie in der Liste **Feldwert** den Filterwert.

     d. Klicken Sie auf die Schaltfläche **Hinzufügen**.

     Der hinzugefügte Filter wird in der Filterliste im Fenster **Filtereinstellungen** angezeigt.

4. Führen Sie erforderlichenfalls eine der folgenden Aktionen durch:
   - Wenn Sie mehrere Filter durch logisches "UND" verknüpfen möchten, wählen Sie die Variante **Wenn alle Bedingungen erfüllt sind**.
   - Wenn Sie mehrere Filter durch logisches "ODER" verknüpfen möchten, wählen Sie die Variante **Wenn eine beliebige Bedingung erfüllt ist**.
5. Klicken Sie auf die Schaltfläche **Übernehmen**, um die Filterkriterien für Ereignisse in den Berichten über die Aufgabeausführung zu speichern.

   In der Ereignisliste der Berichte über die Aufgabenausführung werden nur Ereignisse angezeigt, die den Filterkriterien entsprechen. Die Filterergebnisse der Sortierung bleiben bis zur nächsten Anzeige der Berichte über die Aufgabenausführung erhalten.

Um die Filterfunktion auszuschalten, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Öffnen Sie das Kontextmenü des Knotens **Berichte über Aufgabenausführung** und wählen Sie den Punkt **Filter entfernen**.

   In der Ereignisliste der Berichte über die Aufgabenausführung werden alle Ereignisse angezeigt.

STATISTIK UND INFORMATIONEN ÜBER EINE AUFGABE VON KASPERSKY ANTI-VIRUS IN DEN BERICHTEN ÜBER DIE AUFGABENAUSFÜHRUNG ANZEIGEN

In den Berichten über die Aufgabenausführung können Sie detaillierte Informationen über alle Ereignisse, die in den Aufgaben seit ihrem Start bis zum aktuellen Zeitpunkt aufgetreten sind, sowie eine Statistik über die Aufgabenausführung und die Aufgabeneinstellungen anzeigen.

Gehen Sie folgendermaßen vor, um die Statistik und Informationen über die Ausführung von Aufgaben in Kaspersky Anti-Virus anzuzeigen:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Wählen Sie den untergeordneten Knoten **Berichte über Aufgabenausführung**.
3. Öffnen Sie im Ergebnisfenster das Fenster **Bericht** auf eine der folgenden Arten:
   - Doppelklicken Sie auf ein Ereignis, das in der Aufgabe aufgetreten ist, deren Bericht Sie anzeigen möchten.
   - Öffnen Sie das Kontextmenü für das Ereignis, das in der Aufgabe aufgetreten ist, deren Bericht Sie anzeigen möchten, und wählen Sie den Punkt **Bericht anzeigen**.
4. Im folgenden Fenster werden folgende Informationen angezeigt:
   - Auf der Registerkarte **Statistik** werden Startzeit und Zeitpunkt der Beendigung der Aufgabe sowie deren Statistik angezeigt.
   - Auf der Registerkarte **Ereignisse** wird eine Liste der Ereignisse angezeigt, die bei der Ausführung der Aufgabe aufgetreten sind.
   - Auf der Registerkarte **Einstellungen** werden die Aufgabeneinstellungen angezeigt.
5. **Klicken Sie erforderlichenfalls auf die Schaltfläche** Filter, um die Ereignisse im Bericht über die Aufgabenausführung zu filtern.
6. Klicken Sie erforderlichenfalls auf die Schaltfläche **Export**, um Informationen aus dem Bericht über die Aufgabenausführung in eine csv-Datei oder eine txt-Datei zu exportieren.
7. Klicken Sie auf **Schließen**, um das Fenster **Bericht** zu schließen.

INFORMATIONEN AUS EINEM BERICHT ÜBER DIE AUFGABENAUSFÜHRUNG EXPORTIEREN

Sie können Informationen aus dem Bericht über die Aufgabenausführung in eine csv-Datei oder in eine txt-Datei exportieren.

Gehen Sie folgendermaßen vor, um Informationen aus dem Bericht über die Aufgabenausführung zu exportieren:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Wählen Sie den untergeordneten Knoten **Berichte über Aufgabenausführung**.
3. Öffnen Sie im Ergebnisfenster das Fenster **Bericht** auf eine der folgenden Arten:
   - Doppelklicken Sie auf ein Ereignis, das in der Aufgabe aufgetreten ist, deren Bericht Sie anzeigen möchten.
   - Öffnen Sie das Kontextmenü für das Ereignis, das in der Aufgabe aufgetreten ist, deren Bericht Sie anzeigen möchten, und wählen Sie den Punkt **Bericht anzeigen**.
4. Klicken Sie im unteren Bereich des Fensters **Bericht** auf die Schaltfläche **Export**.

   Das Fenster **Speichern unter** wird angezeigt.
5. Geben Sie den Namen, den Speicherort, den Typ und die Codierung der Datei an, in die Sie die Information aus dem Bericht über die Aufgabenausführung exportieren möchten, und klicken Sie auf die Schaltfläche **Speichern**.

EREIGNISSE AUS DEN BERICHTEN ÜBER DIE AUFGABENAUSFÜHRUNG LÖSCHEN

Standardmäßig werden Einträge in den Berichten über die Aufgabenausführung von Kaspersky Anti-Virus 30 Tage lang ab der Beendigung der Aufgabe aufbewahrt. Sie können die Aufbewahrungsdauer der Einträge in den Berichten über die Aufgabenausführung ändern.

Sie können alle Ereignisse manuell aus den Berichten über die Ausführung der zum aktuellen Zeitpunkt abgeschlossenen Aufgaben löschen.

Ereignisse aus Berichten über Aufgaben, die zum aktuellen Zeitpunkt ausgeführt werden, sowie aus Berichten, die von anderen Benutzern verwendet werden, können nicht gelöscht werden.

Um die Ereignisse aus den Berichten über die Aufgabenausführung zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Berichte**.
2. Wählen Sie den untergeordneten Knoten **Berichte über Aufgabenausführung**.
3. Führen Sie eine der Aktionen durch:
   - Wenn Sie die Ereignisse aus allen Berichten über die Ausführung von Aufgaben, die zum aktuellen Zeitpunkt abgeschlossen sind, löschen möchten, öffnen Sie das Kontextmenü für den untergeordneten Knoten **Berichte über Aufgabenausführung** und wählen Sie den Punkt **Leeren**.
   - Wenn Sie den Bericht über die Ausführung einer einzelnen Aufgabe löschen möchten, öffnen Sie im Ergebnisfenster das Kontextmenü für das Ereignis, das in der Aufgabe aufgetreten ist, dessen Ausführungsbericht Sie löschen möchten, und wählen Sie den Punkt **Löschen**.
   - Gehen Sie folgendermaßen vor, um Berichte über die Ausführung mehrerer Aufgaben zu löschen:
     a. Wählen Sie im Ergebnisfenster mithilfe der Tasten **Strg** oder **Umschalt** die Ereignisse aus, die in den Aufgaben aufgetreten sind, deren Ausführungsberichte Sie leeren möchten.
     b. Öffnen Sie das Kontextmenü eines beliebigen ausgewählten Ereignisses und wählen Sie den Punkt **Löschen**.
4. Klicken Sie im Fenster zur Bestätigung des Löschvorgangs auf die Schaltfläche **Ja**, um das Löschen zu bestätigen.

Die ausgewählten Berichte über die Aufgabenausführung werden gelöscht. Das Löschen von Ereignissen aus den Berichten über die Aufgabenausführung wird im Systemaudit-Bericht protokolliert.

EREIGNISBERICHT VON KASPERSKY ANTI-VIRUS IN DER KONSOLE EREIGNISANZEIGE ANZEIGEN

Mit Hilfe des Snap-ins **Ereignisanzeige** für Microsoft Management Console können Sie den Ereignisbericht von Kaspersky Anti-Virus anzeigen. Darin protokolliert Kaspersky Anti-Virus Ereignisse, die für die Crash-Diagnose von Kaspersky Anti-Virus erforderlich sind.

Sie können auf Grundlage folgender Kriterien Ereignisse auswählen, die im Ereignisbericht registriert werden sollen:

- **nach Ereignistypen**.
- **nach der Genauigkeitsstufe**. Die Genauigkeitsstufe entspricht der Prioritätsstufe von Ereignissen, die im Bericht registriert werden (informative, wichtige oder kritische Ereignisse). Am ausführlichsten ist die Stufe **Informative Ereignisse**, bei der Ereignisse aller Prioritätsstufen aufgezeichnet werden. Dagegen werden auf der relativ oberflächlichen Stufe **Kritische Ereignisse** nur kritische Ereignisse registriert. In der Grundeinstellung gilt für alle Komponente außer für die Komponente **Update** die Genauigkeitsstufe **Wichtige Ereignisse** (Es werden nur wichtige und kritische Ereignisse registriert). Für die Komponente **Update** gilt die Stufe **Informative Ereignisse**.

Um den Ereignisbericht von Kaspersky Anti-Virus anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Start**, geben Sie in der Suchzeile den Befehl `mmc` ein und klicken Sie auf die Taste **EINGABE**.

   Es öffnet sich das Fenster Microsoft Management Console.

2. Wählen Sie **Datei → Snap-in hinzufügen oder löschen**.

   Das Fenster **Snap-in hinzufügen und löschen** wird geöffnet.

3. Wählen Sie aus der Liste der verfügbaren Snap-ins das Snap-in **Ereignisanzeige** und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Computer auswählen** wird geöffnet.

4. Geben Sie im Fenster **Computer auswählen** den Computer an, auf dem Kaspersky Anti-Virus installiert ist, und klicken Sie auf die Schaltfläche **OK**.

5. Klicken Sie im Fenster **Snap-ins hinzufügen/entfernen** auf **OK**.

   In der Konsolenstruktur erscheint der Knoten **Ereignisanzeige**.

6. Öffnen Sie in der Struktur der Konsole den Knoten **Ereignisanzeige** und wählen Sie den untergeordneten Knoten **Berichte für Anwendungen und Dienste → Kaspersky Anti-Virus**.

   Das Ereignisprotokoll für Kaspersky Anti-Virus wird geöffnet.

EINSTELLUNGEN DER BERICHTE VON KASPERSKY ANTI-VIRUS IN DER KONSOLE VON KASPERSKY ANTI-VIRUS ANPASSEN

Sie können folgenden Einstellungen der Berichte von Kaspersky Anti-Virus anpassen:

- Aufbewahrungsdauer der Ereignisse in den Berichten über die Aufgabenausführung und im Systemaudit-Bericht
- Pfad des Ordners, in dem Kaspersky Anti-Virus die Dateien der Berichte über die Aufgabenausführung und den Systemaudit-Bericht speichert
- Ereignisse, die Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung, dem Systemaudit-Bericht und im Ereignisprotokoll von Kaspersky Anti-Virus in der Konsole Ereignisanzeige speichert.

Um die Berichtsparameter von Kaspersky Anti-Virus anzupassen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten **Berichte** und wählen Sie den Punkt **Eigenschaften**.

   Das Fenster **Eigenschaften: Berichte** wird geöffnet.

2. Passen Sie im Fenster **Eigenschaften: Berichte** die Berichtseinstellungen gemäß Ihren Anforderungen an. Gehen Sie hierzu wie folgt vor:

   - Wählen Sie auf der Registerkarte **Allgemein** erforderlichenfalls jene Ereignisse aus, die Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung, dem Systemaudit-Bericht und im Ereignisprotokoll von Kaspersky Anti-Virus in der Konsole Ereignisanzeige speichern soll. Gehen Sie hierzu wie folgt vor:

     - Wählen Sie in der Liste **Komponente** eine Anti-Virus-Komponente, deren Genauigkeitsstufe für Ereignisse Sie anpassen möchten.

Für die Komponenten **Echtzeitschutz für Dateien**, **RPC: Schutz von Netzwerkspeichern**, **ICAP: Schutz von Netzwerkspeichern**, **Skript-Untersuchung**, **Untersuchung auf Befehl** und **Update** ist eine Protokollierung von Ereignissen im Bericht über die Aufgabenausführung und im Ereignisprotokoll vorgesehen. Für diese Komponenten enthält die Ereignisliste die Spalten **Berichte** und **Ereignisbericht**. Für die Komponenten **Quarantäne** und **Backup** werden die Ereignisse im Systemaudit-Bericht und im Ereignisbericht protokolliert. Für diese Komponenten enthält die Ereignisliste die Spalten **Audit** und **Ereignisprotokoll**.

- Wählen Sie in der Liste **Prioritätsstufe** die Genauigkeitsstufe der Ereignisse in den Berichten über die Aufgabenausführung und im Systemaudit-Bericht für die ausgewählte Funktionskomponente.

  In der unten stehenden Tabelle der Ereignisliste sind die Kontrollkästchen neben jenen Ereignissen aktiviert, die in den Berichten über die Aufgabenausführung, dem Systemaudit-Bericht und im Ereignisprotokoll gemäß der ausgewählten Genauigkeitsstufe protokolliert werden.

- Wenn Sie die Protokollierung einzelner Ereignisse für die ausgewählte Funktionskomponente manuell aktivieren möchten, gehen Sie wie folgt vor:

a. Wählen Sie in der Liste **Prioritätsstufe** die Variante **Benutzerdefiniert**.

b. Aktivieren Sie in der Tabelle Ereignisliste die Kontrollkästchen neben jenen Ereignissen, für die Sie die Protokollierung in den Berichten zur Aufgabenausführung, im Systemaudit-Bericht und im Ereignisprotokoll aktivieren möchten.

- Wählen Sie auf der Registerkarte **Erweitert** erforderlichenfalls den Ordner aus, in dem Kaspersky Anti-Virus die Berichtsdateien speichern soll, und geben Sie die Aufbewahrungsdauer der Ereignisse in den Berichten zur Aufgabenausführung und im Systemaudit-Bericht:

  - **Ordner für Berichte**.

    Pfad zum Ordner mit Berichten im UNC-Format (Universal Naming Convention).

    Standardmäßig ist der folgende Pfad festgelegt: C:\ProgramData\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Reports\.

  - **Berichte über Aufgabenausführung und Ereignisse löschen, die älter sind als (Tage)**.

    Das Kontrollkästchen aktiviert / deaktiviert die Funktion, die Berichte über die Ergebnisse beendeter Aufgaben und Ereignisse sowie die in den Berichten veröffentlichten ausgeführten Aufgaben nach Ablauf der vorgegebenen Frist (als Standard gelten 30 Tage) löscht.

    Wenn dieses Kontrollkästchen aktiviert ist, löscht Kaspersky Anti-Virus nach Ablauf der vorgegebenen Frist die Berichte über die Ergebnisse beendeter Aufgaben und Ereignisse sowie die in den Berichten veröffentlichten ausgeführten Aufgaben.

    Das Kontrollkästchen ist standardmäßig aktiviert.

  - **Ereignisse des Audit-Berichts löschen, die älter sind als (Tage)**.

    Das Kontrollkästchen aktiviert / deaktiviert die Funktion, die im Audit-Bericht eingetragene Ereignisse nach Ablauf der vorgegebenen Frist (als Standard gelten 60 Tage) löscht.

    Wenn dieses Kontrollkästchen aktiviert ist, löscht Kaspersky Anti-Virus nach Ablauf der vorgegebenen Frist die im Audit-Bericht eingetragenen Ereignisse.

    Das Kontrollkästchen ist standardmäßig aktiviert.

3. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern und das Fenster zu schließen.

NUTZUNG VON SCHLÜSSELN IN KASPERSKY ANTI-VIRUS

In diesem Abschnitt wird beschrieben, wie ein Schlüssel zum Programm hinzugefügt wird, wie ein Schlüssel aus dem Programm gelöscht wird und wie Informationen über hinzugefügte Schlüssel angezeigt werden können.

In diesem Abschnitt

Schlüssel hinzufügen

Mithilfe der Schlüsseldatei können Sie einen Schlüssel zum Programm hinzufügen.

Wenn Sie einen Schlüssel als aktiven Schlüssel hinzufügen und in Kaspersky Anti-Virus 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 Anti-Virus 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 Anti-Virus bereits ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt worden sind, wird der zuvor hinzugefügte aktive Schlüssel durch den neuen ersetzt und der Reserveschlüssel wird gelöscht.

Um einen Schlüssel hinzufügen, gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten **Lizenzverwaltung** und wählen Sie den Befehl **Schlüssel hinzufügen**.
2. Geben Sie im Fenster **Schlüssel hinzufügen** die Schlüsseldatei an.
3. Wenn Sie den Schlüssel als Reserveschlüssel hinzufügen möchten, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel verwenden**.
4. Klicken Sie auf **OK**.

Siehe:

Schlüssel löschen

Sie können den hinzugefügten Schlüssel löschen.

Wenn in Kaspersky Anti-Virus ein Reserveschlüssel hinzugefügt wurde und Sie den aktiven Schlüssel löschen, wird der Reserveschlüssel automatisch zum aktiven Schlüssel.

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

Gehen Sie folgendermaßen vor, um einen hinzugefügten Schlüssel zu löschen:

1. Wählen Sie in der Konsolenstruktur den Knoten **Lizenzverwaltung**.
2. Öffnen Sie im Ergebnisfenster das Kontextmenü für die Infozeile des betreffenden Schlüssels und wählen Sie den Befehl **Löschen**.
3. Klicken Sie im Bestätigungsfenster auf die Schaltfläche **Ja**, um das Löschen des Schlüssels zu bestätigen.

INFORMATIONEN ÜBER SCHLÜSSEL ANZEIGEN

Um Informationen über die hinzugefügten Schlüssel zu anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten **Lizenzverwaltung**.
2. Öffnen Sie im Ergebnisfenster das Kontextmenü für die Infozeile des Schlüssels, dessen Daten Sie anzeigen möchten, und wählen Sie den Punkt **Eigenschaften**.

Im Ergebnisfenster werden Informationen zum Schlüssel angezeigt (s. Tabelle unten).

Tabelle 22. Informationen zur Lizenz

FELD	BESCHREIBUNG
Schlüssel	Nummer des Schlüssels.
Lizenztyp	Lizenztyp: Test, kommerziell.
Gültig bis	Ablaufdatum der mit dem Schlüssel verknüpften Lizenz.
Status	Status des Schlüssels: aktiv oder Reserve.

Im Fenster Eigenschaften: <Schlüssel> werden auf der Registerkarte Allgemein **detaillierte Informationen zum Schlüssel angezeigt** (s. Tabelle unten).

Tabelle 23. Ausführliche Informationen zur Lizenz

FELD	BESCHREIBUNG
Schlüssel	Nummer des Schlüssels.
Schlüssel hinzugefügt am	Datum, an dem der Schlüssel zum Programm hinzugefügt wurde.
Lizenztyp	Lizenztyp: Test, kommerziell.
Läuft ab in (Tage)	Anzahl der Tage bis zum Ablaufdatum der mit dem Schlüssel verknüpften Lizenz.
Gültig bis	Ablaufdatum der mit dem Schlüssel verknüpften Lizenz.
Programm	Name des Programms, für das der Schlüssel 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.

Im Fenster **Eigenschaften:** <**Schlüssel**> werden auf der Registerkarte **Erweitert** Informationen über den Kunden sowie Kontaktangaben von Kaspersky Lab oder einem Partnerunternehmen angezeigt, bei dem Sie Kaspersky Anti-Virus erworben haben.

BENACHRICHTIGUNGEN ANPASSEN

Dieser Abschnitt enthält Informationen über Möglichkeiten zur Benachrichtigung von Benutzern und Administratoren von Kaspersky Anti-Virus über Programmereignisse und den Schutzstatus des Servers sowie Anleitungen zur Anpassung von Benachrichtigungen.

IN DIESEM ABSCHNITT

METHODEN ZUR BENACHRICHTIGUNG VON ADMINISTRATOR UND BENUTZER

Sie können die Benachrichtigung des Administrators und der Benutzer, die auf den geschützten Server zugreifen, über Ereignisse, die mit den Funktionen von Kaspersky Anti-Virus und dem Status der Antiviren-Sicherheit des Servers zusammenhängen, anpassen.

Das Programm gewährleistet die Ausführung folgender Aufgaben:

- Der Administrator kann Informationen über Ereignisse bestimmter Typen erhalten.
- Die Benutzer des lokalen Netzwerks, die auf den geschützten Server zugreifen, sowie die Terminalbenutzer des Servers können Informationen über Ereignisse des Typs *Objekt gefunden* erhalten, die in der Aufgabe **Echtzeitschutz für Dateien** auftreten.

Der Befehl NET SEND sendet Benachrichtigungen über infizierte Objekte nur dann, wenn der Benutzer auf einem Remote-Computer unter Microsoft Windows Server 2003 oder niedriger oder Microsoft Windows XP arbeitet. Der Befehl NET SEND sendet keine Benachrichtigung über infizierte Objekte, wenn der Benutzer auf dem geschützten Server arbeitet.

In der Konsole von Kaspersky Anti-Virus können Sie die Benachrichtigungen für den Administrator oder die Benutzer auf unterschiedliche Weise aktivieren:

- Methoden für die Benachrichtigung der Benutzer:
  a. Werkzeuge für Terminaldienst.

     Sie können diese Methode für die Benachrichtigung von Terminalbenutzer anwenden, wenn der geschützte Server ein Terminalserver ist.

  b. Werkzeuge für Messenger.

     Sie können diese Methode für die Benachrichtigung über Microsoft Windows Messenger anwenden. Diese Methode wird nicht verwendet, wenn der geschützte Server mit dem Betriebssystem Microsoft Windows Server 2008 arbeitet.
- Methoden für Benachrichtigung von Administratoren:
  a. Werkzeuge für Messenger.

