Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition

Installationshandbuch

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 Handbuch für die Implementierung von 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.

Die Informationen in diesem Handbuch beziehen sich auf folgende 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

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

IN DIESEM ABSCHNITT

IN DIESEM DOKUMENT

Das Installationshandbuch für Kaspersky Anti-Virus enthält folgende Abschnitte.

Informationsquellen zum Programm

Dieser Abschnitt enthält die Beschreibung der Informationsquellen zum Programm.

Hard- und Software-Voraussetzungen

Dieser Abschnitt enthält eine Liste der Hardware- und Softwarevoraussetzungen für Kaspersky Anti-Virus.

Kaspersky Anti-Virus

In diesem Abschnitt werden die Funktionen und Komponenten von Kaspersky Anti-Virus beschrieben.

Installation planen

Dieser Abschnitt beschreibt die Administrations-Tools für Kaspersky Anti-Virus sowie die Besonderheiten, die bei der Installation von Kaspersky Anti-Virus mit folgenden Methoden gelten: mithilfe des Setup-Assistenten, aus der Befehlszeile, über Kaspersky Security Center und über Active Directory®-Gruppenrichtlinien.

Installation und Deinstallation von Kaspersky Anti-Virus mit dem Assistenten

Hier wird beschrieben, wie Kaspersky Anti-Virus und die Konsole für Kaspersky Anti-Virus mithilfe des Setup-Assistenten auf einem geschützten Server installiert und vom Server entfernt werden. Außerdem finden Sie hier Informationen über erweiterte Einstellungen für Kaspersky Anti-Virus und über die Aktionen, die nach der Installation von Kaspersky Anti-Virus erforderlich sind.

Installation und Deinstallation von Kaspersky Anti-Virus aus der Befehlszeile

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

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

Dieser Abschnitt bietet allgemeine Informationen zur Installation von Kaspersky Anti-Virus über Kaspersky Security Center, eine Beschreibung des Vorgehens für die Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center, sowie eine Beschreibung der Aktionen, die nach der Installation von Kaspersky Anti-Virus erforderlich sind.

Installation und Deinstallation von Kaspersky Anti-Virus über Gruppenrichtlinien von Active Directory

Dieser Abschnitt bietet eine Beschreibung der Installation und Deinstallation von Kaspersky Anti-Virus über Active Directory-Gruppenrichtlinien, sowie Informationen über die Aktionen, die nach der Installation von Kaspersky Anti-Virus über Active Directory-Gruppenrichtlinien erforderlich sind.

Upgrade einer Vorgängerversion des Programms

Dieser Abschnitt informiert darüber, welche Einstellungen für installierte Programme in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 gespeichert werden, wie diese Einstellungen heißen und welche Werte diese Einstellungen nach der Migration annehmen.

Einstellungen von Kaspersky Anti-Virus prüfen. Verwendung des EICAR-Testvirus

Dieser Abschnitt beschreibt den EICAR-Testvirus und das Vorgehen, mit dem die Kaspersky Anti-Virus-Funktionen "Echtzeitschutz" und "Untersuchung auf Befehl" mithilfe des EICAR-Testvirus überprüft werden.

Kontaktaufnahme mit dem Technischen Support

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

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

In diesem Abschnitt werden Informationsquellen zum Programm beschrieben.Sie können je nach Dringlichkeit und Wichtigkeit 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) können Sie allgemeine Informationen über das Programm, seine Funktionsmöglichkeiten und -besonderheiten bekommen.

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.

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 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.

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

PROGRAMMKOMPONENTEN VON KASPERSKY ANTI-VIRUS UND IHRE CODES FÜR DEN DIENST WINDOWS INSTALLER.

Die Datei \server\kavws.msi installiert standardmäßig alle Programmkomponenten von Kaspersky Anti-Virus, unter Ausnahme der **Skript-Untersuchung** (Script Checker). Die Installation dieser Komponente kann bei der benutzerdefinierten Programminstallation ausgewählt werden (s. Abschnitt Installation von Kaspersky Anti-Virus auf dem geschütztem Server).

Die Datei \client\kavwstools.msi installiert alle Programmkomponenten des Satzes "Administrationswerkzeuge".