     Sie können diese Methode für die Benachrichtigung über Microsoft Windows Messenger anwenden. Diese Methode wird nicht verwendet, wenn der geschützte Server mit dem Betriebssystem Microsoft Windows Server 2008 arbeitet.

  b. Starten einer ausführbaren Datei.

     Diese Methode wird aufgrund des Ereignisses ausführbare Datei gestartet, die auf der lokalen Festplatte des geschützten Servers gespeichert ist.

  c. Per E-Mail senden.

     Diese Methode dient der Zustellung von Nachrichten per E-Mail.

Sie können einen Nachrichtentext für die einzelnen Ereignistypen festlegen. In den Text können Sie Felder mit Informationen zum Ereignis aufnehmen. Standardmäßig wird für die Benachrichtigung von Benutzern ein bereits vorgegebener Nachrichtentext verwendet.

BENACHRICHTIGUNGEN AN ADMINISTRATOR UND BENUTZER ANPASSEN

Sollen Benachrichtigungen über Ereignisse eingestellt werden, müssen zunächst die Art der Benachrichtigung und der Inhalt der Textnachricht festgelegt sein.

Um die Benachrichtigungen über Ereignisse zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie in der Konsolenstruktur das Kontextmenü für das Snap-in von Kaspersky Anti-Virus und wählen Sie den Befehl **Benachrichtigungseinstellungen anpassen**.

   Das Fenster **Benachrichtigungen** wird geöffnet.

2. **Wählen Sie im Fenster Benachrichtigungen** auf der Registerkarte Benachrichtigungen die entsprechenden Ereignisse aus und geben Sie die Benachrichtigungsmethode für diese an:

   - Um Benachrichtigungsmethoden für den Administrator auszuwählen, gehen Sie folgendermaßen vor:

     a. Wählen Sie in der Liste **Ereignistyp** das Ereignis aus, für das Sie eine Benachrichtigungsmethode festlegen möchten.

     b. Aktivieren Sie in der Optionsgruppe **Benachrichtigung für die Administratoren** das Kontrollkästchen für die Benachrichtigungen, die Sie anpassen möchten.

   - Um die Benachrichtigungsmethoden für Benutzer festzulegen, aktivieren Sie in der Einstellungsgruppe **Benachrichtigung für die Benutzer** das Kontrollkästchen neben den Methoden zur Benutzerbenachrichtigung, die Sie für das Ereignis **Objekt gefunden** anpassen möchten.

3. Klicken Sie zur Erstellung eines Nachrichtentexts auf die Schaltfläche **Text der Nachricht** in der entsprechenden Optionsgruppe. Geben Sie im Fenster **Text der Nachricht** den Text ein, der in der Benachrichtigung über das Ereignis angezeigt werden soll.

   So können Sie den gleichen Nachrichtentext für mehrere Ereignistypen festlegen: Wählen Sie zuerst die Benachrichtigungsmethode für einen Ereignistyp aus. Markieren Sie dann mithilfe der Tasten **Strg** oder **Umschalt** die übrigen Ereignistypen, für die Sie den gleichen Nachrichtentext festlegen möchten. Klicken Sie erst dann auf die Schaltfläche **Text der Nachricht**.

   Um Felder mit Informationen zum Ereignis hinzuzufügen, klicken Sie auf die Schaltfläche **Makros** und wählen Sie die entsprechenden Punkte in der Dropdown-Liste aus. Die Felder mit Informationen über Ereignisse werden in einer Tabelle in diesem Abschnitt beschrieben.

   Um den Text wiederherzustellen, der standardmäßig für Ereignisse vorgesehen ist, klicken Sie auf die Schaltfläche **Standard**.

4. Um die gewählten Benachrichtigungsarten für Administratoren anzupassen, klicken Sie im Fenster **Benachrichtigungen** auf die Schaltfläche **Einstellungen** und nehmen Sie im Fenster **Erweiterte Einstellungen** die entsprechenden Einstellungen vor. Gehen Sie hierzu wie folgt vor:

   a. Für Benachrichtigungen, die per E-Mail erfolgen sollen, öffnen Sie die Registerkarte **E-Mail** und tragen in die entsprechenden Felder die E-Mail-Adressen der Empfänger (durch Semikolon getrennt), den Namen oder die Netzwerkadresse des SMTP-Servers sowie dessen Port ein. Tragen Sie bei Bedarf den Text ein, der in den Feldern **Betreff** und **Von** angezeigt werden soll. In den Text des Feldes **Betreff** können auch Feldwerte mit Informationen über Ereignisse aufgenommen werden (siehe folgende Tabelle).

      Wenn Sie bei der Verbindung mit einem SMTP-Server die Authentifizierung für Benutzerkonten verwenden möchten, aktivieren Sie in der Gruppe **Einstellungen für die Authentifizierung** das Kontrollkästchen **SMTP-Authentifizierung verwenden** und tragen Sie Name und Kennwort des Benutzers ein, dessen Benutzerkonto geprüft werden soll.

   b. Damit Benachrichtigung über den Nachrichtendienst erfolgen, erstellen Sie auf der Registerkarte **Nachrichtendienst** eine Liste für die Computer, die Benachrichtigungen erhalten sollen: Klicken Sie für jeden Computer, den Sie hinzufügen möchten, auf **Hinzufügen** und tragen Sie im Eingabefeld den entsprechenden Netzwerknamen ein.

Bitte beachten Sie, dass Benachrichtigungen mit Hilfe von **Messengern** nicht zum Versand verwendet werden, wenn der geschützte Server unter Microsoft Windows Server 2008 bzw. den nachfolgenden Versionen von Microsoft Windows Server arbeitet.

c. Wenn eine ausführbare Datei gestartet werden soll, wählen Sie auf der Registerkarte **Ausführbare Datei** eine Datei auf einem lokalen Laufwerk des geschützten Servers aus, die nach Eintreten des Ereignisses auf dem Server ausgeführt werden soll, oder geben Sie den vollständigen Pfad der Datei an. Tragen Sie Name und Kennwort des Benutzers ein, unter dessen Benutzerkonto die Datei ausgeführt werden soll.

   Wenn Sie den Pfad einer ausführbaren Datei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable können hingegen nicht verwendet werden.

   Wenn Sie die Anzahl der Benachrichtigungen, die für einen Ereignistyp innerhalb eines bestimmten Zeitraums gesendet werden sollen, begrenzen möchten, aktivieren Sie auf der Registerkarte **Erweitert** das Kontrollkästchen **Die gleiche Benachrichtigung senden höchstens** und legen Sie eine Anzahl und eine Zeiteinheit fest.

5. Klicken Sie auf **OK**.

Tabelle 24. Felder mit Informationen über Ereignisse

FELD	BESCHREIBUNG
%EVENT_TYPE%	Ereignistyp.
%EVENT_TIME%	Zeitpunkt, zu dem ein Ereignis eingetreten ist.
%EVENT_SEVERITY%	Prioritätsstufe des Ereignisses.
%OBJECT%	Name des Objekts (in den Aufgaben zum Echtzeitschutzes und zur Virensuche). In der Aufgabe **Update der Programm-Module** steht der Name des Updates und die Adresse der Internetseite mit näheren Angaben zum Update.
%VIRUS_NAME%	Name des gefundenen Objekts gemäß der Klassifizierung der Viren-Enzyklopädie (http://www.securelist.com/de/). Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Anti-Virus beim Fund des Objekts zurückgibt. Sie können den vollständigen Namen des gefundenen Objekts im Bericht über die Aufgabenausführung anzeigen (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99).
%VIRUS_TYPE%	Typ des gefundenen Objekts gemäß der Klassifizierung von Kaspersky Lab, beispielsweise "Virus" oder "Trojaner". Gehört zur vollständigen Bezeichnung eines gefundenen Objekts, die Kaspersky Anti-Virus zurückgibt, nachdem ein Objekt als infiziert oder möglicherweise infiziert eingestuft wurde. Sie können den vollständigen Namen des gefundenen Objekts im Bericht über die Aufgabenausführung anzeigen (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99).
%USER_COMPUTER%	In den Aufgaben **Echtzeitschutz für Dateien** und **RPC: Schutz von Netzwerkspeichern** ist das der Name des Benutzercomputers, der auf dem Server auf das Objekt zugegriffen hat.
%USER_NAME%	In der Aufgabe **Echtzeitschutz für Dateien** und **RPC: Schutz von Netzwerkspeichern** ist das der Name des Benutzers, der auf dem Server auf das Objekt zugegriffen hat.
%FROM_COMPUTER%	Name des geschützten Servers, von dem die Benachrichtigung geschickt wurde.
%EVENT_REASON%	Grund für Eintreten eines Ereignisses (Dieses Feld ist für bestimmte Ereignisse nicht verfügbar).
%ERROR_CODE%	Fehlercode (Wird nur das Ereignis "Interner Aufgabenfehler" verwendet).
%TASK_NAME%	Name der Aufgabe (Nur für Ereignisse, die mit der Aufgabenausführung verbunden sind).

VERWALTUNG HIERARCHISCHER SPEICHER

Dieser Abschnitt enthält Informationen über die Antiviren-Untersuchung von Dateien, die sich in den hierarchischen Speichern und den Backup-Systemen befinden.

IN DIESEM ABSCHNITT

HIERARCHISCHER SPEICHER

Ein System zur hierarchischen Speicherverwaltung (Hierarchical Storage Management, HSM) (im Folgenden "HSM-System") ermöglicht die Übertragung von Daten zwischen schnellen lokalen Datenträgern und langsamen Geräten, die einer langfristigen Datenspeicherung dienen. Trotz offensichtlicher Vorteile der schnellen Speichergeräte erweist sich ihr Einsatz für viele Unternehmen als zu kostspielig. HSM-Systeme gewährleisten die Auslagerung von Informationen, auf die über längere Zeit nicht zugegriffen wurde, auf kostengünstige Speichermedien, wodurch die Kosten für das Unternehmen sinken.

HSM-Systeme legen einen Teil der Informationen auf ausgelagerten Speichern ab und stellen die Informationen bei Bedarf wieder bereit. Die Verwendung der Dateien wird dabei vom HSM-System permanent überwacht und es wird ermittelt, welche Dateien in einen ausgelagerten Speicher abgelegt werden können und welche sinnvollerweise auf lokalen Speichermedien verbleiben sollen. Dateien werden ausgelagert, wenn für einen bestimmten Zeitraum nicht auf sie zugegriffen wurde. Wenn ein Benutzer auf eine Datei zugreift, die sich in einem ausgelagerten Speicher befindet, wird diese Datei wieder auf den lokalen Datenträger kopiert. Dieses Prinzip bietet den Anwendern schnellen Zugriff auf große Informationsvolumen, die die verfügbare Speicherkapazität wesentlich überschreiten.

Wird eine Datei von einem lokalen Datenträger auf einen ausgelagerten Speicher übertragen, so speichert das HSM-System einen Link auf den tatsächlichen Ort dieser Datei. Wenn auf eine Link-Datei zugegriffen wird, ermittelt das System den Ort, an dem sich die Daten auf dem Archivmedium befinden. Durch das Ersetzen von Dateien durch Links, die auf den entsprechenden Speicherort verweisen, ergibt sich eine praktisch unbeschränkte Speicherkapazität.

Bestimmte HSM-Systeme ermöglichen es, Dateien teilweise in einem lokalen Medium zu speichern. In diesem Fall wird eine Datei fast vollständig ausgelagert und nur ein kleiner Teil der ursprünglichen Datei verbleibt im lokalen Speicher.

In HSM-Systemen werden zwei Methoden für den Zugriff auf Informationen eingesetzt, die in einem hierarchischen Speicher abgelegt wurden:

- Reparse Points
- erweiterte Dateiattribute

EINSTELLUNGEN DES HSM-SYSTEMS ANPASSEN

Wenn Sie kein HSM-System verwenden, belassen Sie den Standardwert für den **Typ des Zugriffs auf den hierarchischen Speicher** (**Kein HSM-System**).

Um den Zugang auf den hierarchischen Speicher einzustellen, müssen Sie angeben, auf welche Art das HSM-System den Speicherort der untersuchten Datei bestimmt. Informationen dazu finden Sie in der Dokumentation des verwendeten HSM-Systems.

Gehen Sie folgendermaßen vor, um die Methode für den Zugriff auf den hierarchischen Speicher anzugeben:

1. Verwenden Sie eine der folgenden Methoden, um das Fenster **Einstellungen des HSM-Systems** zu öffnen:
   - Öffnen Sie in der Konsolenstruktur das Kontextmenü des Knotens **Kaspersky Anti-Virus** und wählen Sie den Punkt **Hierarchischer Speicher** aus.
   - Wählen Sie in der Konsolenstruktur den Knoten **Kaspersky Anti-Virus** und öffnen Sie in der Schnellauswahlleiste über den entsprechenden Link das Fenster **Hierarchischer Speicher**.
2. Legen Sie auf der Registerkarte **Hierarchischer Speicher** die Einstellungen des HSM-Systems fest:
   - **Kein HSM-System**.
   - **HSM-System verwendet Analysepunkte**.
   - **HSM-System verwendet erweiterte Dateiattribute**.
   - **Unbekanntes HSM-System**.

   Wenn Sie eine ungültige Option angeben bzw. die Option **Unbekanntes HSM-System** auswählen, kann Kaspersky den Speicherort von Objekten möglicherweise nicht korrekt bestimmen, wodurch die Verarbeitungszeit für Objekte steigt.
3. Klicken Sie auf **OK**, um die festgelegten Einstellungen zu speichern.

IMPORT UND EXPORT VON PARAMETERN

Dieser Abschnitt enthält Informationen über den Export der Einstellungen für die Ausführung von Kaspersky Anti-Virus bzw. der Einstellungen für die Ausführung der verschiedenen Programmkomponenten in eine Konfigurationsdatei im XML-Format, sowie über den Import dieser Einstellungen aus der Konfigurationsdatei ins Programm.

IN DIESEM ABSCHNITT

PARAMETER EXPORTIEREN

Um Parameter in eine Konfigurationsdatei zu exportieren, gehen Sie wie folgt vor:

1. Wenn Sie die Parameter in der Konsole von Kaspersky Anti-Virus geändert haben, speichern Sie vor dem Export von Einstellungen die neuen Werte.
2. Führen Sie eine der Aktionen durch:
   - Um alle Einstellungen für Kaspersky Anti-Virus zu exportieren, öffnen Sie im Konsolenfenster das Kontextmenü für den Knoten von Kaspersky Anti-Virus und wählen Sie den Befehl **Einstellungen exportieren**.
   - Um die Parameter einer einzelnen funktionalen Komponente zu exportieren, öffnen Sie in der Konsolenstruktur das Kontextmenü durch Rechtsklick auf den Knoten der entsprechenden Komponenten und wählen Sie den Befehl **Einstellungen exportieren**.
   - Um Einstellungen der Komponente Vertrauenswürdige Zone zu exportieren:
     a. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten Kaspersky Anti-Virus und wählen Sie den Punkt **Einstellungen für vertrauenswürdige Zone anpassen**.

        Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

     b. Klicken Sie auf die Schaltfläche **Export**.

   Darauf öffnet sich das Begrüßungsfenster des Assistenten für den Parameter-Export.
3. Folgen Sie den Anweisungen in den Fenstern des Assistenten: Geben Sie einen Namen und einen Pfad für die Konfigurationsdatei an, in der die Parameter gespeichert werden sollen.

   Wenn Sie den Pfad angeben, können Sie Umgebungsvariablen des Systems verwenden. Benutzerdefinierte Umgebungsvariablen können jedoch nicht verwendet werden.

   > Wenn zum Zeitpunkt des Exports von Parametern eine Richtlinie des Programms Kaspersky Security Center gültig ist, exportiert Kaspersky Anti-Virus die Werte der Einstellungen aus der Richtlinie.

4. Klicken Sie im Fenster **Export der Programmeinstellungen abgeschlossen** auf die Schaltfläche **OK**, um den Assistenten für den Parameter-Export zu schließen.

EINSTELLUNGEN IMPORTIEREN

Um Parameter aus einer Konfigurationsdatei zu importieren, gehen Sie wie folgt vor:

1. Führen Sie eine der Aktionen durch:
   - Um alle Parameter für Kaspersky Anti-Virus zu importieren, öffnen Sie in der Konsolenstruktur das Kontextmenü für den Knoten von Kaspersky Anti-Virus und wählen Sie den Befehl **Einstellungen importieren**.
   - Um die Parameter einer einzelnen funktionalen Komponente zu importieren, öffnen Sie in der Konsolenstruktur das Kontextmenü durch Rechtsklick auf den Knoten der entsprechenden Komponenten und wählen Sie den Befehl **Einstellungen importieren**;

- Um Einstellungen der Komponente Vertrauenswürdige Zone zu importieren:

  a. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus das Kontextmenü für den Knoten Kaspersky Anti-Virus und wählen Sie den Punkt **Einstellungen für vertrauenswürdige Zone anpassen**.

     Das Fenster **Vertrauenswürdige Zone** wird geöffnet.

  b. Klicken Sie auf die Schaltfläche **Import**.

Darauf öffnet sich das Begrüßungsfenster des Assistenten für den Parameter-Import.

2. Folgen Sie den Anweisungen in den Fenstern des Assistenten: Geben Sie die Konfigurationsdatei an, aus der die Parameter importiert werden sollen.

Nachdem Sie allgemeine Einstellungen für Kaspersky Anti-Virus oder Einstellungen für funktionale Kaspersky Anti-Virus-Komponenten auf dem Server importiert haben, können die vorherigen Werten nicht wiederhergestellt werden.

3. Klicken Sie im Fenster **Import der Programmeinstellungen abgeschlossen** auf die Schaltfläche **OK**, um den Assistenten für den Import von Einstellungen zu schließen.
4. Klicken Sie in der Werkzeugleiste der Konsole von Kaspersky Anti-Virus auf die Schaltfläche **Aktualisieren**, um die importierten Parameter anzuzeigen.

Kaspersky Anti-Virus importiert keine Kennwörter (Daten von Benutzerkonten für den Aufgabenstart oder für die Proxyserver-Verbindung) aus einer Datei, die auf einem anderen Computer angelegt wurde oder auf dem gleichen Computer gespeichert wurde, nachdem Kaspersky Anti-Virus auf diesem neu installiert oder aktualisiert wurde. Die Kennwörter müssen nach dem Abschluss des Imports manuell angegeben werden.

VERWALTUNG VON KASPERSKY ANTI-VIRUS AUS DER BEFEHLSZEILE

Dieser Abschnitt enthält Informationen und Anweisungen über die Verwaltung von Kaspersky Anti-Virus über die Befehlszeile.

IN DIESEM ABSCHNITT

BEFEHLE ZUR VERWALTUNG VON KASPERSKY ANTI-VIRUS AUS DER BEFEHLSZEILE

Sie können die Basisbefehle zur Verwaltung von Kaspersky Anti-Virus aus der Befehlszeile des geschützten Servers erteilen, wenn Sie bei der Installation von Kaspersky Anti-Virus den Punkt **Befehlszeilen-Tool** zur Installation ausgewählt haben.

Mit Hilfe der Befehlszeile können Sie nur Funktionen, für die Sie in Kaspersky Anti-Virus zugriffsberechtigt sind, steuern.

Bestimmte Befehle von Kaspersky Anti-Virus werden synchron ausgeführt: Die Kontrolle kehrt erst zur Konsole zurück, nachdem ein Befehl ausgeführt wurde. Andere Befehle erfolgen asynchron: Die Kontrolle kehrt sofort nach dem Befehlsstart auf die Konsole zurück.

- *Um die Ausführung eines synchronen Befehls zu unterbrechen,*

  drücken Sie die Tasten <**Strg**+**C**>.

Beachten Sie bei der Eingabe von Befehlen für Kaspersky Anti-Virus folgende Regeln:

- 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"

Mit Hilfe der Befehlszeile können Sie das gesamte Spektrum an Operationen zur Steuerung und Administration von Kaspersky Anti-Virus ausführen (s. Tabelle unten).

Tabelle 25. Befehle für Kaspersky Anti-Virus

BEFEHL	BESCHREIBUNG
KAVSHELL HELP (s. S. 113)	Öffnet die Hilfe zu den Befehlen für Kaspersky Anti-Virus.
KAVSHELL START (s. S. 113)	Starten des Dienstes von Kaspersky Anti-Virus..
KAVSHELL STOP (s. S. 113)	Beendet den Dienst von Kaspersky Anti-Virus..
KAVSHELL SCAN (s. S. 114)	Erstellt und startet eine temporäre Untersuchungsaufgabe mit einem Untersuchungsbereich und Sicherheitseinstellungen, die durch Befehlsschlüssel vorgegeben werden.
KAVSHELL SCANCRITICAL (s. S. 117)	Startet die Systemaufgabe **Untersuchung kritischer Bereiche**.
KAVSHELL TASK (s. S. 118)	Startet / Hält an / Setzt fort / Beendet die angegebene Aufgabe im asynchronen Modus. / Gibt den aktuellen Aufgabenstatus / eine Statistik für die Aufgabe zurück.

BEFEHL	BESCHREIBUNG
KAVSHELL RTP (s. S. 119)	Startet oder beendet alle Echtzeitschutz-Aufgaben.
KAVSHELL UPDATE (s. S. 119)	Startet die Update-Aufgabe für die Datenbanken von Kaspersky Anti-Virus mit den festgelegten Befehlszeilen-Parametern.
KAVSHELL ROLLBACK (s. S. 122)	Kehrt zur vorherigen Version der Datenbanken zurück.
KAVSHELL LICENSE (s. S. 122)	Schlüssel verwalten.
KAVSHELL TRACE (s. S. 123)	Aktiviert oder deaktiviert das Führen des Ablaufverfolgungsprotokoll, Verwalten der Parameter für das Ablaufverfolgungsprotokoll.
KAVSHELL DUMP (s. S. 124)	Aktiviert oder deaktiviert die Dump-Erstellung für Kaspersky Anti-Virus-Prozesse bei einem Absturz von Prozessen.
KAVSHELL IMPORT (s. S. 125)	Importiert aus einer zuvor erstellten Konfigurationsdatei die allgemeinen Einstellungen für Kaspersky Anti-Virus, sowie Einstellungen für seine Funktionen und Aufgaben.
KAVSHELL EXPORT (s. S. 125)	Exportiert alle Parameter von Kaspersky Anti-Virus und aller vorhandenen Aufgaben in eine Konfigurationsdatei.

HILFE ZU DEN BEFEHLEN FÜR KASPERSKY ANTI-VIRUS ÖFFNEN. KAVSHELL HELP

Um eine Liste aller -Befehle für Kaspersky Anti-Virus zu öffnen, geben Sie einen der folgenden Befehle ein:

```
KAVSHELL
KAVSHELL HELP
KAVSHELL /?
```

Um die Beschreibung und Syntax eines Befehls zu erhalten, geben Sie einen der folgenden Befehle ein:

```
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
```

DIENST VON KASPERSKY ANTI-VIRUS STARTEN UND ANHALTEN KAVSHELL START, KAVSHELL STOP

Um den Dienst von Kaspersky Anti-Virus zu beenden, verwenden Sie den Befehl `KAVSHELL START`.

Wenn Kaspersky Anti-Virus gestartet wird, werden standardmäßig folgende Aufgaben gestartet: **Echtzeitschutz für Dateien**, **Skript-Untersuchung** und **Untersuchung beim Hochfahren des Computers**, sowie andere Aufgaben, für deren Zeitplan das Startintervall **Bei Programmstart** gilt.

Um den Dienst von Kaspersky Anti-Virus zu beenden, verwenden Sie den Befehl `KAVSHELL STOP`.

Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP (auf S. 126)

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 geben die Aufgabenparameter vor (Untersuchungsbereich und Sicherheitseinstellungen).

Eine Untersuchungsaufgabe, die mit dem Befehl `KAVSHELL SCAN` gestartet wurde, ist temporär. Sie wird nur während ihrer Ausführung in der Konsole von Kaspersky Anti-Virus angezeigt (Die Aufgabenparameter können nicht in der Konsole von Kaspersky Anti-Virus angezeigt werden). Gleichzeitig wird ein Bericht über die Aufgabenausführung geführt, der im Knoten **Berichte über Aufgabenausführung** der Konsole von Kaspersky Anti-Virus angezeigt wird. Für Untersuchungsaufgaben, die in der Konsole von Kaspersky Anti-Virus erstellt wurden, und für Aufgaben, die mit Hilfe des Befehls SCAN angelegt wurden, können Richtlinien der Anwendung Kaspersky Security Center übernommen werden. Informationen darüber, wie Anti-Virus mit Hilfe von Kaspersky Security Center verwaltet wird, finden Sie im Abschnitt "Verwaltung von Anti-Virus aus Kaspersky Security Center" (s. S. 132).

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 vorhandene Aufgabe zur Virensuche aus der Befehlszeile zu starten, verwenden Sie den Befehl KAVSHELL TASK (s. S. 118).

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
Aufgabenausführungsprotokoll>] [/ANSI] [/ALIAS:<Alias des Aufgabenamens>] [/ANSI]
```

Der Befehl KAVSHELL SCAN enthält sowohl obligatorische als auch zusätzliche Schlüssel, 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:report.log
```

Tabelle 26. Syntax des Befehls `KAVSHELL SCAN` und Bestimmung seiner Schlüssel

SCHLÜSSEL	BESCHREIBUNG
Untersuchungsbereich. Obligatorischer Schlüssel.	
<Dateien>	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 untersuchen möchten, ein Leerzeichen enthält, muss dieser Name in Klammern stehen. Wenn Sie einen Ordner ausgewählt haben, wird Kaspersky Anti-Virus auch alle eingebetteten Unterordner für diesen Ordner untersuchen. Um eine Gruppe der Datei zu untersuchen, können Sie die Zeichen * und ? verwenden.
<Ordner>	
<Netzwerkpfad>	
/MEMORY	Objekte im Arbeitsspeicher untersuchen.
/SHARED	Gemeinsame Ordner auf dem Server untersuchen.

SCHLÜSSEL	BESCHREIBUNG
/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 Anti-Virus die Objekte nach Format.	
/FA	Alle Objekte untersuchen.
/FC	Objekte, die nach Format untersucht werden (Standard). Kaspersky Anti-Virus untersucht nur Objekte, die dem Format nach als infizierbar gelten.
/FE	Objekte nach Erweiterung untersuchen. Kaspersky Anti-Virus untersucht nur Objekte, die der Erweiterung nach als infizierbar gelten.
/NEWONLY	Nur neue und veränderte Dateien untersuchen. Wenn Sie diesen Schlüssel nicht angeben, untersucht Kaspersky Anti-Virus alle Objekte.
/AI: **Aktionen für infizierte Objekte**. Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Anti-Virus die Aktion **Überspringen** aus.	
DISINFECT	Desinfizieren, irreparable Objekte überspringen
DISINFDEL	Desinfizieren. Irreparable Objekte löschen
DELETE	Löschen Die Parameter DISINFECT und DELETE wurden in der aktuellen Version von Kaspersky Anti-Virus beibehalten, um die Kompatibilität mit den vorherigen Versionen zu gewährleisten. Sie können diese Einstellungen anstelle der Befehlsparameter /AI: und /AS: verwenden. In diesem Fall wird Kaspersky Anti-Virus möglicherweise infizierte Objekte nicht bearbeiten.
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
/AS: **Aktionen für möglicherweise infizierte Objekte** (**actions**). Wenn Sie keine Werte für diesen Schlüssel angeben, führt Kaspersky Anti-Virus die Aktion **Überspringen** aus.	
QUARANTINE	In Quarantäne verschieben
DELETE	Löschen
REPORT	Bericht senden (Standard)
AUTO	Empfohlene Aktion ausführen
Ausnahmen (Exclusions)	

SCHLÜSSEL	BESCHREIBUNG
/E:ABMSPO	Dieser Schlüssel schließt zusammengesetzte Objekte der folgenden Typen aus: A – SFX-Archive; B – 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. In der Grundeinstellung untersucht Kaspersky Anti-Virus Objekte jeder Größe.
/TZOFF	Ausnahmen der vertrauenswürdigen Zone verschieben.
/AI: **Aktionen für autonome Dateien** (HSM options)	
/SKIP	Autonome Dateien überspringen.
/RESIDENT	Nur den residenten Teil der Datei untersuchen.
/SCAN	Alle autonomen Dateien untersuchen.
/SCAN=<Tage>	Nur die autonomen Dateien untersuchen, auf die Kaspersky Anti-Virus innerhalb des angegebenen Zeitraums zugegriffen hat.
/SCAN NORECALL	Autonomen Dateien untersuchen, ohne Sie möglichst auf dem Laufwerk zu kopieren.
/SCAN=<Tage>	Nur die autonomen Dateien untersuchen, auf die Kaspersky Anti-Virus innerhalb des angegebenen Zeitraums zugegriffen hat, ohne Sie möglichst auf dem Laufwerk zu kopieren.
Erweiterte Einstellungen (Options)	
/NOICHECKER	iChecker-Technologie deaktivieren (standardmäßig aktiviert).
/NOISWIFT	iSwift-Technologie deaktivieren (standardmäßig aktiviert).
/ANALYZERLEVEL:<Analysestufe>	Verwendung der heuristische 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 Anti-Virus die heuristische Analyse nicht.
/NOCHECKMSSIGN	Dateien, die über eine elektronische Unterschrift des Unternehmens Microsoft verfügen, nicht untersuchen (standardmäßig aktiviert).
/ALIAS:<Alias des Aufgabenamens>	Dieser Schlüssel weist einer Untersuchungsaufgabe 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 funktionellen Komponenten von Kaspersky Anti-Virus einmalig sein. Wenn dieser Schlüssel nicht vorgegeben ist, erhält die Aufgabe den alternativen Name scan_<kavshell_pid> (z.B. scan_1234). In der Konsole von Kaspersky Anti-Virus erhält die Aufgabe den Namen Scan objects (<Datum und Uhrzeit>) (z.B. Scan objects 8/16/2007 05:13:14 PM).

SCHLÜSSEL	BESCHREIBUNG
Parameter der Berichte über Aufgabenausführung (Report settings)	
/W:<Dateiname für Bericht zur Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Anti-Virus eine Datei mit dem Aufgabenausführungsbericht. Die Datei erhält den durch diesen Schlüssel vorgegebenen Namen. Die Berichtsdatei 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 Kaspersky Anti-Virus-Ereignisbericht in der Konsole "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Berichtsdatei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Protokolldatei überschrieben. Sie können die Protokolldatei während der Aufgabenausführung anzeigen. Das Bericht wird im Knoten **Berichte über Aufgabenausführung** der Konsole von Kaspersky Anti-Virus angezeigt. Wenn Kaspersky Anti-Virus keine Berichtdatei anlegen kann, wird die Befehlsausführung nicht abgebrochen, es erfolgt aber eine Fehlermeldung.
/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.

Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL (auf S. 127)

AUFGABE "UNTERSUCHUNG KRITISCHER BEREICHE" STARTEN. KAVSHELL SCANCRITICAL

Verwenden Sie den Befehl `KAVSHELL SCANCRITICAL`, um die System-Untersuchungsaufgabe **Untersuchung kritischer Bereiche** mit den Parametern zu starten, die in der Konsole von Kaspersky Anti-Virus festgelegt wurden.

Syntax des Befehls KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<Dateiname für Bericht über Aufgabenausführung>]
```

Beispiele für den Befehl KAVSHELL SCANCRITICAL

Um die Aufgabe zur Untersuchung auf Befehl **Untersuchung kritischer Bereiche** auszuführen und den Bericht über die 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 die Aufgabenausführung je nach Syntax des Schlüssels /W einstellen (s. Tabelle unten).

Syntax des Schlüssels `/W` des Befehls `KAVSHELL SCANCRITICAL`

SCHLÜSSEL	BESCHREIBUNG
/W:<Dateiname für Bericht zur Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Anti-Virus eine Datei mit dem Aufgabenausführungsbericht. Die Datei erhält den durch diesen Schlüssel vorgegebenen Namen. Die Berichtsdatei 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 Anti-Virus-Ereignisbericht in der Konsole "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Berichtsdatei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Protokolldatei überschrieben. Sie können die Protokolldatei während der Aufgabenausführung anzeigen. Das Bericht wird im Knoten **Berichte über Aufgabenausführung** der Konsole von Kaspersky Anti-Virus angezeigt. Wenn Kaspersky Anti-Virus keine Berichtdatei anlegen kann, wird die Befehlsausführung nicht abgebrochen, es erfolgt aber eine Fehlermeldung.

Rückgabecodes für die Befehle KAVSHELL SCAN und KAVSHELL SCANCRITICAL (auf S. 127)

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.

Mit diesem Befehl können Sie Gruppenaufgaben von Kaspersky Security Center nicht verwalten.

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 27. Syntax des Befehls KAVSHELL TASK

SCHLÜSSEL	BESCHREIBUNG
Ohne Schlüssel	Der Befehl gibt eine Liste aller vorhandenen Aufgaben von Kaspersky Anti-Virus 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 Anti-Virus an Aufgaben vergibt. Um die alternativen Namen der Aufgaben von Kaspersky Anti-Virus anzuzeigen, führen Sie den Befehl KAVSHELL TASK ohne einen Schlüssel aus.
/START	Die angegebenen Aufgabe im asynchronen Modus starten.
/STOP	Beenden einer angegebenen Aufgabe.
/PAUSE	Anhalten einer angegebenen Aufgabe.

SCHLÜSSEL	BESCHREIBUNG
/RESUME	Asynchrones Fortsetzen einer angegebenen Aufgabe.
/STATE	Den aktuellen Aufgabenstatus ermitteln (zum Beispiel, **Wird ausgeführt**, **Abgeschlossen**, **Angehalten**, **Beendet**, **Fehlerhaft abgeschlossen**, **Wird gestartet**, **Wird fortgesetzt**)
/STATISTICS	Aufgabenstatistik abfragen – Informationen über die Anzahl der Objekte, die seit dem Aufgabenstart bis zum jetzigen Zeitpunkt verarbeitet wurden.

Rückgabecode für den Befehl KAVSHELL TASK (auf S. 127)

ECHTZEITSCHUTZ-AUFGABEN STARTEN UND BEENDEN. KAVSHELL RTP

Mit dem Befehl `KAVSHELL RTP` können Sie alle Aufgaben des Echtzeitschutzes starten oder beenden.

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).

Schlüssel des Befehls KAVSHELL RTP

SCHLÜSSEL	BESCHREIBUNG
/START	Starten aller Echtzeitschutz-Aufgaben
/STOP	Beenden aller Echtzeitschutz-Aufgaben

Rückgabecode für den Befehl KAVSHELL RTP (auf S. 128)

AUFGABE ZUM UPDATE DER DATENBANKEN VON KASPERSKY ANTI-VIRUS STARTEN. KAVSHELL UPDATE

Mit dem Befehl `KAVSHELL UPDATE` können Sie die Aufgabe zum Update der Datenbanken von Kaspersky Anti-Virus im Synchronmodus starten.

Eine Aufgabe zum Update der Datenbanken von Kaspersky Anti-Virus, die mit dem Befehl `KAVSHELL UPDATE` gestartet wird, ist temporär. Sie wird nur während ihrer Ausführung in der Konsole von Kaspersky Anti-Virus angezeigt. Gleichzeitig wird ein Bericht über die Aufgabenausführung geführt, der im Knoten **Berichte über Aufgabenausführung** der Anti-Virus-Konsole angezeigt wird. Für Update-Aufgaben, die mit dem Befehl `KAVSHELL UPDATE` erstellt und gestartet wurden, sowie für Update-Aufgaben, die in der Anti-Virus-Konsole angelegt wurden, können Richtlinien der Anwendung Kaspersky Security Center übernommen werden. Informationen darüber, wie Anti-Virus auf Servern mit Hilfe der Anwendung Kaspersky Security Center verwaltet wird, finden Sie im Abschnitt "Verwaltung von Anti-Virus aus Kaspersky Security Center" (s. S. 132).

Wenn Sie in dieser Aufgabe den Pfad eine Update-Quelle angeben, können Sie Umgebungsvariable verwenden. Wenn Sie einer 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:<Dateiname für Aufgabenausführungsprotokoll>] [/ALIAS:<Alias
des Aufgabennamens>]
```

Der Befehl KAVSHELL UPDATE enthält sowohl obligatorische als auch zusätzliche Schlüssel, deren Verwendung optional ist (s. Tabelle unten).

Beispiele für den Befehl KAVSHELL UPDATE

Um eine benutzerdefinierte Aufgabe zum Datenbankupdate zu starten, führen Sie folgenden Befehl aus:

```
KAVSHELL UPDATE
```

Um eine Aufgabe zum Datenbankupdate zu starten, dessen Update-Dateien 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 Berichtsdatei 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 Updates der Datenbanken von Kaspersky Anti-Virus vom Kaspersky-Lab-Update-Server 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 28. Schlüssel des Befehls KAVSHELL UPDATE

SCHLÜSSEL	BESCHREIBUNG
Update-Quellen (obligatorischer Schlüssel). Geben Sie eine oder mehrere Quellen an. Kaspersky Anti-Virus greift der angegebenen Reihenfolge nach auf die Update-Quellen zu. Trennen Sie die Quellen durch Leerzeichen.	
<Pfad im Format UNC>	Benutzerdefinierte Update-Quelle – Pfad eines Netzwerkordners mit Updates im UNC-Format (Universal Naming Convention).
<URL>	Benutzerdefinierte Update-Quelle – Adresse eine HTTP- oder FTP-Servers, auf dem sich der Update-Ordner befindet
<Lokaler Ordner>	Benutzerdefinierte Update-Quelle – Ordner auf dem geschützten Server
/AK	Administrationsserver von Kaspersky Security Center als Update-Quelle
/KL	Update-Server von Kaspersky Lab als Update-Quelle
/NOUSEKL	Die Update-Server von Kaspersky Lab nicht verwenden, wenn die anderen angegebenen Update-Quellen nicht verfügbar sind (Quellen, die standardmäßig verwendet werden).
Parameter des Proxyservers	
/PROXY:<Adresse>:<Port>	Netzwerkname oder IP-Adresse des Proxyservers und dessen Port. Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Anti-Virus automatisch die Parameter des Proxyservers, 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 Anti-Virus greift unter dem Benutzerkonto **Lokales System** (**SYSTEM**) auf den Proxyserver zu; **1** – integrierte Microsoft Windows-Authentifizierung (NTLM-Authentifizierung). Kaspersky Anti-Virus greift unter dem Benutzerkonto, dessen Login-Daten durch die Schlüssel /PROXYUSER und /PROXYPWD angegeben werden, auf den Proxyserver zu; **2** – Authentifizierung mit Benutzername und Kennwort, die durch die Schlüssel /PROXYUSER und /PROXYPWD (Basic authentication) angegeben werden. Wenn für den Zugriff auf den Proxyserver keine Authentifizierung erforderlich ist, muss dieser Schlüssel nicht angeben werden.
/PROXYUSER:<Benutzername>	Benutzername, der 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.

SCHLÜSSEL	BESCHREIBUNG
/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-Parameter für die Verbindung zu den Updateservern von Kaspersky Lab nicht verwenden (Sie werden standardmäßig verwendet).
/USEPROXYFORCUSTOM	Proxyserver-Einstellungen für die Verbindung zu benutzerdefinierten Update-Quellen verwenden (Sie werden standardmäßig nicht verwendet).
/USEPROXYFORLOCAL	Proxyserver-Einstellungen für die Verbindung zu lokalen Update-Quellen verwenden. Wenn kein Wert angegeben wurde, wird der Wert **Proxyserver-Einstellungen für die Verbindung zu benutzerdefinierten Update-Quellen nicht verwenden** verwendet.
Allgemeine Parameter eines FTP- und HTTP-Servers	
/NOFTPPASSIVE	Wenn Sie diesen Schlüssel angeben, verwendet Kaspersky Anti-Virus den FTP-Server im aktiven Modus für eine Verbindung zum geschützten Server. Wenn Sie diesen Schlüssel nicht angeben, verwendet Kaspersky Anti-Virus nach Möglichkeit den passiven Modus des FTP-Servers.
/TIMEOUT:<Anzahl der Sekunden>	Wartezeit für Verbindung mit einem FTP- oder HTTP-Server. Wenn Sie diesen Parameter nicht angeben, verwendet Kaspersky Anti-Virus den Standardwert 10 Sekunden. Für diesen Parameter können nur ganze Zahlen verwendet werden.
/REG:<Code iso3166>	Der Schlüssel "Regionsoptionen" wird beim Update-Download von den Kaspersky-Lab-Updateservern verwendet. Kaspersky Anti-Virus optimiert den Update-Download auf den geschützten Server, indem er den geografisch am nächsten liegenden Update-Server auswählt. 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 Sie diesen Schlüssel auslassen oder einen unbekannten Ländercode angeben, ermittelt Kaspersky Anti-Virus den Standort des geschützten Servers aus den Regionsoptionen des geschützten Servers (Für Microsoft Windows 2003 Server und höher handelt es sich dabei um den Wert der Variable **Ort** (Location)).
/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 funktionellen Komponenten von Kaspersky Anti-Virus einmalig sein. Wenn dieser Schlüssel nicht angegeben wird, erhält die Aufgabe den Alias update_<kavshell_pid> (z.B. update_1234) In der Konsole von Kaspersky Anti-Virus erhält die Aufgabe den Namen Update-bases (<date time>) (z.B. Update-bases 8/16/2007 5:41:02 PM).
/W:<Dateiname für Bericht zur Aufgabenausführung>	Wenn Sie diesen Schlüssel angeben, speichert Kaspersky Anti-Virus eine Datei mit dem Aufgabenausführungsbericht. Die Datei erhält den durch diesen Schlüssel vorgegebenen Namen. Die Berichtsdatei 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 Kaspersky Anti-Virus-Ereignisbericht in der Konsole "Ereignisanzeige" festgelegt wurden. Sie können einen absoluten oder einen relativen Pfad für die Berichtsdatei angeben. Wenn Sie nur einen Dateinamen, aber keinen Pfad angeben, wird die Berichtsdatei im aktuellen Ordner angelegt. Wenn der Befehl wiederholt mit den gleichen Parametern ausgeführt wird, werden die Einträge der vorhandenen Protokolldatei überschrieben. Sie können die Protokolldatei während der Aufgabenausführung anzeigen. Das Bericht wird im Knoten **Berichte über Aufgabenausführung** der Konsole von Kaspersky Anti-Virus angezeigt. Wenn Kaspersky Anti-Virus keine Berichtsdatei anlegen kann, unterbricht er die Befehlsausführung nicht und gibt keine Fehlermeldung aus.

Rückgabecode für den Befehl KAVSHELL UPDATE (s. Pkt. “Rückgabecode für den Befehl RTP" auf S. 128)

ROLLBACK DES UPDATES FÜR DIE DATENBANKEN VON KASPERSKY ANTI-VIRUS. KAVSHELL ROLLBACK

`Mit dem Befehl` KAVSHELL ROLLBACK können Sie die Systemaufgabe **Rollback des Datenbank-Updates** ausführen. Dadurch werden die Datenbanken von Kaspersky Anti-Virus mit den zuvor installierten Updates wiederhergestellt. Der Befehl wird synchron ausgeführt.