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

IN DIESEM ABSCHNITT

PROGRAMMKOMPONENTEN VON KASPERSKY ANTI-VIRUS

Die folgende Tabelle enthält die Codes und eine Beschreibung der Programmkomponenten für Kaspersky Anti-Virus

Tabelle 2. Beschreibung der Programmkomponenten von Kaspersky Anti-Virus

KOMPONENTE	CODE	FUNKTION
Virensuche	core	Installiert Systemdateien von Kaspersky Anti-Virus und Dateien, die die Aufgaben zur Untersuchung auf Befehl (Untersuchung von Objekten des geschützten Servers) erledigen. Wenn Sie beim Installieren des Anti-Virus aus der Befehlszeile andere Komponenten von Kaspersky Anti-Virus angeben, ohne die Core-Komponente zu nennen, wird die Core-Komponente automatisch installiert.
Echtzeitschutz für Dateien	Oas	Umsetzung der Aufgabe **Echtzeitschutz für Dateien** (Untersuchung von Objekten des geschützten Servers bei Zugriff auf diese Dateien).
ICAP: Schutz von Netzwerkspeichern.	ICAPStorageProtection	Realisiert die Aufgabe **ICAP: Schutz von Netzwerkspeichern** (wenn Client-Computer versuchen, Dateien zu lesen oder zu ändern, die sich in den Netzwerkfreigaben (network share) von Netzwerkspeichern befinden, die per ICAP-Protokoll verbunden werden, werden diese Dateien von Kaspersky Anti-Virus untersucht).
RPC: Schutz von Netzwerkspeichern.	NetApp	Realisiert die Aufgabe **RPC: Schutz von Netzwerkspeichern** (wenn Client-Computer versuchen, Dateien zu lesen oder zu ändern, die sich in den Netzwerkfreigaben (network share) von Netzwerkspeichern befinden, die per RPC-Protokoll verbunden werden, werden diese Dateien von Kaspersky Anti-Virus untersucht).
Skript-Untersuchung	ScriptChecker	Umsetzung der Aufgabe **Skript-Untersuchung** (Untersuchung des Programmcodes von Skripts, die mit Microsoft Windows Script Technologies erstellt worden sind, wenn versucht wird, sie auszuführen).
Modul für die Integration in den Administrationsagenten von Kaspersky Security Center	AKIntegration	Koordination der Verbindung von Kaspersky Anti-Virus mit dem Administrationsagenten von Kaspersky Security Center. Installieren Sie diese Komponente auf dem geschützten Server, wenn Sie vorhaben, Anti-Virus über Kaspersky Security Center zu verwalten.
Satz von Produktivitäts-Countern der Anwendung "Systemmonitor"	PerfMonCounters	Fügt einen Satz von Leistungsindikatoren der Anwendung "Systemmonitor" ein. Die Leistungsindikatoren messen die Leistungsfähigkeit von Kaspersky Anti-Virus und finden mögliche Engpässe bei gleichzeitiger Ausführung von Kaspersky Anti-Virus und anderen Programme.
Counter und SNMP-Schwachstellen	SnmpSupport	Veröffentlicht die Indikatoren und Traps für Kaspersky Anti-Virus über den Dienst Simple Network Management Protocol (SNMP) von Microsoft Windows. Sie können diese Komponente auf dem geschützten Server nur installieren, wenn der Service Microsoft SNMP auf dem Server installiert ist.
Symbol für Kaspersky Anti-Virus	TrayApp	Anzeige des Kaspersky Anti-Virus-Symbols im Infobereich der Taskleiste des geschützten Servers. Das Kaspersky Anti-Virus-Symbol zeigt den Status des Echtzeitschutzes auf dem Server an, erlaubt es, die Konsole von Kaspersky Anti-Virus (falls installiert) und das Fenster **Über das Programm** zu öffnen.
Befehlszeilen-Utility	Shell	Erlaubt die Verwaltung von Kaspersky Anti-Virus über die Befehlszeile des geschützten Servers.