Syntax des Befehls

```
KAVSHELL ROLLBACK
```

Rückgabecode für den Befehl KAVSHELL ROLLBACK (auf S. 129)

SCHLÜSSEL HINZUFÜGEN UND ENTFERNEN. KAVSHELL LICENSE

Mit dem Befehl `KAVSHELL LICENSE` können Sie in Kaspersky Anti-Virus Schlüssel hinzufügen und löschen.

Syntax des Befehls KAVSHELL LICENSE

```
KAVSHELL LICENSE [/ADD:<Name der Schlüsseldatei> [/R] | /DEL:<Schlüsselnummer>]
```

Beispiele für den Befehl KAVSHELL LICENSE

Um einen Schlüssel aus einer Schlüsseldatei hinzuzufügen, führen Sie folgenden Befehl aus:

```
KAVSHELL LICENSE /ADD:C:/License.key
```

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 löschen, 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 29. 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 Test) • 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:<Pfad der Schlüsseldatei>	Fügt mithilfe der angegebenen Datei einen Schlüssel hinzu. Wenn Sie den Pfad einer Schlüsseldatei angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariable sind dagegen nicht zugelassen.
/R	Der Parameter /R ist ein zusätzlicher Parameter für den Schlüssel /ADD und gibt an, dass der Schlüssel als Reserveschlüssel hinzugefügt wird.
/DEL:<Schlüsselnummer>	Lösche den Schlüssel mit der angegebenen Nummer.

Rückgabecode für den Befehl KAVSHELL LICENSE (auf S. 129)

ERSTELLEN EINES ABLAUFVERFOLGUNGSPROTOKOLLS AKTIVIEREN, ANPASSEN UND DEAKTIVIEREN. KAVSHELL TRACE

Mit dem Befehl `KAVSHELL TRACE` können Sie das Anlegen eines Ablaufverfolgungsberichts für alle Subsysteme von Kaspersky Anti-Virus aktivieren oder deaktivieren, und die entsprechende Genauigkeitsstufe festlegen.

Informationen in Speicherdump- und Protokolldateien werden von Kaspersky Anti-Virus im Klartext aufgezeichnet.

Syntax des Befehls KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<Ordner mit Dateien des Ablaufverfolgungsprotokolls> [/S:<maximale Größe einer Protokolldatei in MB>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

Wenn ein Ablaufverfolgungsbericht 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 30. Schlüssel des Befehls KAVSHELL TRACE

SCHLÜSSEL	BESCHREIBUNG
/ON	Führen eines Ablaufverfolgungsberichts aktivieren
/F:<Ordner für Dateien des Ablaufverfolgungsprotokolls>	Dieser Schlüssel gibt den vollständigen Pfad des Ordners an, in dem die Dateien des Ablaufverfolgungsprotokolls gespeichert werden (obligatorischer Schlüssel). Wenn Sie den Pfad eines nicht vorhandenen Ordners angeben, wird kein Ablaufverfolgungsbericht 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 Dateien des Ablaufverfolgungsberichts angeben, können Sie Umgebungsvariable des Systems verwenden. Benutzerdefinierte Umgebungsvariablen sind dagegen nicht zulässig.
/S:<maximale Größe einer Berichtsdatei in MB>	Dieser Schlüssel bestimmt die maximale Größe einer Datei des Ablaufverfolgungsberichts. Sobald eine Berichtsdatei den Grenzwert erreicht, beginnt Kaspersky Anti-Virus, 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 Berichtsdatei 50 MB.
/LVL:debug|info|warning|error|critical	Dieser Schlüssel legt die Genauigkeitsstufe des Berichts fest. Auf der maximalen Stufe (**Debug-Informationen**) werden alle Ereignisse protokolliert, auf der minimalen Stufe (**Kritische Ereignisse**) nur kritische Ereignisse. Wenn Sie diesen Schlüssel nicht angeben, werden Ereignisse mit der Genauigkeitsstufe **Debug-Informationen** im Ablaufverfolgungsbericht aufgezeichnet.
/OFF	Dieser Schlüssel deaktiviert das Führen des Ablaufverfolgungsprotokolls.

Beispiele für den Befehl KAVSHELL TRACE

Um das Anlegen eines Ablaufverfolgungsberichts mit der Genauigkeitsstufe Debug-Informationen und einer maximalen Dateigröße von 200 MB zu aktiveren und die Berichtsdatei 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 Ablaufverfolgungsberichts mit der Genauigkeitsstufe Wichtige Ereignisse zu aktiveren und die Berichtsdatei im Ordner C:\Trace Folder zu speichern, führen Sie folgenden Befehl aus:

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

Um die Erstellung eine Ablaufverfolgungsberichts zu aktivieren, führen Sie folgenden Befehl aus:

```
KAVSHELL TRACE /OFF
```

Rückgabecode für den Befehl KAVSHELL TRACE (auf S. 129)

iSWIFT-DATENBANK LEEREN. KAVSHELL FBRESET

Kaspersky Anti-Virus verwendet die Technologie iSwift, um eine erneute Untersuchung einer Datei zu vermeiden, wenn die Datei seit der vorherigen Untersuchung nicht verändert wurde (**iSwift-Technologie verwenden**).

Kaspersky Anti-Virus erstellt im Systemverzeichnis %SYSTEMDRIVE%\System Volume Information die Dateien fidbox.dat und fidbox2.dat, die Informationen über bereits untersuchte, virenfreie Objekte enthalten. Je größer die Anzahl der Dateien, die von Kaspersky Anti-Virus untersucht worden sind, desto größer ist die Datei fidbox.dat (fidbox2.dat). Diese Datei enthält nur aktuelle Informationen über die tatsächlich im System vorhandenen Dateien: Wenn eine Datei im System gelöscht wird, löscht Kaspersky Anti-Virus die entsprechenden Informationen aus der Datei fidbox.dat (fidbox2.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 Anti-Virus 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 Anti-Virus verursachte Belastung des Servers erhöhen. Dabei untersucht das Antiviren-Programm alle Dateien, auf die nach dem Leeren der Datei fidbox.dat zum ersten Mal zugegriffen wird. Nach der Untersuchung trägt Kaspersky Anti-Virus 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.

Wenn Ihr Betriebssystem die Funktion Benutzerkontensteuerung (UAC, User Account Control) verwendet, so muss bei Ausführung des Befehls `KAVSHELL FBRESET` **die Befehlszeile mit Administratorrechten gestartet werden**.

ANLEGEN VON DUMP-DATEIEN EIN- UND AUSSCHALTEN. KAVSHELL DUMP

Mit dem Befehl `KAVSHELL DUMP` können Sie das Erstellen von Speicherauszügen (Dumps), die bei Abstürzen für die Prozesse von Kaspersky Anti-Virus erstellt werden, aktivieren oder deaktivieren (s. Tabelle unten). Außerdem können Sie jederzeit Speicher-Images der von Kaspersky Anti-Virus ausgeführten Prozesse anfertigen.

Syntax des Befehls KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<Ordner für Dump-Dateien>|/SNAPSHOT /F:<Ordner für Dump-Dateien> /
P:<pid> | /OFF>
```

Beispiele für den Befehl KAVSHELL DUMP

Um die Erstellung von Speicherauszügen zu aktivieren und die erstellten Dump-Dateien im Ordner C:\Dump Folder zu speichern, führen Sie folgenden Befehl aus:

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

Um einen Speicherauszug 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 von Speicherauszügen zu aktivieren, führen Sie folgenden Befehl aus:

```
KAVSHELL DUMP /OFF
```

Tabelle 31. Schlüssel des Befehls KAVSHELL DUMP

SCHLÜSSEL	BESCHREIBUNG
/ON	Erstellung von Speicher-Dump für einen Prozess für den Fall eines Absturzes aktivieren.
/F:<Pfad der Dump-Dateien>	Obligatorischer Schlüssel, der den Pfad des Ordners angibt, 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	Speicher-Image eines bestimmten laufenden Prozesses von Kaspersky Anti-Virus anfertigen und in einer Dump-Datei im Ordner, dessen Pfad durch den Schlüssel /F definiert wird, speichern.
/P	Prozess-PID, die im **Task-Manager** von Microsoft Windows angezeigt wird.
/OFF	Deaktivieren der Dump-Erstellung für Prozesse bei einem Absturz.

Rückgabecode für den Befehl KAVSHELL DUMP (auf S. 130)

PARAMETER IMPORTIEREN. KAVSHELL IMPORT

Mit dem Befehl `KAVSHELL IMPORT` können Sie Einstellungen, Funktionen und Aufgaben von Kaspersky Anti-Virus aus einer Konfigurationsdatei in Kaspersky Anti-Virus auf den geschützten Server importieren. Mit dem Befehl `KAVSHELL EXPORT` können Sie eine Konfigurationsdatei erstellen.

Syntax des Befehls KAVSHELL IMPORT

```
KAVSHELL IMPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiele für den Befehl KAVSHELL IMPORT

```
KAVSHELL IMPORT Server1.xml
```

Tabelle 32. 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 (s. S. 130)

PARAMETER EXPORTIEREN. KAVSHELL EXPORT

Mit dem Befehl `KAVSHELL EXPORT` können Sie alle Einstellungen von Kaspersky Anti-Virus und die vorhandenen Aufgaben in eine Konfigurationsdatei exportieren, um sie auf anderen Servern in Kaspersky Anti-Virus zu importieren.

Syntax des Befehls KAVSHELL EXPORT

```
KAVSHELL EXPORT <Name und Pfad der Konfigurationsdatei>
```

Beispiele für den Befehl KAVSHELL EXPORT

```
KAVSHELL EXPORT Server1.xml
```

Tabelle 33. 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.

Rückgabecode für den Befehl KAVSHELL EXPORT (auf S. 131)

RÜCKGABECODES

IN DIESEM ABSCHNITT

RÜCKGABECODES FÜR DIE BEFEHLE KAVSHELL START UND KAVSHELL STOP

Tabelle 34. Rückgabecodes für die Befehle KAVSHELL START und KAVSHELL STOP

BESCHREIBUNG	
0	Operation wurde erfolgreich ausgeführt.
-3	Zugriffsfehler
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (zum Beispiel ist der Anti-Virus-Service bereits gestartet oder schon beendet)
-7	Service ist nicht registriert
-8	Service-Start ist unterbunden
-9	Versuch zum Starten des Diensts unter einem anderen Benutzerkonto war erfolglos (In der Grundeinstellung arbeitet der Anti-Virus-Dienst unter dem Benutzerkonto **Lokales System**).
-99	Unbekannter Fehler

RÜCKGABECODES FÜR DIE BEFEHLE KAVSHELL SCAN UND KAVSHELL SCANCRITICAL

Tabelle 35. 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	Es wurden infizierte Objekte gefunden
-81	Es wurden möglicherweise infizierte Objekte gefunden
-82	Es wurden Verarbeitungsfehler erkannt
-83	Es wurden nicht untersuchte Objekte gefunden
-84	Es wurden beschädigte Objekte gefunden
-85	Das Erstellen einer Datei für den Aufgabenausführungsbericht ist fehlgeschlagen.
-99	Unbekannter Fehler
-301	Ungültiger Schlüssel

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL TASK

Tabelle 36. Rückgabecode 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	Ausführungsfehler (Ändern des Aufgabenstatus führte zum Absturz)

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL RTP

Tabelle 37. Rückgabecode 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

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL UPDATE

Tabelle 38. Rückgabecode 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	Update-Dateien 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 Anti-Virus hat die Authentifizierungsprüfung beim Verbinden mit Update-Quelle nicht bestanden
-236	Die Anti-Virus-Datenbanken sind beschädigt.
-301	Ungültiger Schlüssel

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL ROLLBACK

Tabelle 39. Rückgabecode für den Befehl KAVSHELL ROLLBACK

FEEDBACK-CODE	BESCHREIBUNG
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-99	Unbekannter Fehler
-221	Sicherungskopie der Datenbanken nicht gefunden
-222	Sicherungskopie der Datenbanken ist beschädigt

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL LICENSE

Tabelle 40. Rückgabecode 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

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL TRACE

Tabelle 41. Rückgabecode 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 Dateien für den Ablaufverfolgungsbericht führt)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch, den Befehl KAVSHELL TRACE/OFF auszuführen, wenn Erstellen des Ablaufverfolgungsbericht schon deaktiviert ist)
-99	Unbekannter Fehler

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL FBRESET

Tabelle 42. Rückgabecode für den Befehl KAVSHELL FBRESET

FEEDBACK-CODE	BESCHREIBUNG
0	Operation wurde erfolgreich ausgeführt.
-99	Unbekannter Fehler

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL DUMP

Tabelle 43. Rückgabecode 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 den Auszugsdateien führt; keinen Prozess mit PID gefunden)
-5	Ungültige Befehlssyntax
-6	Ungültiger Vorgang (Versuch, den Befehl KAVSHELL DUMP /OFF auszuführen, wenn Erstellen der Speicherauszugsdateien deaktiviert ist)
-99	Unbekannter Fehler
-237	Inkompatible Update-Quellen wurden angegeben

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL IMPORT

Tabelle 44. Rückgabecode für den Befehl KAVSHELL IMPORT

FEEDBACK-CODE	BESCHREIBUNG
0	Operation wurde erfolgreich ausgeführt.
-2	Service nicht gestartet
-3	Zugriffsfehler
-4	Objekt nicht gefunden (zu importierende Konfigurationsdatei nicht gefunden)
-5	Ungültige Syntax
-99	Unbekannter Fehler
501	Der Vorgang wurde erfolgreich ausgeführt. Bei der Befehlsausführung ist jedoch ein Fehler / eine Meldung aufgetreten (z.B. Kaspersky Anti-Virus hat die Parameter einer bestimmten funktionellen Komponente nicht importiert).
-502	Zu importierende Datei ist nicht vorhanden oder hat ein unbekanntes Format
-503	Inkompatible Parameter (Konfigurationsdatei aus anderer Anwendung exportiert oder Kaspersky Anti-Virus mit höherer Version oder inkompatibler Version).

RÜCKGABECODE FÜR DEN BEFEHL KAVSHELL EXPORT

Tabelle 45. Rückgabecode 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 (z. B.; 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 / eine Meldung aufgetreten (z.B. Kaspersky Anti-Virus hat die Parameter einer bestimmten funktionellen Komponente nicht exportiert).

VERWALTUNG VON KASPERSKY ANTI-VIRUS AUS KASPERSKY SECURITY CENTER

Dieser Abschnitt enthält Informationen und Anweisungen über die Verwaltung von Kaspersky Anti-Virus und die Anpassung der Einstellungen von Kaspersky Anti-Virus mithilfe der Administrationskonsole von Kaspersky Security Center.

IN DIESEM ABSCHNITT

KASPERSKY ANTI-VIRUS IM FENSTER PROGRAMMEINSTELLUNGEN ANPASSEN

Im Fenster **Programmeinstellungen** können Sie Kaspersky Anti-Virus im Remote-Betrieb auf dem geschützten Server verwalten.

IN DIESEM ABSCHNITT

FENSTER PROGRAMMEINSTELLUNGEN ÖFFNEN

*Gehen Sie folgendermaßen vor, um das Fenster **Programmeinstellungen** zu öffnen:*

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Computer** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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**.
4. Verwenden Sie eine der folgenden Methoden, um im Fenster **Eigenschaften: <Computername>** im Abschnitt **Programme** das Fenster **Programmeinstellungen** zu öffnen:
   - 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 die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthalten ist, können diese Einstellungen nicht über das Fenster Programmeinstellungen geändert werden.

VERWALTUNG VON QUARANTÄNE-OBJEKTEN UND ANPASSEN DER QUARANTÄNE-EINSTELLUNGEN

Objekte, die von Kaspersky Anti-Virus als möglicherweise infiziert eingestuft worden sind, werden in die Quarantäne verschoben, d. h. die Objekte werden von ihrem ursprünglichen Speicherort in den *Quarantäne-Ordner* verschoben. Aus Sicherheitsgründen werden die Objekte im Quarantäne-Ordner in verschlüsselter Form gespeichert.

In diesem Abschnitt werden die Funktionen der Quarantäne und die Verwaltungswerkzeuge beschrieben, mit deren Hilfe diese Funktionen angepasst werden können. Darüber hinaus enthält der Abschnitt Anweisungen zur Anpassung der Quarantäne-Einstellungen über Kaspersky Security Center.

IN DIESEM ABSCHNITT

QUARANTÄNE-FUNKTIONEN UND EINSTELLUNGSWERKZEUGE

In folgender Tabelle sind Funktionen der Quarantäne und Administrationswerkzeuge aufgeführt. Mit den Werkzeugen können Sie die Funktionen verwalten.

Tabelle 46. Quarantäne-Funktionen und Einstellungswerkzeuge

QUARANTÄNE-FUNKTION	ADMINISTRATIONSKONSOLE VON KASPERSKY SECURITY CENTER	KONSOLE VON KASPERSKY ANTI-VIRUS
Ansicht, Sortierung und Objektentfernung	Ja (Detaillierte Informationen dazu finden Sie im *Administratorhandbuch für Kaspersky Security Center*.)	Ja
Objektfilterung	Nein	Ja
Möglicherweise infizierte Objekte aus Quarantäne zur Analyse im Virenlabor einschicken	Nein	Ja
Objekte per Hand in Quarantäne verschieben	Nein	Ja
Objekte aus Quarantäne wiederherstellen	Ja Es stehen folgende Varianten für die Wiederherstellung von Objekten zur Verfügung: • in den ursprünglichen Speicherort; • in den eingegebenen Speicherort in der Administrationskonsole von Kaspersky Security Center (Detaillierte Informationen dazu finden Sie im *Administratorhandbuch für Kaspersky Security Center*.)	Ja
Objekte in der Quarantäne untersuchen	Ja Aufgabe zur **Untersuchung von Quarantäne-Objekten** starten	Ja
Quarantäne-Einstellungen anpassen	Ja	Ja
Statistik für Quarantäne anzeigen	Ja	Ja

QUARANTÄNE-EINSTELLUNGEN IN KASPERSKY SECURITY CENTER ANPASSEN

Um die Quarantäne-Einstellungen anzupassen, gehen Sie wie folgt vor:

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Computer** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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**.
4. Verwenden Sie eine der folgenden Methoden, um im Fenster **Eigenschaften: <Computername>** im Abschnitt **Programme** das Fenster **Programmeinstellungen** zu öffnen:
   - 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 die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthalten ist, können diese Einstellungen nicht über das Fenster Programmeinstellungen geändert werden.
5. Klicken Sie im Abschnitt **Einstellungen** im Block **Speicher** auf die Schaltfläche **Einstellungen**.
6. Passen Sie im Fenster **Storage-Einstellungen** auf der Registerkarte **Quarantäne** die Quarantäne-Einstellungen an:
   - Wenn Sie den Quarantäne-Ordner ändern möchten, geben Sie im Eingabefeld **Ordner für die Quarantäne** den vollständigen Pfad zum Ordner 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 festzulegen möchten, aktivieren Sie die Kontrollkästchen **Maximale Größe der Quarantäne (MB)** und **Grenzwert für verfügbaren Speicherplatz (MB)**, und tragen Sie im Eingabefeld den Wert in MB 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.
7. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern.

VERWALTUNG VON BACKUP-OBJEKTEN UND ANPASSEN DER BACKUP-PARAMETER

IN DIESEM ABSCHNITT

BACKUP-FUNKTIONEN UND -EINSTELLUNG

In folgender Tabelle sind die Backup-Funktionen aufgezählt und die Administrationswerkzeuge angegeben, mit denen dessen Funktionen verwalten werden können.

Tabelle 47. Backup-Funktionen

BACKUP-FUNKTION	ADMINISTRATIONSKONSOLE VON KASPERSKY SECURITY CENTER (S. *ADMINISTRATORHANDBUCH FÜR KASPERSKY SECURITY CENTER*)	KONSOLE VON KASPERSKY ANTI-VIRUS
Anzeigen, Sortieren und Löschen von Dateien	Ja	Ja
Dateien filtern	Nein	Ja
Dateien aus Backup wiederherstellen	Ja Es stehen folgende Varianten für die Wiederherstellung von Objekten zur Verfügung: • in den ursprünglichen Speicherort; • in den eingegebenen Speicherort in der Administrationskonsole von Kaspersky Security Center	Ja
Anpassen der Backup-Parameter	Ja	Ja
Statistik für Backup ansehen	Ja	Ja

BACKUP-EINSTELLUNGEN IN KASPERSKY SECURITY CENTER ANPASSEN

Im Fenster **Programmeinstellungen** des ausgewählten geschützten Servers können Sie die Backup-Einstellungen anpassen.

Über Sicherungskopien von Objekten vor dem Desinfizieren oder Löschen finden Sie mehr auf S. 90.

Um die Backup-Parameter anzupassen, gehen Sie wie folgt vor:

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Computer** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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**.
4. Verwenden Sie eine der folgenden Methoden, um im Fenster **Eigenschaften: <Computername>** im Abschnitt **Programme** das Fenster **Programmeinstellungen** zu öffnen:
   - 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 die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthalten ist, können diese Einstellungen nicht über das Fenster Programmeinstellungen geändert werden.
5. Klicken Sie im Abschnitt **Einstellungen** im Gruppenfeld **Storage-Einstellungen** auf die Schaltfläche **Einstellungen**.
6. Passen Sie bei Bedarf im Fenster **Storage-Einstellungen** 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 Namen und 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 des Parameters **Maximale Größe des Backups (MB)**, aktivieren Sie das Kontrollkästchen **Grenzwert für verfügbaren Speicherplatz (MB)** und tragen Sie den entsprechenden Mindestwert für den freien Speicherplatz im Backup in MB ein.
- Um einen anderen Wiederherstellungsordner anzugeben, wählen Sie in der Einstellungsgruppe **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 an.

7. Klicken Sie auf **OK**.

VERWALTUNG VON DER VERTRAUENSWÜRDIGEN ZONE

In Kaspersky Security Center können Sie die vertrauenswürdige Zone von Kaspersky Anti-Virus verwalten.

IN DIESEM ABSCHNITT

PROZESSE ZUR VERTRAUENSWÜRDIGEN LISTE HINZUFÜGEN (KASPERSKY SECURITY CENTER)

In der Administrationskonsole von Kaspersky Security Center können Sie ausführbare Prozessdateien, die sich auf einem Laufwerk des geschützten Servers befinden, zur vertrauenswürdigen Zone hinzufügen. Prozesse aus der Liste der auf dem Server aktiven Prozesse können nicht hinzugefügt werden.

Gehen Sie folgendermaßen vor, um einen Prozess zur Liste der vertrauenswürdigen Prozesse von Kaspersky Anti-Virus hinzuzufügen:

1. Öffnen Sie in der Administrationskonsole von Kaspersky Security Center das Fenster **Programmeinstellungen**.
2. Klicken Sie im Abschnitt **Einstellungen** im Einstellungsblock **Vertrauenswürdige Zone** auf die Schaltfläche **Einstellungen**.
3. Aktivieren Sie im Fenster **Vertrauenswürdige Zone anpassen** auf der Registerkarte **Vertrauenswürdige Prozesse** die Funktion **Vertrauenswürdige Prozesse**: Aktivieren Sie dazu das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen**.
4. Wenn Sie die Einstellungen für die vertrauenswürdige Zone zuvor aus Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition in eine Konfigurationsdatei exportiert haben, können Sie die Einstellungen für die vertrauenswürdige Zone aus dieser Datei importieren. Gehen Sie hierzu wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Import**.
   b. Geben Sie im Fenster **Öffnen** die Konfigurationsdatei mit den Einstellungen für die vertrauenswürdige Zone an.
   c. Klicken Sie auf **OK**.

   Bitte beachten Sie, dass alle Parameter für die vertrauenswürdige Zone aus der Datei importiert werden.
5. Um die ausführbare Datei eines Prozesses auf einem Laufwerk des geschützten Servers auszuwählen, gehen Sie folgendermaßen vor:
   a. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   b. Klicken Sie im Fenster **Vertrauenswürdigen Prozess hinzufügen** auf die Schaltfläche **Durchsuchen** und wählen Sie die ausführbare Datei des Prozesses auf dem lokalen Laufwerk, auf dem die Management-Konsole von Kaspersky Security Center installiert ist.

c. Im Fenster **Vertrauenswürdigen Prozess hinzufügen** werden Name und Pfad der Datei angezeigt.

d. Klicken Sie auf **OK**.

Der Name der ausgewählten ausführbaren Prozessdatei wird auf der Registerkarte **Vertrauenswürdige Prozesse** in der Liste der vertrauenswürdigen Prozesse angezeigt.

Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

ECHTZEITSCHUTZ FÜR DATEIEN WÄHREND BACKUP-OPERATIONEN DEAKTIVIEREN

Sie können den Echtzeitschutz für Dateien, auf die bei Operationen zum Sicherungskopieren zugegriffen wird, während dem Anlegen von Sicherungskopien ausschalten. Kaspersky Anti-Virus untersucht Dateien nicht, die von einem Backup-Programm mit dem Attribut FILE_FLAG_BACKUP_SEMANTICS zum Lesen geöffnet werden.

Um den Echtzeitschutz für Dateien während des Anlegens von Sicherungskopien zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Programmeinstellungen**.
2. Klicken Sie im Abschnitt **Einstellungen** im Einstellungsblock **Vertrauenswürdige Zone** auf die Schaltfläche **Einstellungen**.
3. Um den Echtzeitschutz für Dateien, auf die beim Anlegen von Sicherungskopien zugegriffen wird, zu deaktivieren, aktivieren Sie auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Operationen beim Sicherungskopieren nicht untersuchen**.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.
5. Übernehmen Sie, falls erforderlich, die Ausnahmen der vertrauenswürdigen Zone in den ausgewählten Aufgaben und Richtlinien.

AUSNAHMEN ZUR VERTRAUENSWÜRDIGEN ZONE HINZUFÜGEN

Sie können der vertrauenswürdigen Zone Objekte hinzufügen, die von der Untersuchung ausgeschlossen werden sollen.

Gehen Sie folgendermaßen vor, um der vertrauenswürdigen Zone eine Ausnahme hinzuzufügen:

1. Öffnen Sie in der Administrationskonsole von Kaspersky Security Center das Fenster **Programmeinstellungen**.
2. Klicken Sie im Abschnitt **Einstellungen** im Einstellungsblock **Vertrauenswürdige Zone** auf die Schaltfläche **Einstellungen**.
3. Öffnen Sie im Fenster **Einstellungen der vertrauenswürdigen Zone anpassen** die Registerkarte **Ausnahmeregeln**.
4. Wenn Sie die Einstellungen für die vertrauenswürdige Zone von Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition zuvor in eine Konfigurationsdatei exportiert haben, können Sie die Einstellungen für die vertrauenswürdige Zone aus dieser Datei importieren:

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

   b. Geben Sie im Fenster **Öffnen** die Konfigurationsdatei mit den Einstellungen für die vertrauenswürdige Zone an.

   c. Klicken Sie auf **OK**.

   Bitte beachten Sie, dass alle Parameter für die vertrauenswürdige Zone aus der Datei importiert werden.
5. Um die Ausnahmen, die von der Firma Microsoft empfohlen werden, zur vertrauenswürdigen Zone hinzuzufügen, klicken Sie auf der Registerkarte **Ausnahmeregeln** auf **Empfohlene Ausnahmen hinzufügen** und bestätigen Sie den Vorgang im folgenden Fenster mit **OK**.
6. Um eine neue Ausnahmeregel hinzuzufügen, klicken Sie unter dem Feld **Beschreibung der Ausnahmeregel** auf **Hinzufügen**. Das Fenster **Ausnahmeregel** wird geöffnet.

   Geben Sie die Regel an, nach der Kaspersky Anti-Virus das Objekt ausschließen soll. Bitte beachten Sie die folgenden Empfehlungen:

   - Um gefundene Bedrohungen in bestimmten Ordnern oder Dateien auszuschließen, aktivieren Sie die Kontrollkästchen **Zu untersuchendes Objekt** und **Zu erkennende Objekte**.

- Damit alle gefundenen Objekte in den festgelegten Ordnern oder Dateien ausgeschlossen werden, aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt** und deaktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**.
- Damit die festgelegten gefundenen Objekte im gesamten Untersuchungsbereich ausgeschlossen werden, deaktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt** und aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**.

Wenn Sie den Speicherort des Objekts festlegen möchten, aktivieren Sie das Kontrollkästchen **Zu untersuchendes Objekt**, klicken Sie auf **Ändern** und geben Sie im Fenster **Objekt auswählen** das Objekt an, das von der Untersuchung ausgeschlossen werden soll. Klicken Sie anschließend auf **OK**. Sie können folgende Orte für ein Objekt auswählen:

- **Vordefinierter Bereich**. Wählen Sie einen vordefinierten Untersuchungsbereich aus der Liste aus.
- **Laufwerk, Ordner oder Netzwerkobjekt**. Geben Sie ein Laufwerk auf einem Server, einen Ordner auf einem Server oder in einem lokalen Netzwerk, oder ein Objekt in einem lokalen Netzwerk an.
- **Datei**. Geben Sie eine Datei auf dem Server oder im lokalen Netzwerk an.
- **Datei oder URL-Adresse des Skripts**. Geben Sie ein Skript auf dem geschützten Server, im lokalen Netzwerk oder im Internet an.

  Bei der Angabe von Masken für Ordner- und Dateinamen können die Zeichen **?** und ***** verwendet werden.

7. Wenn Sie ein gefundenes Objekt nach Namen oder Namensmaske ausschließen möchten, aktivieren Sie das Kontrollkästchen **Zu erkennende Objekte**, klicken Sie auf die Schaltfläche **Ändern** und geben Sie im Fenster **Liste der gefundenen Objekte** den erforderlichen Wert ein.

   Klicken Sie auf **OK**. Führen Sie eine der Aktionen durch:

   - Um eine Regel anzupassen, wählen Sie die betreffende Regel auf der Registerkarte **Ausnahmeregeln** aus, klicken Sie auf die Schaltfläche **Ändern** und nehmen Sie im Fenster **Ausnahmeregel** die entsprechenden Änderungen vor.
   - Um eine Regel zu löschen, wählen Sie die betreffende Regel auf der Registerkarte **Ausnahmeregeln** aus, klicken Sie auf **Löschen** und bestätigen Sie die Operation.
8. Aktivieren Sie die Kontrollkästchen neben den Namen der funktionalen Komponenten, in deren Aufgaben die Ausnahmeregel übernommen werden soll.

   Klicken Sie im Fenster **Einstellungen der vertrauenswürdigen Zone** auf **OK**.
9. Übernehmen Sie, falls erforderlich, die Ausnahmen der vertrauenswürdigen Zone in den ausgewählten Aufgaben und Richtlinien.

VERWENDUNG DER VERTRAUENSWÜRDIGEN ZONE IN KASPERSKY SECURITY CENTER

Sie können das Übernehmen der vertrauenswürdigen Zone in den vorhandenen Richtlinien sowie in den Aufgaben aktivieren oder deaktivieren (beim Erstellen einer Aufgabe oder im Fenster **Eigenschaften: <Aufgabename>**).

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

➧ *Gehen Sie folgendermaßen vor, um die vertrauenswürdige Zone in einer Richtlinie zu übernehmen:*

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Öffnen Sie im Ergebnisbereich die Registerkarte **Richtlinien**.
3. Öffnen Sie im Detailfenster das Kontextmenü für die Richtlinie, deren Parameter Sie anpassen möchten, und wählen Sie den Befehl **Eigenschaften**.
4. Gehen Sie im Fenster **Eigenschaften: <Programmname>** wie folgt vor:

   - Klicken Sie im Abschnitt **Einstellungen** im Einstellungsblock **Vertrauenswürdige Zone** auf die Schaltfläche **Einstellungen**.
   - Um die Ausnahme *vertrauenswürdige Prozesse* zu übernehmen, vergewissern Sie sich, dass auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Aktivität der angegebenen Prozesse nicht untersuchen** aktiviert ist und schließen Sie das Schloss in der Optionsgruppe **Vertrauenswürdige Prozesse**.

- Um die Ausnahme *Operationen beim Sicherungskopieren* zu übernehmen, vergewissern Sie sich, dass auf der Registerkarte **Vertrauenswürdige Prozesse** das Kontrollkästchen **Datei-Operationen beim Sicherungskopieren nicht untersuchen** aktiviert ist und schließen Sie das Schloss in der Optionsgruppe **Vertrauenswürdige Prozesse**.
- Um Ausnahmen zu übernehmen, die vom Benutzer festgelegt wurden, schließen Sie das Schloss im Einstellungsblock **Ausnahmeregeln** auf der Registerkarte **Ausnahmeregeln**.

5. Klicken Sie auf **OK**.

Gehen Sie folgendermaßen vor, um die vertrauenswürdige Zone in einer vorhandenen Aufgabe zu übernehmen:

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Öffnen Sie im Ergebnisfenster die Registerkarte **Computer**, öffnen Sie das Kontextmenü für die Zeile mit Informationen über den geschützten Server und wählen Sie den Befehl **Eigenschaften**.
3. Öffnen Sie im Fenster **Eigenschaften: <Computername>** im Abschnitt **Aufgaben** das Kontextmenü für die Aufgabe, die Sie anpassen möchten, und wählen Sie den Befehl **Eigenschaften**.
4. Aktivieren Sie im Fenster **Eigenschaften: <Aufgabenname>** im Abschnitt **Einstellungen** das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.

Die vertrauenswürdige Zone kann auch beim Erstellen einer Aufgabe übernommen werden.

BENACHRICHTIGUNGSEINSTELLUNGEN IN KASPERSKY SECURITY CENTER ANPASSEN

IN DIESEM ABSCHNITT

ALLGEMEINE INFORMATIONEN ÜBER DIE EINSTELLUNG VON BENACHRICHTIGUNGEN IN KASPERSKY SECURITY CENTER

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 Anti-Virus 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.

Die Benachrichtigungen über Ereignisse in Kaspersky Anti-Virus können entweder für einen einzelnen Server im Fenster **Eigenschaften** des ausgewählten Servers oder für eine Servergruppe im Fenster **Eigenschaften: <Name der Richtlinie>** der ausgewählten Gruppe angepasst werden.

Sie können die Benachrichtigungen auf der Registerkarte **Ereignisse** oder im Fenster **Benachrichtigungseinstellungen** anpassen. Sie können folgende Update-Typen anpassen:

- Auf der Registerkarte **Ereignisse** (standardmäßige Registerkarte des Programms Kaspersky Security Center) können Sie die Benachrichtigungen an den Administrator anpassen, die über Ereignisse der ausgewählten Typen erfolgen sollen. Welche Benachrichtigungsmöglichkeiten Sie haben und wie diese eingestellt werden, erfahren Sie im Dokument *Kaspersky Security Center. Administratorhandbuch*.
- Im Fenster **Benachrichtigungseinstellungen** können Sie Benachrichtigungen sowohl für den Administrator als auch für Benutzer einstellen.

  Details über die Benachrichtigungsarten, die Sie im Fenster **Benachrichtigungseinstellungen** anpassen können, finden Sie auf S. 105.

Die Benachrichtigungen über Ereignisse einiger Typen können nur auf einer der Registerkarten eingestellt werden. Ereignisse anderer Typen lassen sich auf beiden Registerkarten einstellen.

Wenn Sie die Benachrichtigungen über Ereignisse eines Typs mittels einer Methode gleichzeitig auf zwei Registerkarten, nämlich sowohl auf der Registerkarte **Ereignisse** als auch im Fenster **Benachrichtigungseinstellungen** einstellen, erhält der Systemadministrator Benachrichtigungen über diese Ereignisse durch die angegebene Methode zweimal.

BENACHRICHTIGUNGEN AN ADMINISTRATOR UND BENUTZER IM FENSTER BENACHRICHTIGUNGSEINSTELLUNGEN ANPASSEN

Gehen Sie folgendermaßen vor, um die Benachrichtigungen anzupassen:

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Computer** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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**.
4. Verwenden Sie eine der folgenden Methoden, um im Fenster **Eigenschaften: <Computername>** im Abschnitt **Programme** das Fenster **Programmeinstellungen** zu öffnen:
   - 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 die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthalten ist, können diese Einstellungen nicht über das Fenster Programmeinstellungen geändert werden.
5. Klicken Sie im Abschnitt **Berichte und Benachrichtigungen** im Block **Ereignisbenachrichtigungen** auf die Schaltfläche **Einstellungen**.
6. Passen Sie im Fenster **Benachrichtigungseinstellungen** die Ereignis-Benachrichtigungen der gewünschten Typen an und klicken Sie auf die Schaltfläche **OK**.

   Das Einstellen von Benachrichtigungen im Fenster **Benachrichtigungseinstellungen** gleicht dem Einstellen von Benachrichtigungen im Fenster **Benachrichtigungen** der Konsole von Kaspersky Anti-Virus.
7. Klicken Sie auf die Schaltfläche **OK**, um die eingegebenen Änderungen zu speichern.

ALLGEMEINE EINSTELLUNGEN IN KASPERSKY SECURITY CENTER ANPASSEN

Um die allgemeine Parameter von Kaspersky Anti-Virus anzupassen, gehen Sie wie folgt vor:

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Computer** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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**.
4. Verwenden Sie eine der folgenden Methoden, um im Fenster **Eigenschaften: <Computername>** im Abschnitt **Programme** das Fenster **Programmeinstellungen** zu öffnen:
   - 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 die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthalten ist, können diese Einstellungen nicht über das Fenster Programmeinstellungen geändert werden.

5. Passen Sie in den folgenden Abschnitten die Einstellungen für Kaspersky Anti-Virus entsprechend an.
6. Passen Sie im Abschnitt **Crash-Diagnose** die folgenden Einstellungen für die Crash-Diagnose an:
   - Aktivieren oder deaktivieren Sie das Erstellen eines Ablaufverfolgungsberichts.
   - Passen Sie, falls erforderlich, die Berichtseinstellungen an.
   - Aktivieren oder deaktivieren Sie die Erstellung von Dump-Dateien für Kaspersky Anti-Virus-Prozesse.

Informationen in Speicherdump- und Protokolldateien werden von Kaspersky Anti-Virus im Klartext aufgezeichnet.

7. Klicken Sie im Abschnitt **Einstellungen** im Einstellungsblock **Skalierbarkeit und Zuverlässigkeit** auf die Schaltfläche **Einstellungen** und passen Sie im folgenden Fenster folgende Anti-Virus-Einstellungen gemäß Ihren Anforderungen an:
   - Maximale Anzahl der aktiven Prozesse, die von Kaspersky Anti-Virus gestartet werden können.
   - Anzahl der Prozesse für Echtzeitschutz-Aufgaben
   - Maximale Anzahl der Prozesse für im Hintergrund laufende Aufgaben zur Untersuchung auf Befehl
   - Anzahl der Versuche zur Wiederherstellung von Aufgaben nach deren Absturz

   Klicken Sie auf **OK**.
8. Klicken Sie im Abschnitt **Einstellungen** im Einstellungsblock **Erweitert** auf die Schaltfläche **Einstellungen** und passen Sie im folgenden Fenster folgende Anti-Virus-Einstellungen gemäß Ihren Anforderungen an:
   - Soll das Kaspersky Anti-Virus-Symbol im Infobereich der Taskleiste des Servers jedes Mal angezeigt werden, wenn Kaspersky Anti-Virus nach dem Neustart des Servers automatisch gestartet wird? Details finden Sie in Pkt. "Anti-Virus-Symbol im Infobereich der Taskleiste" (s. S. 32).
   - Aktionen von Kaspersky Anti-Virus bei der Nutzung einer unterbrechungsfreien Stromversorgungsquelle
   - Anzahl der Tage, nach deren Ablauf die Ereignisse *Datenbanken sind veraltet*, *Datenbanken sind stark veraltet* und *Untersuchung wichtiger Bereiche liegt lange zurück* eintreten sollen

   Klicken Sie auf **OK**.

   Wählen Sie auf der Registerkarte **Hierarchischer Speicher** eine der folgenden Optionen für den Zugriff auf den hierarchischen Speicher aus:
   - **Kein HSM-System**.
   - **HSM-System verwendet Analysepunkte**.
   - **HSM-System verwendet erweiterte Dateiattribute**.
   - **Unbekanntes HSM-System**.

Wenn Sie kein HSM-System verwenden, belassen Sie den vorgegebenen Wert für den Parameter **Einstellungen des HSM-Systems** (**Kein HSM-System**).

9. Nachdem Sie die Werte der erforderlichen Einstellungen von Kaspersky-Anti-Virus entsprechend angepasst haben, klicken Sie im Fenster **Programmeinstellungen** auf die Schaltfläche **OK**.

BERICHTSEINSTELLUNGEN IN KASPERSKY SECURITY CENTER ANPASSEN

Um die Berichtsparameter von Kaspersky Anti-Virus anzupassen, gehen Sie wie folgt vor:

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Wählen Sie im Ergebnisbereich die Registerkarte **Computer** aus.
3. Verwenden Sie eine der folgenden Methoden, um das Fenster **Eigenschaften: <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**.
4. Verwenden Sie eine der folgenden Methoden, um im Fenster **Eigenschaften: <Computername>** im Abschnitt **Programme** das Fenster **Programmeinstellungen** zu öffnen:
   - 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 die Richtlinie von Kaspersky Security Center angewendet wird und diese Richtlinie ein Änderungsverbot für Programmeinstellungen enthalten ist, können diese Einstellungen nicht über das Fenster Programmeinstellungen geändert werden.
5. Klicken Sie im Abschnitt **Berichte und Benachrichtigungen** im Einstellungsblock **Berichte über Aufgabenausführung** auf die Schaltfläche **Einstellungen**.
6. Passen Sie im Fenster **Einstellungen für Berichte** die folgenden Eigenschaften für Kaspersky Anti-Virus 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** eine Anti-Virus-Komponente, deren Genauigkeitsstufe für Ereignisse Sie festlegen möchten.
     b. Um eine Genauigkeitsstufe in den Berichte über Aufgabenausführung und im Systemaudit-Bericht einer bestimmten Komponente anzugeben, wählen Sie die entsprechende Stufe in der Liste **Prioritätsstufe** aus.
   - Um den Standardordner zum Speichern von Berichten zu ändern, geben Sie den vollständigen Pfad des Ordners an oder wählen Sie den Ordner mit Hilfe der Schaltfläche **Durchsuchen** aus.
   - Geben Sie an, wie viele Tage die Berichte über die Aufgabenausführung gespeichert bleiben sollen.
   - Geben Sie an, wie viele Tage die im Knoten **Systemaudit-Bericht** angezeigten Informationen gespeichert werden sollen.
7. Klicken Sie auf **OK**, nachdem Sie die Werte der entsprechenden allgemeinen Berichtseinstellungen für Kaspersky-Anti-Virus angepasst haben.
8. Klicken Sie im Fenster **Programmeinstellungen** auf **OK**.

ERSTELLEN UND EINRICHTEN DER RICHTLINIEN

IN DIESEM ABSCHNITT

RICHTLINIEN

Sie können einheitliche Richtlinien in Kaspersky Security Center Richtlinien erstellen, um den Schutz auf mehreren Server zu verwalten, auf denen Kaspersky Anti-Virus installiert ist.