PROGRAMMKOMPONENTEN DER "ADMINISTRATIONS-TOOLS"

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

Tabelle 3. Beschreibung der Programmkomponenten des Satzes Administrationswerkzeuge

KOMPONENTE	CODE	FUNKTION
Snap-in von Kaspersky Anti-Virus	MmcSnapin	Installiert das Microsoft Management Console Snap-in für die Verwaltung über die Konsole von Kaspersky Anti-Virus. Wenn Sie beim Installieren eines Satzes der Administrationswerkzeuge aus der Befehlszeile andere Satz-Komponenten angeben, ohne die MmcSnapin-Komponente zu nennen, wird die MmcSnapin-Komponente automatisch installiert.
Hilfe	Help	chm-Datei der Hilfe. Die Datei befindet sich im Ordner mit den Dateien von Kaspersky Anti-Virus. Sie können die Hilfe-Datei aus dem Menü **Start** öffnen.
Dokumentation	Docs	Die PDF-Dokumente "Administratorhandbuch", "Installationshandbuch" und "Handbuch zur Software-Verteilung" sind im Ordner von Kaspersky Anti-Virus gespeichert. Das "Administratorhandbuch" kann aus dem **Startmenü** geöffnet werden.

BERICHT ÜBER INSTALLATION UND DEINSTALLATION VON KASPERSKY ANTI-VIRUS

Wenn Sie die Installation oder Deinstallation von Kaspersky Anti-Virus mit Hilfe des Assistenten zur Installation (Deinstallation) ausführen, erstellt der Dienst Windows Installer einen Bericht über die Installation (Deinstallation). Die Berichtsdatei mit dem Namen kav8wsee_install_<uid>.log (wobei <uid> – einmalige achtstellige ID des Berichts) wird im Ordner %temp% des Benutzers gespeichert, mit dessen Rechten der Installationsassistent gestartet wurde.

Wenn Sie die Installation oder Deinstallation von Kaspersky Anti-Virus aus der Befehlszeile ausführen, wird in der Grundeinstellung kein Installationsbericht erstellt.

- *Damit bei der Installation von Kaspersky Anti-Virus die Berichtsdatei kavws.log auf dem Laufwerk C:\ angelegt wird, geben Sie folgenden Befehl ein:*

```
msiexec /i kavws.msi /l*v C:\kavws.log /qn EULA=1
```

PARAMETER FÜR INSTALLATION UND DEINSTALLATION SOWIE DEREN SCHLÜSSEL FÜR DEN DIENST WINDOWS INSTALLER

In den folgenden Tabellen werden die Parameter für die Installation und Deinstallation von Kaspersky Anti-Virus und deren Standardwerte beschrieben. Außerdem werden spezielle Schlüssel für die Änderung der Parameterwerte und deren mögliche Werte erläutert. Sie können diese Schlüssel gemeinsam mit den Standardschlüsseln des Befehls msiexec des Dienstes Windows Installer verwenden, wenn Kaspersky Anti-Virus aus der Befehlszeile installiert wird.

Tabelle 4. Installationsparameter und deren Schlüssel in Windows Installer

EINSTELLUNGEN	STANDARDWERT	SCHLÜSSEL VON WINDOWS INSTALLER UND DESSEN WERTE	BESCHREIBUNG
Bedingungen des Lizenzvertrags akzeptieren	Bedingungen des Lizenzvertrags ablehnen	EULA=<Wert> **0** – Sie lehnen die Bedingungen des Lizenzvertrags ab. **1** – Sie akzeptieren die Bedingungen des Lizenzvertrags.	Um Kaspersky Anti-Virus zu installieren, müssen Sie die Bedingungen des Lizenzvertrags akzeptieren.
Untersuchung von aktiven Prozessen und von Bootsektoren auf lokalen Datenträgern vor der Installation (**Computer auf Viren untersuchen**)	Untersuchung nicht ausführen	PRESCAN=<Wert> **0** – Untersuchung vor der Installation nicht ausführen; **1** – Untersuchung vor der Installation ausführen.	Es wird empfohlen, die Untersuchung von aktiven Prozessen und von Bootsektoren auf lokalen Datenträgern vor der Installation auszuführen, da Malware in diesen Computerbereichen eine erfolgreiche Installation von Kaspersky Anti-Virus stören kann. Die Untersuchung kann einige Minuten dauern. Wenn während der Untersuchung infizierte oder möglicherweise infizierte Prozesse erkannt werden, werden sie aus dem Arbeitsspeicher des Computers gelöscht (ausführbare Prozessdateien werden nicht gelöscht). In diesem Fall können Daten in den laufenden Anwendungen verloren gehen. Aus diesem Grund wird geraten, vor der Installation alle laufenden Anwendungen zu schließen.
Zielordner	Kaspersky Anti-Virus: %Program Files%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Administrationswerkzeuge: %Program Files%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Admins Tools In der 64-Bit-Version von Microsoft Windows heißt der Ordner %ProgramFiles(x86)%	INSTALLDIR=<Vollständiger Pfad zum Ordner>	Ordner, in dem die Dateien für Kaspersky Anti-Virus bei der Installation gespeichert werden. Sie können einen anderen Ordner angeben.
Echtzeitschutz für Dateien und Skript-Untersuchung beim Start von Kaspersky Anti-Virus starten (**Echtzeitschutz nach der Installation des Programms aktivieren**)	Starten	RUNRTP=<Wert> **1** – starten **0** – nicht starten	Aktivieren Sie diesen Parameter, damit der Echtzeitschutz für Dateien und die Skript-Untersuchung beim Start von Kaspersky Anti-Virus gestartet werden (empfohlen).