Eine Richtlinie übernimmt die in ihr eingetragenen Parameterwerte des Kaspersky Anti-Virus, seine Funktionen und Aufgaben auf allen geschützten Servern einer Administrationsgruppe.

Sie können mehrere Richtlinien für eine Administrationsgruppe erstellen und sie temporär übernehmen. In der Administrationskonsole hat eine Richtlinie, die zurzeit in der Gruppe gilt, den Status *aktiv*.

Informationen über den Geltungsbereich einer Richtlinie werden im Bericht zum System-Audit des Kaspersky Anti-Virus registriert. Diese Informationen stehen in der Konsole von Kaspersky Anti-Virus unter dem Knoten **Systemaudit-Bericht** zur Verfügung.

Beachten Sie, dass in Kaspersky Security Center nur eine Methode zum Übernehmen von Richtlinien existiert: **Obligatorische Einstellungen ändern**. Nach der Übernahme der Richtlinie für Kaspersky Security Center übernimmt Kaspersky Anti-Virus die Parameterwerte, neben denen Sie in den Richtlinieneigenschaften das Symbol 🔒 gesetzt haben, statt die Parameterwerte heranzuziehen, die bis zur Übernahme der Richtlinie gegolten haben. Kaspersky Anti-Virus übernimmt keine Parameterwerte, neben denen in den Richtlinieneigenschaften ein entsprechendes Zeichen gesetzt ist.

🔓 Während der Gültigkeitsdauer der Richtlinie werden in der Konsole von Kaspersky Anti-Virus und im Fenster **Programmeinstellungen <Programmname>** der Administrationskonsole die Einstellungswerte angezeigt, die in der Richtlinie mit dem Symbol 🔒 markiert sind. Diese Werte jedoch können nicht geändert werden. Die Werte der übrigen Einstellungen (die in der Richtlinie mit dem Symbol 🔓 markiert sind) können in der Konsole von Kaspersky Anti-Virus und im Fenster **Programmeinstellungen <Programmname>** der Administrationskonsole geändert werden.

Wenn die Richtlinie Einstellungen für eine der Aufgaben zum Echtzeitschutz und/oder für die Aufgaben zum Schutz von Netzwerkspeichern 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. Wenn die Richtlinie Einstellungen für die Update-Aufgaben oder die Aufgaben zur Untersuchung auf Befehl festlegt, so ändern sich diese Einstellungen nach der Übernahme der Richtlinie erst beim nächsten Start der Aufgabe.

ERSTELLEN DER RICHTLINIE IN KASPERSKY SECURITY CENTER

Das Erstellen einer neuen Richtlinie umfasst folgende Etappen:

1. Mit dem Assistenten für die Erstellung von Richtlinien erstellen Sie eine Richtlinie. In den Fenstern des Assistenten können Sie die Parameter für Echtzeitschutz anpassen.
2. Im Fenster **Eigenschaften** der erstellten Richtlinie können Sie Folgendes anpassen: Einstellungen für den Echtzeitschutz, Einstellungen für den Schutz von Netzwerkspeichern, allgemeine Einstellungen für Kaspersky Anti-Virus, Einstellungen für Quarantäne und Backup, Genauigkeitsstufe für Berichte über die Aufgabenausführung, Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Anti-Virus.

➧ *Gehen Sie folgendermaßen vor, um eine Richtlinie für eine Gruppe von Servern zu erstellen, auf denen Kaspersky Anti-Virus installiert ist:*

1. Im Baum der Administrationskonsole klappen Sie das Element **Verwaltete Computer** auf, dann klappen Sie die Administrationsgruppe auf, für deren Server Sie eine Richtlinie anlegen wollen.
2. Öffnen Sie im Ergebnisfenster die Registerkarte **Richtlinien** und klicken Sie dort auf den Link **Richtlinie erstellen**, um den Richtlinien-Assistenten zu öffnen.
3. Tragen Sie im Fenster **Name der Gruppenrichtlinie für das Programm festlegen** im Eingabefeld **Name** einen Namen für die zu erstellende Richtlinie ein (dabei sind folgende Zeichen unzulässig: `" * < : > ?`
4. Wählen Sie im Fenster **Programm zum Erstellen der Gruppenrichtlinie auswählen** im Abschnitt **Programmname** den Punkt **Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition** aus.
5. Wählen Sie im Fenster **Vorgangsart auswählen** eine der folgenden Optionen aus:
   - **Erstellen**, um eine neue Richtlinie mit Parametern zu erstellen, die als Standard für neu erstellten Richtlinie des bestimmten Typs gelten.
   - **Richtlinie aus der vorherigen Version von Kaspersky Anti-Virus importieren**, um eine früher erstellte Richtlinie von Kaspersky Anti-Virus 6.0 für Windows Servers als Vorlage zu verwenden.

   Klicken Sie auf die Schaltfläche **Durchsuchen** wählen Sie die Konfigurationsdatei , in der Sie die vorhandene Richtlinie gespeichert haben.

6. Passen Sie im Fenster **Echtzeitschutz** bei Bedarf die Einstellungen der Aufgabe **Echtzeitschutz für Dateien** und der Aufgabe **Skript-Untersuchung** gemäß Ihren Anforderungen an.

   In der neu erstellten Richtlinie sind die Einstellungen der Aufgabe **Echtzeitschutz für Dateien** und die Einstellungen der Aufgabe **Skript-Untersuchung** standardmäßig festgelegt.

   - Um die Einstellungen der Aufgabe **Echtzeitschutz für Dateien** zu ändern, klicken Sie in der Einstellungsgruppe **Echtzeitschutz für Dateien** auf die Schaltfläche **Einstellungen**. Passen Sie im Fenster **Einstellungen** den Schutzbereich an und wählen Sie eine der festgelegten Sicherheitsstufen aus, oder passen Sie die Sicherheitseinstellungen manuell an. Wählen Sie den Schutzmodus für Objekte aus und passen Sie die Verwendung der heuristischen Analyse und der vertrauenswürdigen Zone an. Stellen Sie den Aufgabenzeitplan ein. Klicken Sie auf **OK**.
   - Um die Einstellungen der Aufgabe **Skript-Untersuchung** zu ändern, klicken Sie in der Optionsgruppe **Skript-Untersuchung** auf **Einstellungen**. Wählen Sie dann im Fenster **Einstellungen** die Aktionen für potenziell gefährliche Skripte aus und passen Sie die Verwendung der heuristischen Analyse sowie das Übernehmen der vertrauenswürdigen Zone an. Stellen Sie den Aufgabenzeitplan ein. Klicken Sie auf **OK**.

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.
   - **Richtlinie für autonome Benutzer**, wenn Sie eine Richtlinie für einen verwalteten Computer erstellen möchten, der sich außerhalb des Unternehmensnetzwerks befindet. Eine Richtlinie für autonome Benutzer ist nur verfügbar für Kaspersky Anti-Virus für Workstations (auf der Plattform Microsoft Windows).

8. Im Fenster **Beenden** klicken Sie auf die Schaltfläche **Fertig**.

   Die erstellte Richtlinie wird in der Richtlinienliste im Knoten **Richtlinien** der ausgewählten Administrationsgruppe angezeigt. Jetzt können Sie im Fenster **Eigenschaften: <Name der Richtlinie>** weitere Einstellungen für Kaspersky Anti-Virus sowie für dessen Funktionen und Aufgaben anpassen.

EINRICHTEN DER RICHTLINIE IN KASPERSKY SECURITY CENTER

Im Fenster **Eigenschaften:<Name der Richtlinie>** der vorhandenen Richtlinie können Sie folgende Einstellungen anpassen: allgemeine Einstellungen von Kaspersky Anti-Virus, Einstellungen für Quarantäne und Backup, Einstellungen für die vertrauenswürdige Zone, Einstellungen für den Echtzeitschutz, Einstellungen für den Schutz von Netzwerkspeichern, Genauigkeitsstufe für Berichte über die Aufgabenausführung, Benachrichtigungen für Administrator und Benutzer über die Ereignisse in Kaspersky Anti-Virus.

➧ *Um die Einstellungen für die Richtlinie im Fenster **Eigenschaften: <Name der Richtlinie>,** anzupassen, gehen Sie wie folgt vor:*

1. Klappen Sie in der Struktur der Administrationskonsole den Knoten **Verwaltete Computer** auf, öffnen Sie die Administrationsgruppe, deren Richtlinie Sie anpassen möchten, und wählen Sie dann im Ergebnisfenster die Registerkarte **Richtlinien** aus.
2. Gehen Sie im Kontextmenü der Richtlinie, deren Einstellungen Sie anpassen möchten, auf **Eigenschaften**.
3. Passen Sie die erforderlichen Richtlinieneinstellungen im Fenster **Einstellungen: <Name der Richtlinie>** an.

   Im Abschnitt **Einstellungen** können Sie wie im Fenster **Programmeinstellungen** allgemeine Einstellungen für Kaspersky Anti-Virus, Quarantäne- und Backup-Einstellungen anpassen.

   Im Abschnitt **Berichte und Benachrichtigungen** können Sie Einstellungen für folgende Objekte anpassen:

   - Berichte über Aufgabenausführung und Systemaudit-Berichte. Analog zum Dialogfenster **Programmeinstellungen**.
   - Benachrichtigungen an Benutzer und Administrator über Ereignisse von Kaspersky Anti-Virus Analog zum Dialogfenster **Programmeinstellungen**.

   Im Abschnitt **Echtzeitschutz** können Sie folgende Einstellungen für den Echtzeitschutz anpassen:

   - in der Aufgabe **Echtzeitschutz für Dateien**:
     - Schutzmodus für Objekte
     - Verwendung der heuristischen Analyse

- Vertrauenswürdige Zone übernehmen
- Schutzbereich
- Sicherheitseinstellungen für den ausgewählten Schutzbereich: Sie können eine vordefinierte Sicherheitsstufe auswählen oder die Sicherheitseinstellungen manuell anpassen (auf gleiche Weise wie in der Konsole von Kaspersky Anti-Virus).
- Einstellungen für den Aufgabenstart

- in der Aufgabe **Skript-Untersuchung**:
  - Schutzbereich
  - Erlaubnis oder Verbot für das Ausführen von potentiell gefährlichen Skripten
  - Verwendung der heuristischen Analyse
  - Vertrauenswürdige Zone übernehmen
  - Einstellungen für den Aufgabenstart

Im Abschnitt **Schutz von Netzwerkspeichern** in der Aufgabe **RPC: Schutz von Netzwerkspeichern**:

- Schutzbereich
- Verwendung der heuristischen Analyse
- Vertrauenswürdige Zone übernehmen
- Einstellungen für die Verbindung mit einem Netzwerkspeicher
- Einstellungen für den Aufgabenstart

Im Abschnitt **Schutz von Netzwerkspeichern** in der Aufgabe **ICAP: Schutz von Netzwerkspeichern**:

- Verwendung der heuristischen Analyse
- Einstellungen für die Verbindung mit einem Netzwerkspeicher
- Einstellungen für den Aufgabenstart
- Sicherheitsstufe

4. Nachdem Sie die gewünschten Parameter der Richtlinie eingestellt haben, klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

ZEITGESTEUERTEN START FÜR LOKALE SYSTEMAUFGABEN DEAKTIVIEREN

Mit Richtlinien können Sie auf allen Servern aus einer Administrationsgruppe das Gelten des Zeitplans für folgende lokale Systemaufgaben deaktivieren:

- Aufgaben zur Virensuche: **Untersuchung kritischer Bereiche**, **Untersuchung von Quarantäne-Objekten** und **Untersuchung bei Systemstart**.
- Update-Aufgaben: **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 folgendermaßen vor, um den geplanten Start einer Systemaufgabe von Kaspersky Anti-Virus auf den Servern einer Gruppe zu deaktivieren:

1. Klappen Sie in der Struktur der Administrationskonsole den Knoten **Verwaltete Computer** auf, klappen Sie die entsprechende Gruppe auf und öffnen Sie im Ergebnisfenster die Registerkarte **Richtlinien**.
2. Wählen Sie auf der Registerkarte im Kontextmenü der Richtlinie, mit deren Hilfe Sie den geplanten Start von Systemaufgaben für Kaspersky Anti-Virus auf den Gruppenservern deaktivieren möchten, den Befehl **Eigenschaften**.
3. Öffnen Sie im Fenster **Eigenschaften**: **<Name der Richtlinie>** den Abschnitt **Systemaufgaben**.

4. Deaktivieren Sie das Kontrollkästchen neben den genannten Systemaufgaben, deren zeitgesteuerten Start Sie deaktivieren möchten.

   Um den Zeitplan der Systemaufgabe eines gewünschten Typs erneut zu aktivieren, kreuzen Sie das Kontrollkästchen neben den genannten Aufgaben dieses Typs wieder an.

5. Klicken Sie auf **OK**.

Wenn der Start von Systemaufgaben nach Zeitplan deaktiviert wurde, können die Aufgaben manuell aus der Konsole von Kaspersky Anti-Virus sowie aus der Administrationskonsole von Kaspersky Security Center gestartet werden.

ERSTELLEN UND EINRICHTEN DER AUFGABE

IN DIESEM ABSCHNITT

AUFGABEN ERSTELLEN

Sie können lokale benutzerdefinierte Aufgaben, Aufgaben für eine zufällige Zusammenstellung von Computern und Gruppenaufgaben folgenden Typs erstellen:

- Schlüssel hinzufügen;
- Update-Verteilung;
- Aufgaben zum Update
- Rollback des Updates der Datenbanken
- Untersuchung auf Befehl

Lokale Aufgaben für den ausgewählten geschützten Server werden im Fenster **Programmeinstellungen** im Abschnitt **Aufgaben** erstellt, Gruppenaufgaben im Knoten **Gruppenaufgabe** der ausgewählten Gruppe, Aufgaben für mehrere Computer, die nicht in einer Gruppe zusammengefasst sind, im Knoten **Aufgaben für eine Auswahl von Computern**.

Mit Richtlinien können Sie den Zeitplan für lokale Systemaufgaben zum Update und zur Untersuchung auf Befehl auf allen geschützten Servern, die zur einen Gruppe gehören, ausschalten.

Allgemeine Informationen über den Aufgaben in Kaspersky Security Center stehen im Dokument *Kaspersky Security Center. Administratorhandbuch*.

ERSTELLEN DER AUFGABE IN KASPERSKY SECURITY CENTER

Um eine neue Aufgabe in der Administrationskonsole von Kaspersky Security Center zu erstellen, gehen Sie wie folgt vor:

1. Starten Sie den Assistenten für die Aufgabenerstellung:
   - Für das Erstellen einer lokalen Aufgabe:
     a. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
     b. Öffnen Sie im Ergebnisfenster auf der Registerkarte **Computer** das Kontextmenü für die Zeile mit Informationen über den geschützten Server und wählen Sie den Punkt **Eigenschaften**.
     c. Klicken Sie im Abschnitt **Aufgaben** auf **Hinzufügen**.

- Für das Erstellen einer Gruppenaufgabe:
  a. in der Administrationskonsole wählen Sie die Gruppe, für die Sie eine Gruppenaufgabe erstellen wollen;
  b. Öffnen Sie im Ergebnisfenster das Kontextmenü auf der Registerkarte **Aufgaben** und wählen Sie den Punkt **Erstellen → Aufgabe**.
- Für das Erstellen einer Aufgabe für eine zufällige Zusammenstellung von Computern öffnen Sie in der Administrationskonsole das Kontextmenü für den Knoten **Aufgaben für Zusammenstellungen von Computern** und wählen Sie den Punkt **Erstellen → Aufgabe**.

Es öffnet sich das Begrüßungsfenster des Assistenten.

2. Geben Sie im Fenster **Aufgabenname festlegen** des Aufgaben-Assistenten einen Aufgabennamen an (maximal 100 Zeichen, wobei folgende Zeichen unzulässig sind: **I * < > ?** Wir empfehlen den Aufgabentyp im Namen anzugeben (z. B. "On-Demand-Scan der gemeinsamen Ordner").
3. Wählen Sie im Fenster **Aufgabentyp auswählen** unter der Überschrift **Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition** den Typ der zu erstellenden Aufgabe aus.
4. Wenn Sie einen anderen Aufgabentyp als **Rollback des Datenbank-Updates** oder **Schlüssel hinzufügen** ausgewählt haben, wird das Fenster **Einstellungen** geöffnet. Wählen Sie darin eine der folgenden Varianten aus
   - **Erstellen**, um eine neue Aufgabe mit Parametern zu erstellen, die als Standard für neu erstellten Aufgaben des bestimmten Typs gelten.
   - **Aufgabe aus der vorherigen Version von Kaspersky Anti-Virus importieren**, um eine früher erstellte Aufgabe von Kaspersky Anti-Virus 6.0 für Windows Servers als Vorlage zu verwenden.

     Klicken Sie auf die Schaltfläche **Durchsuchen** wählen Sie die Konfigurationsdatei , in der Sie die vorhandene Aufgabe gespeichert haben.
5. Je nach Typ der zu erstellenden Aufgabe führen Sie eine der folgenden Aktionen aus:
   - *Wenn Sie eine Aufgabe zur Untersuchung auf Befehl erstellen*:
     a. Im Fenster **Untersuchungsbereich** legen Sie den Untersuchungsbereich an.

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

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

     - Um alle Bereiche von der Untersuchung auszuschließen, öffnen Sie nacheinander für jede einzelne Zeile das Kontextmenü und wählen Sie **Bereich löschen**.
     - Um dem Untersuchungsbereich vordefinierte Bereiche, Festplatten, Ordner, Netzwerkobjekte oder Dateien hinzuzufügen, klicken Sie mit der rechten Maustaste auf die Tabelle **Untersuchungsbereich** und wählen Sie **Untersuchungsbereich hinzufügen**. Wählen Sie entweder im Fenster **Zum Untersuchungsbereich hinzufügen** einen vordefinierten Bereich aus der Liste **Vordefinierter Untersuchungsbereich** aus oder geben Sie eine Festplatte des Servers, einen Ordner, ein Netzwerkobjekt auf dem Server oder auf einem anderen Computer an, und klicken Sie dann auf **OK**.
     - Um eingebettete Ordner oder Dateien von der Untersuchung auszuschließen, wählen Sie den hinzugefügten Ordner (Festplatte) im Fenster **Untersuchungsbereich** des Assistenten aus, öffnen Sie das Kontextmenü und wählen Sie **Anpassen**. Klicken Sie dann im Fenster **Sicherheitsstufe** auf **Einstellungen** und deaktivieren Sie im Fenster **Untersuchung auf Befehl anpassen** auf der Registerkarte **Allgemein** das Kontrollkästchen **Untergeordnete Ordner** (**Untergeordnete Dateien**).
     - Um die Sicherheitseinstellungen für den Untersuchungsbereich zu ändern, öffnen Sie das Kontextmenü mit einem Rechtsklick auf den Bereich, dessen Parameter Sie ändern wollen, und wählen Sie **Anpassen**. Wählen Sie im Fenster **Untersuchung auf Befehl anpassen** eine der vordefinierten Sicherheitsstufe aus oder klicken Sie auf die Schaltfläche **Einstellungen**, um die Sicherheitseinstellungen manuell anzupassen. Die Konfiguration wird ebenso wie in der Anti-Virus-Konsole 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 Untersuchungsbereich** 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 in der Tabelle mit dem Zeichen ☐ markiert sind.

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

Aktivieren Sie das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**, wenn Sie in der Aufgabe vom Untersuchungsbereich diejenigen Objekte ausschließen wollen, die in der vertrauenswürdigen Zone des Kaspersky Anti-Virus beschrieben werden.

Wenn Sie planen, die zu erstellende Aufgabe als Untersuchung kritischer Bereiche zu verwenden, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabenausführung als Untersuchung kritischer Computerbereiche betrachten**. Das Programm Kaspersky Security Center berücksichtigt bei der Bewertung des Sicherheitszustands des Servers (bzw. der Server) die Ergebnisse der Aufgabenausführung mit dem Status "Aufgabe zur Untersuchung wichtiger Bereich", und nicht nur die Ausführungsergebnisse der Systemaufgabe **Untersuchung kritischer 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** (**Low**) zuzuweisen, aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabe im Hintergrundmodus ausführen**. Arbeitsprozesse, in denen Aufgaben für Kaspersky Anti-Virus ausgeführt werden, besitzen 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 anpassen**. Das Fenster **Verbindungseinstellungen anpassen** wird geöffnet.

  c. Gehen Sie auf der Registerkarte **Verbindungseinstellungen anpassen** 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 Proxyserver 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.

- *Wenn Sie die Aufgabe "Update der Programm-Module" erstellen*, passen Sie im Fenster **Update-Einstellungen für die 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 für Programm-Module verteilen und installieren** ausgewählt haben, kann zum Übernehmen der installierten Programm-Module ein Neustart des Servers erforderlich sein. Damit Kaspersky Anti-Virus den Server automatisch neu startet, nachdem die Aufgabe abgeschlossen wurde, aktivieren Sie das Kontrollkästchen **System-Neustart zulassen**. Um den Neustart des Servers zu verschieben, entfernen Sie das Häkchen in **System-Neustart zulassen**.

  c. Wenn Sie Informationen über die Veröffentlichung von geplanten Updates für Module von Kaspersky Anti-Virus, erhalten möchten, aktivieren Sie das Kontrollkästchen **Über verfügbare planmäßige Updates für die Programm-Module benachrichtigen**.

  Geplante Updatepakete werden von Kaspersky Lab nicht auf den Updateservern veröffentlicht, um sie automatisch zu installieren. Sie können solche Updatepakete von der Kaspersky-Lab-Webseite downloaden. Sie können festlegen, dass der Administrator über das Ereignis **Geplante Update für Module von Kaspersky Anti-Virus sind verfügbar** benachrichtigt wird. Die Benachrichtigung enthält die Adresse unserer Webseite, von der Sie geplante Updates herunterladen können.

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

- *Wenn Sie die Aufgabe "Schlüssel hinzufügen" erstellen*, geben Sie im Fenster **Schlüssel hinzufügen** im Feld **Schlüsseldatei** den Namen einer Schlüsseldatei mit der Endung .key und den vollständigen Pfad dieser Datei an.

6. Passen Sie die Einstellungen für den Aufgabenzeitplan an (Sie können den Aufgabenzeitplan für alle Aufgabentypen außer **Rollback des Datenbank-Updates** anpassen). Im Fenster **Zeitplan** führen Sie folgende Aktionen durch:

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

   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 Aufgaben **Update der Programm-Datenbanken**, **Update der Programm-Module** und **Update-Verteilung** 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 **Start** die den ersten Startzeitpunkt für die Aufgabe an, 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 Einstellungen für den Zeitplan** 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 eines Tages angehalten werden soll: Geben Sie in der Gruppe **Einstellungen für das Anhalten der Aufgabe** im Feld **Anhalten von … 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.
      - Schalten Sie den Start von übersprungenen Aufgaben ein: 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**.

7. 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.

8. Im Fenster **Arbeit des Assistenten zum Erstellen der Aufgabe abschließen** klicken Sie auf die Schaltfläche **Fertig**.

Die erstellte Aufgabe erscheint im Fenster **Aufgaben**.

EINRICHTEN DER AUFGABE IN KASPERSKY SECURITY CENTER

Nachdem Sie eine Aufgabe erstellt haben, können Sie folgende Einstellungen anpassen:

- Aufgabenparameter ändern
- Aufgabenzeitplan einstellen / ändern
- Benutzerkonto auswählen, mit dessen Rechten die Aufgabe ausgeführt wird
- Benachrichtigungen über Aufgabenergebnisse einstellen

➧ *Gehen Sie folgendermaßen vor, um eine Aufgabe anzupassen:*

1. In der Administrationskonsole klappen Sie den Knoten **Verwaltete Computer** auf und gehen auf die Gruppe, zu der der geschützte Server gehört.
2. Im Ergebnisfenster öffnen Sie das Kontextmenü mit einem Rechtsklick auf die Zeile mit dem geschützten Server und gehen Sie auf **Eigenschaften**.

3. Öffnen Sie im Fenster **Eigenschaften: <Computername>** im Abschnitt **Aufgaben** das Kontextmenü für die Aufgabe, die Sie anpassen möchten, und wählen Sie den Befehl **Eigenschaften**.
4. Passen Sie bei Bedarf die Aufgabenparameter an: Gehen Sie hierzu wie folgt vor:
   - In der Aufgabe **Echtzeitschutz für Dateien** im Abschnitt **Einstellungen**:
     - Legen Sie den Schutzbereich fest.
     - Aktivieren Sie die Verwendung der heuristischen Analyse: Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Heuristische Analyse verwenden**.
     - Übernehmen Sie die vertrauenswürdige Zone: Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.
     - Ändern Sie den Schutzmodus für Objekte: Wählen Sie im Abschnitt **Einstellungen** den entsprechenden Schutzmodus für Objekte aus.
   - In der Aufgabe **RPC: Schutz von Netzwerkspeichern** im Abschnitt **Einstellungen**:
     - Fügen Sie einen Netzwerkspeicher zum Schutzbereich hinzu.
     - Aktivieren Sie die Verwendung der heuristischen Analyse: Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Heuristische Analyse verwenden**.
     - Konfigurieren Sie die Verbindungseinstellungen für Netzwerkspeicher im Abschnitt **Einstellungen**.
   - In der Aufgabe **ICAP: Schutz von Netzwerkspeichern** im Abschnitt **Einstellungen**:
     - Aktivieren Sie die heuristische Analyse: Setzen Sie das Häkchen im Kontrollkästchen **Heuristische Analyse verwenden**.
     - Konfigurieren Sie die Verbindungseinstellungen für Netzwerkspeicher
     - Konfigurieren Sie die Sicherheitsstufe
   - in der Aufgabe **Skript-Untersuchung** auf der Registerkarte **Einstellungen**:
     - Legen Sie fest, ob die Ausführung von Skripts, die Kaspersky Anti-Virus als potenziell gefährlich einstuft, erlaubt oder verboten werden soll.
     - Aktivieren Sie die Verwendung der heuristischen Analyse: Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Heuristische Analyse verwenden**.
     - Übernehmen Sie die vertrauenswürdige Zone: Aktivieren Sie im Abschnitt **Einstellungen** das Kontrollkästchen **Vertrauenswürdige Zone übernehmen**.
   - In der Aufgabe **Untersuchung kritischer Bereiche** im Abschnitt **Einstellungen**:
     - Legen Sie den Untersuchungsbereich fest.
     - Ändern Sie im Abschnitt **Einstellungen** die Priorität des aktiven Prozesses, in dem die Aufgabe ausgeführt wird.
     - Weisen Sie der Aufgabe im Abschnitt **Einstellungen** erforderlichenfalls den Status Aufgabe zur Untersuchung wichtiger Computerbereiche zu.
     - Übernehmen Sie im Abschnitt **Einstellungen** die vertrauenswürdige Zone.
   - In der Aufgabe **Update-Verteilung**:
     - Geben Sie im Abschnitt **Einstellungen für Update-Verteilung** die Zusammensetzung der Updates und einen Ordner an, in dem sie gespeichert werden sollen.
     - Geben Sie im Abschnitt **Update-Quelle** die Update-Quelle an.
   - In der Aufgabe **Update der Programm-Datenbanken**:
     - Geben Sie im Abschnitt **Update-Quelle** die Update-Quelle an.
   - In der Aufgabe **Update der Programm-Module**:
     - Geben Sie im Abschnitt **Update-Quelle** die Update-Quelle an.
     - Wählen Sie im Abschnitt **Update-Einstellungen für die Programm-Module anpassen** die Verteilungsmethode für das Update der Programm-Module aus und aktivieren Sie das Kontrollkästchen **Informationen über verfügbare geplante Updates für Programm-Module empfangen**.

- Konfigurieren Sie für alle Aufgaben außer **Rollback des Datenbank-Updates** im Abschnitt **Zeitplan** den Aufgabenzeitplan.
- Geben Sie für alle Aufgaben außer **Rollback des Datenbank-Updates** im Abschnitt **Benutzerkonto** das Benutzerkonto an, mit dessen Berechtigungen die Aufgabe ausgeführt wird.
- Konfigurieren Sie für alle Aufgaben außer **Rollback des Datenbank-Updates** im Abschnitt **Benachrichtigung** die Benachrichtigungen über Ergebnisse der Aufgabenausführung (weitere Details finden Sie im Dokument *Kaspersky Security Center. Benutzerhandbuch*);

5. Klicken Sie auf **OK**.
6. Klicken Sie im Fenster **Eigenschaften: <Aufgabenname>** auf **OK**, um die Änderungen zu speichern.

UNTERSUCHUNG DER SERVER VERWALTEN. ZUWEISEN DES STATUS AUFGABE ZUR UNTERSUCHUNG KRITISCHER COMPUTERBEREICHE AN EINE UNTERSUCHUNGSAUFGABE

In der Grundeinstellung weist Kaspersky Security Center einem Server den Status **Warnung** zu, wenn die Aufgabe **Untersuchung kritischer Bereiche** seltener ausgeführt wird, als durch den Anti-Virus-Parameter **Grenzwert für Ereigniserstellung "Untersuchung kritischer Bereiche liegt lange zurück"** angegeben.

Gehen Sie folgendermaßen vor, um die Untersuchung aller Server anzupassen, die zu einer Administrationsgruppe gehören:

1. Erstellen Sie eine Gruppenaufgabe zur Virensuche. Aktivieren Sie im Fenster **Einstellungen** des Assistenten für die Aufgabenerstellung das Kontrollkästchen **Aufgabenausführung als Untersuchung kritischer Computerbereiche betrachten**. Die von Ihnen angegebenen Aufgabenparameter, nämlich der Untersuchungsbereich und die Parameter für Sicherheit, sind für alle Server der Gruppe gleich. Stellen Sie den Aufgabenzeitplan ein. Weitere Informationen über das Erstellen einer Aufgabe.

   Sie können das Kontrollkästchen **Aufgabenausführung als Untersuchung kritischer Computerbereiche betrachten** im Fenster **Eigenschaften: <Aufgabenname>** entweder dann aktivieren, wenn Sie eine Aufgabe zur Untersuchung auf Befehl für eine Computergruppe oder für eine Auswahl von Computern erstellen, oder zu einem späteren Zeitpunkt.

2. Deaktivieren Sie die Systemaufgabe **Untersuchung kritischer Bereiche** auf den Servern der Gruppe. Verwenden Sie dazu eine neue oder die vorhandene Richtlinie.

Von diesem Zeitpunkt an berücksichtigt der Administrationsserver für Kaspersky Security Center bei der Bewertung des Sicherheitszustands des geschützten Servers und bei der Benachrichtigung darüber die Ergebnisse der letzten Aufgabenausführung mit dem Status "Aufgabe zur vollständigen Untersuchung des Computers", nicht die Ausführungsergebnisse der Systemaufgabe **Untersuchung kritischer Bereiche**.

Sie können den Status "Aufgabe zur Untersuchung kritischer Bereiche" nicht nur Gruppenaufgaben, sondern auch Aufgaben für Zusammenstellungen von Computern zur Untersuchung auf Befehl zuweisen.

In der Konsole von Kaspersky Anti-Virus können Sie überprüfen, ob eine Aufgabe zur Untersuchung auf Befehl als Aufgabe zur Untersuchung kritischer Bereiche betrachtet wird.

In der Konsole von Kaspersky Anti-Virus wird das Häkchen in **Aufgabenausführung als Untersuchung kritischer Bereiche auffassen** in den Aufgabeneigenschaften nur angezeigt und kann nicht geändert werden.

KASPERSKY ANTI-VIRUS-INDIKATOREN

Dieser Abschnitt informiert über die Indikatoren von Kaspersky Anti-Virus: Leistungsindikatoren für das Programm "Systemmonitor" sowie Indikatoren und SNMP-Traps.

IN DIESEM ABSCHNITT

LEISTUNGSINDIKATOREN FÜR DIE ANWENDUNG SYSTEMMONITOR

IN DIESEM ABSCHNITT

LEISTUNGSINDIKATOREN FÜR KASPERSKY ANTI-VIRUS

Wenn als zu installierende Anti-Virus-Komponenten die Komponente **Leistungsindikatoren** aktiviert wurde, registriert Anti-Virus während der Installation seine Leistungsindikatoren für die Anwendung "Systemmonitor" von Microsoft Windows.

Mit den Kaspersky Anti-Virus-Indikatoren können Sie die Leistung von Kaspersky Anti-Virus bei der Ausführung von Echtzeitschutz-Aufgaben kontrollieren. Sie können Engpässe beim Zusammenwirken mit anderen Anwendungen und bei ungenügenden Ressourcen überwachen. Außerdem können Sie nicht so optimale Einstellungen von Kaspersky Anti-Virus und Abstürze diagnostizieren.

Sie können die Leistungsindikatoren für Kaspersky Anti-Virus anzeigen, indem Sie die Konsole **Leistung** im Element des Verwaltungsfensters **Administration** öffnen.

Die folgenden Punkte erklären die Indikatoren, nennen die empfohlenen Intervalle für das Ablesen der Werte und entsprechende Grenzwerte. Außerdem werden Empfehlungen zur Konfiguration von Kaspersky Anti-Virus bei Grenzwertüberschreitungen gegeben.

ANZAHL DER ABGELEHNTEN ANFRAGEN

Tabelle 48. Anzahl der abgelehnten Anfragen

Bezeichnung	Summe der abgelehnten Anfragen (Number of requests denied)
Definition	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die nicht von Anti-Virus-Prozessen angenommen wurden. Es wird ab dem letzten Start von Kaspersky Anti-Virus gezählt. Anti-Virus überspringt Objekte, deren Verarbeitungsanfragen von aktiven Anti-Virus-Prozessen zurückgewiesen werden.
Ziel	Ein Indikator kann überwachen: • Qualitätsverluste beim Echtzeitschutz wegen hoher Belastung der Arbeitsprozesse von Kaspersky Anti-Virus • Unterbrechung des Echtzeitschutzes wegen Abweisungen vom File-Interception-Dispatcher
Normalwert / Schwellenwert	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: • Indikator zeigt mehrere abgelehnte Anfrage im Laufe einer längeren Zeit: Alle Arbeitsprozesse von Kaspersky Anti-Virus waren vollständig ausgelastet, deshalb konnte Kaspersky Anti-Virus die Objekte nicht untersuchen. Um das Überspringen von Objekten auszuschließen, erhöhen Sie die Menge an Anti-Virus-Prozessen für Aufgaben des Echtzeitschutzes. Sie können die Kaspersky Anti-Virus-Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** verwenden. • Die Summe der abgelehnten Anfragen übersteigt den kritischen Schwellenwert erheblich und steigt schnell an: Der File-Interception-Dispatcher ist ausgefallen. Kaspersky Anti-Virus untersucht keine Objekte beim Zugriff. Starten Sie Kaspersky Anti-Virus neu.

ANZAHL DER ÜBERSPRUNGENEN ANFRAGEN

Tabelle 49. Anzahl der übersprungenen Anfragen

Bezeichnung	Anzahl der übersprungenen Anfragen (Number of requests skipped).
Definition	Anzahl der Anfragen des File-Interceptor-Treibers zur Verarbeitung von Objekten, die von Kaspersky Anti-Virus angenommen wurden, über die aber kein Ereignis über den Verarbeitungsabschluss gesendet wurde. Es wird ab dem letzten Anti-Virus-Start 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 Anti-Virus das Objekt und erhöht den Wert des Indikators **Anzahl der abgelehnten Anfragen** um 1.
Ziel	Der Indikator kann einen Produktivitätsverlust wegen ausbleibender Datenströme vom File-Interception-Dispatcher überwachen.
Normalwert / Schwellenwert	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 den Anzahl der Datenströme, die zurzeit stillstehen. Wenn das Untersuchungstempo nicht befriedigt, starten Sie Kaspersky Anti-Virus noch einmal, um die angehaltenen Datenströme wiederherzustellen.

ANZAHL DER ANFRAGEN, DIE WEGEN UNZUREICHENDER SYSTEMRESSOURCEN NICHT VERARBEITET WURDEN

Tabelle 50. Anzahl der Anfragen, die wegen unzureichender Systemressourcen nicht verarbeitet wurden

Bezeichnung	Summe der Anfragen, die aufgrund nicht genügender Systemressourcen nicht verarbeitet wurden (Number of requests not processed due to lack of resources)
Definition	Anzahl der Anfragen des File-Interception-Treibers, die aufgrund ungenügender Systemressourcen (beispielsweise des Arbeitsspeichers) nicht verarbeitet wurden. Es wird ab dem letzten Start von Kaspersky Anti-Virus gezählt. Kaspersky Anti-Virus überspringt Objekte, deren Verarbeitungsanfragen von den aktiven Anti-Virus-Prozessen zurückgewiesen werden.
Ziel	Der Indikator kann mögliche Qualitätsverluste des Echtzeitschutzes erkennen und beseitigen, die aufgrund nicht genügender Systemressourcen eintreten.
Normalwert / Schwellenwert	0 / 1
Empfohlenes Intervall zum Ablesen der Werte	1 Stunde
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Indikatorwert ungleich Null ist, brauchen die Prozesse von Kaspersky Anti-Virus 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 51. Anzahl der Anfragen, die zur Verarbeitung weitergeleitet wurden

Bezeichnung	Summe der Anfragen, zur Verarbeitung weitergeleitet wurden (Nummer of requests sent to be processed)
Definition	Anzahl der Objekte, die auf Verarbeitung durch aktive Prozesse warten.
Ziel	Der Indikator kann das Laden der Anti-Virus-Prozesse und das Niveau der Dateiaktivität auf dem Server verlangsamen.
Normalwert / Schwellenwert	Der Indikatorwert kann schwanken, je nach Niveau 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 52. Durchschnittliche Anzahl der Datenströme des File-Interception-Dispatchers

Bezeichnung	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 Anti-Virus zurückgehen.
Normalwert / Schwellenwert	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 Anti-Virus überspringt das Objekt. Vergrößern Sie die Anzahl der Prozesse von Kaspersky Anti-Virus für die Aufgaben des Echtzeitschutzes. Sie können in Kaspersky Anti-Virus die Einstellungen **Maximale Anzahl aktiver Prozesse** und **Anzahl der Prozesse für den Echtzeitschutz** verwenden.

MAXIMALE ANZAHL DER DATENSTRÖME DES FILE-INTERCEPTION-DISPATCHERS

Tabelle 53. Maximale Anzahl der Datenströme des File-Interception-Dispatchers

Bezeichnung	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 / Schwellenwert	Variiert / 40.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.
Konfigurationstipps bei Grenzwertüberschreitung	Wenn der Wert dieses Indikators dauerhaft und erheblich von dem Indikatorwert **Mittelwert der Datenströme vom File-Interception-Dispatcher** abweicht, verteilt Kaspersky Anti-Virus die Belastung ungleichmäßig auf die ausführenden Prozesse. Starten Sie Kaspersky Anti-Virus neu.

ANZAHL DER INFIZIERTEN OBJEKTE IN DER VERARBEITUNGSWARTESCHLANGE

Tabelle 54. Anzahl der infizierten Objekte in der Verarbeitungswarteschlange

Bezeichnung	Anzahl der infizierten Objekte in der Verarbeitungswarteschlange (Number of items in the infected object queue)
Definition	Anzahl der infizierten Objekte, die momentan auf die Verarbeitung (Desinfektion oder Löschen) warten.
Ziel	Dieser Indikator erlaubt es, folgende Situationen zu erkennen: • Unterbrechung des Echtzeitschutzes wegen möglichen Abweisungen vom File-Interception-Dispatcher • Überlastung des Prozessors wegen ungleichmäßiger Verteilung der Prozessorzeit zwischen den anderen laufenden Anwendungen und Kaspersky Anti-Virus • Virenepidemie
Normalwert / Schwellenwert	Der Indikatorwert kann von Null abweichen, wenn Kaspersky Anti-Virus 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 Anti-Virus verarbeitet keine Objekte (möglicherweise hat ihn der File-Interception-Dispatcher abgewiesen) Starten Sie Kaspersky Anti-Virus neu. • Es steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Anti-Virus zusätzliche Prozessorzeit ein, indem Sie beispielsweise die Serverbelastung 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**. Sie können Informationen über die Menge der gefundenen Objekte in der Aufgabenstatistik (s. S. 61) oder im Bericht über die Aufgabenausführung (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99) anzeigen.

ANZAHL DER PRO SEKUNDE VERARBEITETEN OBJEKTE

Tabelle 55. Anzahl der pro Sekunde verarbeiteten Objekte

Bezeichnung	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	Der Indikator zeigt das Tempo der Objektverarbeitung. So können Produktivitätsverluste des Servers erkannt und beseitigt werden, die wegen schlecht verteilter Prozessorzeit an Arbeitsprozesse oder wegen eines Anti-Virus-Absturzes eingetreten sind.
Normalwert / Schwellenwert	Variiert / Nein.
Empfohlenes Intervall zum Ablesen der Werte	1 Min.

Konfigurationstipps bei Grenzwertüberschreitung	Die Indikatorwerte hängen von den aktivierten Werten der Parameter für Kaspersky Anti-Virus und von der Belastung des Server durch Prozesse anderer Anwendungen 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 Anti-Virus-Prozessen steht zu wenig Prozessorzeit für die Objektverarbeitung zur Verfügung. Räumen Sie Kaspersky Anti-Virus zusätzliche Prozessorzeit ein, indem Sie beispielsweise die Serverbelastung durch andere Anwendungen senken. • Kaspersky Anti-Virus ist abgestürzt (Mehrere Datenströme stehen still). Starten Sie Kaspersky Anti-Virus neu.

INDIKATOREN UND SNMP-TRAPS FÜR KASPERSKY ANTI-VIRUS

IN DIESEM ABSCHNITT

INDIKATOREN UND SNMP-TRAPS FÜR KASPERSKY ANTI-VIRUS

Wenn Sie als zu installierende Komponente von Kaspersky Anti-Virus die Komponente **Indikatoren und SNMP-Traps** aktiviert haben, können Sie Counter und Traps für Kaspersky Anti-Virus mit den Protokollen Simple Network Management Protocol (SNMP) anzeigen.

Um die Indikatoren und Traps für Kaspersky Anti-Virus am Arbeitsplatz (Rechner) des Administrators anzuzeigen, starten Sie auf dem geschützten Server den SNMP-Dienst (SNMP Service), und Administrator-Arbeitsplatz den SNMP-Dienst (SNMP Service) und den Dienst SNMP-Traps (SNMP Trap Service).