EINSTELLUNGEN	STANDARDWERT	SCHLÜSSEL VON WINDOWS INSTALLER UND DESSEN WERTE	BESCHREIBUNG
Untersuchungsausnahmen, die von der Firma Microsoft empfohlen werden (**Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen**)	Ausschließen	ADDMSEXCLUSION=<Wert> **1** – ausschließen **0** – nicht ausschließen	In der Aufgabe **Echtzeitschutz für Dateien** werden Objekte auf dem Server aus dem Schutzbereich ausgeschlossen, deren Ausschluss die Firma Microsoft empfiehlt (empfohlen). Einige Anwendungen auf dem Server laufen möglicherweise nicht stabil, wenn Antiviren-Anwendungen Dateien abfangen oder ändern, auf die diese Programme zugreifen. Zu solchen Programmen zählt Microsoft beispielsweise einige Anwendungen wie Domain-Controller.
Untersuchungsausnahmen, die von Kaspersky Lab empfohlen werden (**Ausnahmen berücksichtigen, die Kaspersky Lab empfiehlt**)	Ausschließen	ADDKLEXCLUSION=<Wert> **1** – ausschließen **0** – nicht ausschließen	In der Aufgabe **Echtzeitschutz für Dateien** werden Objekte auf dem Server aus dem Schutzbereich ausgeschlossen, deren Ausschluss die Kaspersky Lab empfiehlt (empfohlen).
Ausnahme von der Bearbeitung der Programme zur Remote-Administration (**Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen**)	Objekte nach der Maske not-a-virus:RemoteAdmin* nicht zu Ausnahmen hinzufügen	RADMINEXCLUSION=<Wert> 1 – Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen. 0 – Objekte nach der Maske not-a-virus:RemoteAdmin* nicht zu Ausnahmen hinzufügen.	Wenn Sie die Utility Remote Administrator starten, erkennt Kaspersky Anti-Virus in ihr eine Möglichkeit der Verwendung durch Angreifer und löscht das ausführbare Modul vom Datenträger des Servers. Kaspersky Anti-Virus gibt diesen Objekten den Namen mit der Maske: not-a-virus:RemoteAdmin*. Wenn Sie vorhaben, nach der Installation von Kaspersky Anti-Virus Utilities zur Remote-Administration einzusetzen, können Sie das angegebene Objekt mit dem Installationsparameter **Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen** von der Anti-Virus-Bearbeitung ausschließen. Sie können Hilfsprogramme für die Remote-Administration von der Verarbeitung in der Aufgabe **Echtzeitschutz für Dateien** und in den Aufgaben zur **Untersuchung auf Befehl** und auch nach Installation des Kaspersky Anti-Virus ausschließen (s. *Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition.. Administratorhandbuch*).