SNMP-INDIKATOREN FÜR KASPERSKY ANTI-VIRUS

IN DIESEM ABSCHNITT

LEISTUNGSINDIKATOREN

Tabelle 56. Leistungsindikatoren

INDIKATOREN	DEFINITION
currentRequestsAmount	Summe der Anfragen, die zur Verarbeitung weitergeleitet wurden (s. S. 154)
currentInfectedQueueLength	Summe der infizierten Objekte in Warteschlange für Verarbeitung (s. S. 156)
currentObjectProcessingRate	Summe der Objekte, die pro Sekunde verarbeitet werden (s. S. 156)
currentWorkProcessesAmount	Anzahl der Arbeitsprozesse von Kaspersky Anti-Virus, die momentan aktiv sind

ALLGEMEINE INDIKATOREN

Tabelle 57. Allgemeine Indikatoren

INDIKATOREN	DEFINITION
currentApplicationUptime	Arbeitszeit von Kaspersky Anti-Virus seit dem letzten Start, in Hundertstelsekunden
currentFileMonitorTaskStatus	Status der Aufgabe **Echtzeitschutz für Dateien**: **On** – wird ausgeführt; **Off** – wurde beendet oder angehalten.
currentScriptCheckerTaskStatus	Status der Aufgabe **Skript-Untersuchung**: **On** – wird ausgeführt; **Off** – wurde beendet oder angehalten.
lastCriticalAreasScanAge	Der seit der letzten Untersuchung der kritischen Serverbereiche vergangene Zeitraum (in Sekunden angegebener Zeitraum zwischen dem Abschluss einer Aufgabe mit dem Status "Aufgabe zur Untersuchung kritischer Bereiche" und dem gegenwärtigen Zeitpunkt)
licenseExpirationDate	Ablaufdatum der Lizenz. Wenn ein aktiver Schlüssel und ein Reserveschlüssel hinzugefügt wurden, wird das Ablaufdatum der Lizenz des Reserveschlüssels angezeigt.

UPDATE-INDIKATOREN

Tabelle 58. Update-Indikatoren

INDIKATOREN	DEFINITION
avBasesAge	"Alter" der Datenbanken (in Hundertstelsekunden angegebener Zeitraum zwischen Erscheinungsdatum der zuletzt installierten Datenbank-Updates und dem gegenwärtigen Zeitpunkt)

INDIKATOREN FÜR DEN ECHTZEITSCHUTZ

Tabelle 59. 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 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

INDIKATOREN	DEFINITION
totalObjectsQuarantined	Anzahl der infizierten oder möglicherweise infizierten Objekte, die von Kaspersky Anti-Virus in die Quarantäne verschoben wurden. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsNotQuarantined	Anzahl der infizierten oder möglicherweise infizierten Objekte, die Kaspersky Anti-Virus erfolglos versuchte, in die Quarantäne zu verschieben. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsDisinfected	Anzahl der infizierten Objekte, die von Kaspersky Anti-Virus desinfiziert wurden. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsNotDisinfected	Anzahl der infizierten Objekte, deren Desinfektion durch Kaspersky Anti-Virus fehlgeschlagen ist. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsDeleted	Anzahl der infizierten oder möglicherweise infizierten Objekte, die von Kaspersky Anti-Virus gelöscht wurden. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsNotDeleted	Anzahl der infizierten oder möglicherweise infizierten Objekte, die Kaspersky Anti-Virus erfolglos zu löschen versuchte. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsBackedUp	Anzahl der infizierten Objekte, die von Kaspersky Anti-Virus nach Backup verschoben wurden. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.
totalObjectsNotBackedUp	Anzahl der infizierten Objekte, die Kaspersky Anti-Virus erfolglos versuchte, nach Backup zu verschieben. Gezählt seit dem letzten Start der Aufgabe **Echtzeitschutz für Dateien**.

INDIKATOREN FÜR QUARANTÄNE

Tabelle 60. 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 61. Indikatoren für Backup

INDIKATOREN	DEFINITION
currentBackupStorageSize	Volumen der Daten im Backup-Ordner (MB)

INDIKATOREN FÜR DIE SKRIPT-UNTERSUCHUNG

Tabelle 62. Indikatoren für die Skript-Untersuchung

INDIKATOREN	DEFINITION
totalScriptsProcessed	Anzahl der untersuchten Skripts
totalInfectedIDangerousScriptsFound	Summe der erkannten gefährlichen Skripts
totalSuspiciousScriptsFound	Summe der erkannten potenziell gefährlichen Skripts
totalScriptsBlocked	Anzahl der Skripts, auf die der Zugriff blockiert wurde.

SNMP-TRAPS

Die Parameter der SNMP-Traps für Kaspersky Anti-Virus werden in nachstehender Tabelle beschrieben.

Tabelle 63. SNMP-Traps für Kaspersky Anti-Virus

SCHWACHSTELLE	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 den Parameter **Maximale Größe des Backups festgelegt ist.** Kaspersky Anti-Virus reserviert weiter infizierte Objekte.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Maximale Größe des Backups ist erreicht. Die Größe des freien Speicherplatzes im Backup-Ordner, die in der Einstellung **Grenzwert für verfügbaren Speicherplatz**, eingegeben wurde, ist auf den angegebenen Wert gesunken. Kaspersky Anti-Virus reserviert weiter 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** festgelegt ist. Kaspersky Anti-Virus verschiebt weiter möglicherweise infizierte Objekte in die Quarantäne.	eventDateAndTime eventSeverity eventSource

SCHWACHSTELLE	BESCHREIBUNG	EINSTELLUNGEN
eventThresholdQuarantineStorageSizeExceeds	Maximale Größe der Quarantäne ist erreicht. Die Größe des freien Speicherplatzes im Quarantäne-Ordner, die mit dem Parameter Grenzwert für freien Speicherplatz in Quarantäne eingegeben wurde, ist auf den angegebenen Wert gesunken. Kaspersky Anti-Virus verschiebt weiter möglicherweise infizierte Objekte in die Quarantäne.	eventDateAndTime eventSeverity eventSource
eventObjectNotQuarantined	Fehler beim Verschieben des Objekts in die Quarantäne.	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	Es ist ein Fehler mit der Quarantäne aufgetreten.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Es ist ein Fehler mit dem Backup aufgetreten.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	Datenbanken sind veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Update der Datenbanken zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).	eventSeverity eventDateAndTime eventSource days
eventAVBasesTotallyOutdated	Datenbanken sind stark veraltet. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe zum Update der Datenbanken zum letzten Mal abgeschlossen wurde (lokale Aufgabe, Gruppenaufgabe oder Aufgabe für Zusammenstellungen von Computern).	eventSeverity eventDateAndTime eventSource days

SCHWACHSTELLE	BESCHREIBUNG	EINSTELLUNGEN
eventApplicationStarted	Kaspersky Anti-Virus wurde gestartet.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Anti-Virus wurde beendet.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	Untersuchung kritischer Bereiche liegt lange zurück. Es werden die Tage gezählt, die vergangen sind, seit die Aufgabe mit dem Status "Aufgabe zur Untersuchung kritischer Bereiche" zum letzten Mal abgeschlossen wurde.	eventSeverity eventDateAndTime eventSource days
eventLicenseHasExpired	Die Gültigkeitsdauer der Lizenz ist abgelaufen.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	Die Gültigkeitsdauer der Lizenz läuft bald ab. 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 Aufgabe zum Update	eventSeverity eventDateAndTime taskName updaterErrorEventReason

In der folgenden Tabelle werden die Trap-Parameter und die entsprechenden Parameterwerte beschrieben.

Tabelle 64. Parameterwerte von SNMP-Traps

EINSTELLUNGEN	BESCHREIBUNG UND MÖGLICHE WERTE
eventDateAndTime	Zeitpunkt, zu dem ein Ereignis eingetreten ist.
eventSeverity	Prioritätsstufe des Ereignisses. Der Parameter nimmt die folgenden Werte an: • critical (1) – kritisch • warning (2) – Warnung • info (3) – informativ
UserName	Benutzername (z.B. des Benutzers, der versucht hat, Zugriff auf eine infizierte Datei zu erhalten).
computerName	Computername (beispielsweise des Computers, von dem versucht wurde, Zugriff auf eine infizierte Datei zu bekommen)

EINSTELLUNGEN	BESCHREIBUNG UND MÖGLICHE WERTE
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) – Virensuche • product (7) – Ereignis, das nichts mit einzelnen Komponenten, sondern mit Kaspersky Anti-Virus als Ganzem zu tun hat. • systemAudit (8) – Systemaudit-Bericht; • nasProtection (10) – Schutz von Netzwerkspeichern
eventReason	Grund für Ereigniseintritt. Der Parameter nimmt die folgenden Werte an: • reasonUnknown (0) – 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 Quarantäne-Einstellungen falsch angegeben, z.B. ein Netzwerkpfad wurde angegeben). In diesem Fall verwendet Kaspersky Anti-Virus den standardmäßigen Backup- Ordner oder Quarantäne-Ordner.
objectName	Objektname (beispielsweise Name der Datei, in der eine Bedrohung gefunden wurde).
threatName	Name des gefundenen Objekts gemäß der Klassifizierung der Viren-Enzyklopädie (http://www.securelist.com/de/). Dieser Name gehört zur vollständigen Bezeichnung des gefundenen Objekts, die Kaspersky Anti-Virus beim Fund des Objekts zurückgibt. Sie können den vollständigen Namen des gefundenen Objekts im Bericht über die Aufgabenausführung anzeigen (s. Abschnitt "Statistiken und Informationen über eine Aufgabe von Kaspersky Anti-Virus in den Berichten über die Aufgabenausführung anzeigen" auf S. 99).
detectType	Typ des gefundenen Objekts. Der Parameter nimmt die folgenden Werte an: • undefined (0) – nicht definiert • virware – klassische Viren und Netzwerkwürmer • trojware – trojanische Programme • malware – sonstige Schadprogramme • 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 Anti-Virus hat erkannt, dass ein Codeabschnitt des Objekts teilweise mit einem bekanntem Schadcode übereinstimmt. • Sure (infiziert)– Kaspersky Anti-Virus 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).

EINSTELLUNGEN	BESCHREIBUNG UND MÖGLICHE WERTE
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 – Der Dienst ist nicht verfügbar. • reasonConnectionError – Verbindungsfehler • reasonModuleNotFound – Das Objekt wurde nicht gefunden. • reasonBlstCheckFailed(16) – Fehler beim Überprüfen der schwarzen Schlüsselliste. Möglicherweise wurde während des Update-Vorgangs Datenbank-Updates veröffentlicht. Wiederholen Sie bitte das Update in einigen Minuten. Beachten Sie die Beschreibung der Gründe und die möglichen Aktionen des Administrators auf der Seite des Technischen Kundendienstes im Pkt. "Wenn das Programm einen Fehler ausgegeben hat" (http://support.kaspersky.com/de/error).
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 reparieren Sie Kaspersky Anti-Virus. • reasonStorageReadOnly – Die Datenbank steht nur zum Lesen zur Verfügung. Bitte reparieren Sie Kaspersky Anti-Virus. • reasonStorageIOError – Ein-/Ausgabefehler: a) Kaspersky Anti-Virus wurde beschädigt. Bitte reparieren Sie Kaspersky Anti-Virus. b) Das Laufwerk, auf dem die Dateien von Kaspersky Anti-Virus gespeichert sind, ist beschädigt. • reasonStorageCorrupted – Der Speicher ist beschädigt. Bitte reparieren Sie Kaspersky Anti-Virus. • reasonStorageFull – Die Datenbank ist voll. Bitte geben Sie Speicherplatz auf dem Datenträger frei. • reasonStorageOpenError – Die Datenbankdatei konnte nicht geöffnet werden. Bitte reparieren Sie Kaspersky Anti-Virus. • reasonStorageOSFeatureError – Einige Besonderheiten des Betriebssystems entsprechen den Anforderungen für Kaspersky Anti-Virus nicht. • reasonObjectNotFound – Das in den Speicher 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 beschreibt die Möglichkeiten für die technische Unterstützung und die Support-Richtlinien.

IN DIESEM ABSCHNITT

ÜBER TECHNISCHEN SUPPORT

Wenn Sie keine Lösung für Ihr Problem in der Dokumentation oder in anderen Informationsquellen zum Programm gefunden haben, empfehlen wir Ihnen, den technischen Support von Kaspersky Lab 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 (http://support.kaspersky.com/de/support/rules).

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Telefonische Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Anfrage an den Technischen Support von Kaspersky Lab über den Webdienst Kaspersky CompanyAccount senden.

TECHNISCHER SUPPORT ÜBER DAS KASPERSKY COMPANYACCOUNT

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) ist ein Webservice für Unternehmen, die Kaspersky-Lab-Programme verwenden. Der Webdienst von Kaspersky CompanyAccount ist für die Interaktion der Benutzer mit den Spezialisten von Kaspersky Lab mithilfe elektronischer Anfragen vorgesehen. Im Webdienst Kaspersky CompanyAccount kann der Status der Verarbeitung elektronischer Anfragen durch Kaspersky Lab-Spezialisten zurückverfolgt sowie die 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.

Der Webdienst Kaspersky CompanyAccount ist in folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch

- Russisch
- Französisch
- Japanisch

Mehr über Kaspersky CompanyAccount erfahren Sie auf der Webseite des Technischen Supports (http://support.kaspersky.com/de/faq/companyaccount_help).

TECHNISCHER SUPPORT AM TELEFON

Bei dringenden Problemen können Sie die Spezialisten vom Technischen Support von Kaspersky Lab telefonisch kontaktieren. (http://support.kaspersky.com/de/support/contacts).

Bitte machen Sie sich mit den Regeln für die Nutzung des Technischen Supports vertraut, bevor Sie sich an den Technischen Support wenden (http://support.kaspersky.com/de/support/rules). Die Regeln enthalten Informationen darüber, zu welchen Zeiten Sie beim Technischen Support von Kaspersky Lab anrufen können und welche Daten die Spezialisten des Technischen Supports benötigen, um Ihnen helfen zu können.

PROTOKOLLDATEI UND AVZ-SKRIPT VERWENDEN

Wenn Sie sich mit einem Problem an die Support-Experten von Kaspersky Lab wenden, werden Sie möglicherweise darum gebeten, einen Bericht über Kaspersky Anti-Virus zu erstellen und den Bericht an den Kaspersky-Lab-Support zu schicken. Die Support-Experten von Kaspersky Lab können zusätzlich 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 Support-Experten 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 bzw. gelöscht, und ein Ergebnisbericht über die 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 Sammlung 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 gesammelter Diagnosedaten.
- Konfiguration der Überwachung und Speicherung des Netzwerkverkehrs in einer Datei.

GLOSSAR

A

ADMINISTRATIONSAGENT

Programmkomponente von Kaspersky Security Center, die für die Interaktion zwischen dem Administrationsserver und den auf einem bestimmten Netzwerkknoten (Workstation oder Server) installierten Programmen von Kaspersky Lab zuständig ist. Die entsprechenden Komponente ist für alle Windows Programme aus dem Produktsortiment des Unternehmens eindeutig.

ADMINISTRATIONSGRUPPE

Zusammenstellung von Computern, die entsprechend der ausgeführten Funktionen und der auf ihnen installierten Programme von Kaspersky Lab zusammengefasst sind. Die Computer werden zusammengefasst, damit Sie gemeinsam bequemt wie eine Einheit verwaltet werden können. Zu einer Gruppe können andere Gruppen gehören. Für jedes der in der Gruppe installierten Programme können eine Gruppenrichtlinie und Gruppenaufgaben erstellt werden.

ADMINISTRATIONSSERVER

Programmkomponente von Kaspersky Security Center, mit der die zentralisierte Speicherung von Informationen über die im Unternehmensnetzwerk installierten Programme von Kaspersky Lab sowie deren Verwaltung realisiert wird.

AKTIVER SCHLÜSSEL

Schlüssel, der im Augenblick für die Programmausführung verwendet wird.

ANTIVIREN-DATENBANKEN

Datenbanken mit Informationen über Computer-Bedrohungen, die Kaspersky Lab beim Erscheinen der Antiviren-Datenbanken bekannt sind. 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

Datei, die in sich eine oder mehrere Dateien "enthält", die selbst wiederum Archive sein können.

AUFGABE

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben implementiert sind: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbanken-Update.

AUFGABENEINSTELLUNGEN

Einstellungen für die Programmausführung, die für den jeweiligen Aufgabentyp gelten.

AUTOSTART-OBJEKTE

Auswahl von Programmen, die für den Start und die ordnungsgemäße Ausführung des auf Ihrem Computer installierten Betriebssystems und der Software. Diese Objekte werden bei jedem Start des Betriebssystems gestartet. Es gibt Viren, die genau diese Objekte infizieren können, was beispielsweise dazu führen kann, dass das Betriebssystem nicht gestartet wird.

B

BACKUP

Spezieller Speicher für die Aufbewahrung von Sicherungskopien der Dateien, die vor deren erster Desinfizierung oder Löschung erstellt werden.

D

DATEIMASKE

Darstellung der Bezeichnung und Erweiterung einer Datei durch ein allgemeines Symbol.

Zur Erstellung einer Dateimaske können beliebige Symbole verwenden werden, die für die Dateibezeichnung verfügbar sind, darunter auch Sonderzeichen:

- * – Symbol, das anstelle von Null oder mehr als Null beliebigen Zeichen steht.
- ? – Symbol, das für genau ein beliebiges Zeichen steht.

Bitte beachten Sie, dass Bezeichnung und Erweiterung einer Datei immer durch einen Punkt verbunden sein müssen.

DESINFEKTION DER OBJEKTE

Verarbeitungsmethode für infizierte Objekte, die eine vollständige oder teilweise Wiederherstellung der Daten zum Ergebnis hat. Nicht alle infizierten Objekte können desinfiziert werden.

F

FEHLALARM

Situation, in der ein nicht infiziertes Objekt von einem Programm von Kaspersky Lab als infiziert eingestuft wird, weil sein Code an einen Viruscode erinnert.

H

HEURISTISCHE ANALYSE

Technologie zur Erkennung von Bedrohungen, die mithilfe der aktuellen Version der Programm-Datenbanken von Kaspersky Lab nicht bestimmt werden können. Erlaubt das Auffinden von Dateien, die möglicherweise einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus enthalten.

Dateien, in denen während der heuristischen Analyse Schadcode erkannt wurde, erhalten den Status möglicherweise infiziert.

HEURISTISCHE ANALYSE

Modul von Kaspersky Anti-Virus, das die heuristische Analyse durchführt.

I

INFIZIERBARE DATEI

Datei, die Kraft 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 hierbei um ausführbare Dateien mit den Erweiterungen com, exe, dll u. a. Das Risiko eines Eindringens von schädlichem Code in solche Dateien ist ausreichend hoch.

INFIZIERTE DATEI

Datei, innerhalb derer sich schädlicher Code befindet (bei der Untersuchung der Datei wurde Code eines bekannten Programms gefunden, das eine Bedrohung darstellt). Die Experten von Kaspersky Lab empfehlen, nicht mit solchen Dateien zu arbeiten, da dies zu einer Infizierung Ihres Computers führen könnte.

M

MÖGLICHERWEISE INFIZIERTE DATEI

Datei, innerhalb derer sich entweder modifizierter Code eines bekannten Virus, oder Code, der an einen Virus erinnert, bis jetzt jedoch Kaspersky Lab nicht bekannt war, befindet. Möglicherweise infizierte Dateien werden mithilfe der heuristischen Analyse gefunden.

O

OLE-OBJEKT

Datei, die mit einer anderen Datei verbunden oder in ihr integriert ist. Die Programme von Kaspersky Lab ermöglichen eine Untersuchung auf Viren in OLE-Objekten. Wenn Sie beispielsweise eine bestimmte Microsoft Office Excel® - Tabelle in ein Microsoft Office Word-Dokument einfügen, wird diese Tabelle als OLE-Objekt untersucht.

P

PROGRAMMEINSTELLUNGEN

Einstellungen für die Programmfunktionen, die für alle Aufgabentypen gelten und sich auf die allgemeine Programmfunktion beziehen. Beispiele: Leistungseinstellungen für das Programm, Einstellungen für die Berichtsführung, Backup-Einstellungen.

Q

QUARANTÄNE

Ordner, in den möglicherweise infizierte Objekte verschoben werden, die Kaspersky Anti-Virus findet. Dateien werden in der Quarantäne in verschlüsselter Form gespeichert, um eine Gefährdung des Computers auszuschließen.

R

RESERVESCHLÜSSEL

Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist.

S

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 im Betriebssystem macht es unsicher, da Viren, die in das Betriebssystem eindringen, Abstürze sowohl des Betriebssystems selbst als auch der installierten Programme hervorrufen können.

SIGNATURANALYSE

Technologie zum Erkennen von Bedrohungen, die die Datenbanken in Kaspersky Anti-Virus verwendet, welche eine Beschreibung der bekannten Bedrohungen und Methoden für ihre Beseitigung enthalten. Ein Schutz mithilfe der Signaturanalyse gewährleistet die minimal erforderliche Sicherheitsstufe. Gemäß der Empfehlung der Experten von Kaspersky Lab ist diese Methode immer aktiviert.

U

UPDATE

Vorgang des Austauschens bzw. Hinzufügens von neuen Dateien (Datenbanken oder Programm-Module), die vom Update-Server von Kaspersky Lab stammen.

KASPERSKY LAB

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Schadsoftware, Spam, Netzwerk- und Hackerangriffen schützen.

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 einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

PRODUKTE. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Programme für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert*, *die Anti-Spam-Datenbanken im 5-Minuten-Takt*.

TECHNOLOGIEN. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Großbritannien), CommuniGate Systems (USA), Openwave Messaging (Irland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), Netasq+Arkoon (Frankreich), NETGEAR (USA), Parallels (USA), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). 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 wurde Kaspersky Anti-Virus 2010 in Tests des renommierten österreichischen Antiviren-Labors AV-Comparatives mehrfach mit dem Premium-Award Advanced+ 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 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	http://www.kaspersky.com/de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Viren-Labor:	newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN

Informationen zu fremden Codes finden Sie in der Datei legal_notices.txt, die sich im Installationsordner des Programms befindet.

MARKENHINWEISE

SACHREGISTER

M

O

P

Q

R

S

T

Ü

U

V

W

Z