EINSTELLUNGEN	STANDARDWERT	SCHLÜSSEL VON WINDOWS INSTALLER UND DESSEN WERTE	BESCHREIBUNG
Pfad der Schlüsseldatei (**Schlüssel**)	Ordner im Lieferumfang \server	LICENSEKEYPATH=<Pfad der Schlüsseldatei>	Das Installationsprogramm sucht standardmäßig in dem im Lieferumfang enthaltenen Ordner \server nach einer Schlüsseldatei mit der Erweiterung .key. Wenn der Ordner \server mehrere Schlüsseldateien enthält, wählt das Installationsprogramm die Datei, deren Schlüssel die längste Gültigkeitsdauer aufweist. Sie können die Schlüsseldatei zuvor im Ordner \server\ speichern oder mit dem Installationsparameter **Schlüssel hinzufügen** einen anderen Pfad für die Schlüsseldatei angeben. Sie können den Schlüssel während der Installation von Kaspersky Anti-Virus hinzufügen, mithilfe der von Ihnen gewählten Administrationswerkzeuge, zum Beispiel mit der Konsole von Kaspersky Anti-Virus. Beachten Sie jedoch, wenn Sie während der Installation keinen Schlüssel für Kaspersky Anti-Virus hinzufügen, ist Kaspersky Anti-Virus nach der Installation nicht funktionstüchtig. Details über die Lizenzierung von Anti-Virus finden Sie im Dokument "*Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition. Administratorhandbuch*".
Pfad der Konfigurationsdatei	Nicht festgelegt	CONFIGPATH=<Pfad der Schlüsseldatei>	Kaspersky Anti-Virus importiert die Einstellungen aus der angegebenen Konfigurationsdatei, die in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition erstellt wurde. Kennwörter, wie z.B. Kennwörter von Benutzerkonten für den Start von Aufgaben oder Kennwörter für die Verbindung mit einem Proxyserver, werden von Kaspersky Anti-Virus nicht aus der Konfigurationsdatei importiert. Nach dem Import der Parameter müssen alle Kennwörter manuell eingegeben werden. Wenn Sie die Konfigurationsdatei nicht angeben, beginnt Anti-Virus nach der Installation mit den Standardparametern zu arbeiten.

EINSTELLUNGEN	STANDARDWERT	SCHLÜSSEL VON WINDOWS INSTALLER UND DESSEN WERTE	BESCHREIBUNG
Netzwerkverbindungen für die Anti-Virus-Konsole erlauben	Ausgeschaltet	ADDWFEXCLUSION=<Wert> **1** – erlauben **0** – nicht erlauben	Sie können diesen Parameter verwenden, wenn Sie Kaspersky Anti-Virus nicht auf dem geschützten Server, sondern auf einem anderen Computer installieren. Mit Hilfe dieser Konsole können Sie den Schutz fernsteuern. Auf dem Computer wird in der Firewall von Microsoft Windows der TCP-Port 135 geöffnet, Netzwerkverbindungen für die ausführbare Datei kavfsrcn.exe werden erlaubt (Prozess zur Fernverwaltung von Kaspersky Anti-Virus) und der Zugriff auf DCOM-Programme wird zugelassen. Nachdem die Installation abgeschlossen wurde, fügen Sie die Benutzer, die zur Fernverwaltung von Anti-Virus berechtigt werden sollen, auf dem Server zur Gruppe **KAVWSEE Administrators** hinzu und, wenn der Server unter Microsoft Windows Server 2008 läuft, erlauben Sie auf dem Server Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus (Datei kavfsgt.exe). Sie können nachlesen, wie Zusatzeinstellungen bei Installation der Anti-Virus-Konsole auf einem anderen Computer vorzunehmen sind (s. S. 29).

Tabelle 5. Deinstallationsparameter und deren Schlüssel in Windows Installer

EINSTELLUNGEN	STANDARDWERT	BESCHREIBUNG, SCHLÜSSEL VON WINDOWS INSTALLER UND DEREN WERTE
Wiederherstellung des Quarantäne-Inhalts	Löschen	RESTOREQTN =<Wert> **0** – Quarantäne-Inhalt löschen **1** – Inhalt der Quarantäne in dem Ordner wiederherstellen, der mit dem Parameter RESTOREPATH vorgegeben ist.
Wiederherstellen des Backup-Inhalt	Löschen	RESTOREBCK =<Wert> **0** – Backup-Inhalt löschen **1** – Inhalt des Backups in dem Ordner wiederherstellen, der mit dem Parameter RESTOREPATH vorgegeben ist.
Ordner für wiederhergestellte Objekte	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0\Uninstall	RESTOREPATH=<vollständiger Pfad des Ordners> Wiederhergestellte Objekte werden in dem Ordner gespeichert, der durch folgende Parameter angegeben wird: Objekte aus der Quarantäne werden im Unterordner \Quarantine gespeichert. Objekte aus dem Backup werden im Unterordner \Backup gespeichert.

VERÄNDERUNGEN, DIE SICH NACH DER INSTALLATION VON KASPERSKY ANTI-VIRUS IM SYSTEM ERGEBEN

Bei der Installation von Kaspersky Anti-Virus und der Konsole von Kaspersky Anti-Virus (Satz "Administrationswerkzeuge") nimmt der Dienst Windows Installer auf dem Computer folgende Veränderung vor:

- Auf dem geschützten Server und auf dem Computer, auf dem die MMC-Konsole von Kaspersky Anti-Virus installiert wird, werden die Ordner für Kaspersky Anti-Virus angelegt.
- die Dienste von Kaspersky Anti-Virus werden registriert;
- eine Benutzergruppe für Kaspersky Anti-Virus wird erstellt;
- die Schüssel von Kaspersky Anti-Virus werden in der Systemregistrierung eingetragen.

Diese Veränderungen werden im Folgenden beschrieben.

Ordner von Kaspersky Anti-Virus

Tabelle 6. Ordner von Kaspersky Anti-Virus auf dem geschütztem Server

ORDNER	DATEIEN FÜR KASPERSKY ANTI-VIRUS
%Ordner von Kaspersky Anti-Virus%; Standard: • In der 32-Bit-Version von Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition\ • In der 64-Bit-Version von Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition\	Ausführbare Dateien von Kaspersky Anti-Virus (Zielordner, der bei der Installation angegeben wird.)
%Ordner von Kaspersky Anti-Virus%**mibs**	Dateien für die Management Information Base (MIB). Diese Dateien enthalten eine Beschreibung der Indikatoren und Traps, die von Kaspersky Anti-Virus mit dem SMNP-Protokoll veröffentlicht werden.
%Ordner von Kaspersky Anti-Virus%**x64**	64-Bit-Version der ausführbaren Dateien von Kaspersky Anti-Virus (Der Ordner wird nur erstellt, wenn Kaspersky Anti-Virus auf eine 64-Bit-Version von Microsoft Windows installiert wird.)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Data**\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Settings**\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Dskm**\	Dienstdateien für Kaspersky Anti-Virus
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Update**\	Dateien mit Parametern für die Update-Quellen
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Update\Distribution**\	Updates der Datenbanken und Programm-Module, die mit Hilfe der Aufgabe **Update-Verteilung** empfangen wurden (Der Ordner wird erstellt, wenn zum ersten Mal Updates mit Hilfe der Aufgabe **Update-Verteilung** empfangen werden)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Reports**\	Berichte über Aufgabenausführung und Systemaudit-Bericht
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Bases\Current**	Satz der Datenbanken, die im Moment verwendet werden

ORDNER	DATEIEN FÜR KASPERSKY ANTI-VIRUS
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Bases****Backup**\	Sicherungskopie der Datenbanken; wird bei jedem Update überschrieben
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Bases****Temp**\	Temporäre Dateien, die beim Ausführen der Update-Aufgabe angelegt werden
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Quarantine**\	Objekte in der Quarantäne (standardmäßiger Ordner)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Backup**\	Objekte im Backup (standardmäßiger Ordner)
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\KAV for Windows Servers Enterprise Edition\8.0**Restored**\	Objekte, die aus Backup oder Quarantäne wiederhergestellt wurden (standardmäßiger Ordner für die Wiederherstellung von Objekten)

Tabelle 7. Ordner, die bei der Installation der Konsole von Kaspersky Anti-Virus erstellt werden

ORDNER	DATEIEN FÜR KASPERSKY ANTI-VIRUS
%Ordner von Kaspersky Anti-Virus%; Standard: • in der 32-Bit-Version von Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition\; • in der 64-Bit-Version von Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition\	Dateien des Satzes "Administrationswerkzeuge" (Zielordner, der bei der Installation der Konsole von Kaspersky Anti-Virus angegeben wird)

Dienste von Kaspersky Anti-Virus

Die Dienste von Kaspersky Anti-Virus werden unter dem Benutzerkonto **Lokales System** (**SYSTEM**) gestartet.

Tabelle 8. Dienste von Kaspersky Anti-Virus

DIENST	ZIEL
Kaspersky Anti-Virus Service	Basisdienst von Kaspersky Anti-Virus; steuert die Aufgaben und Arbeitsprozesse von Kaspersky Anti-Virus
Verwaltungsdienst für Kaspersky Anti-Virus (Kaspersky Anti-Virus Management Service)	Dienst für die Administration des Anti-Virus über die Konsole von Kaspersky Anti-Virus.
Script Interceptor Dispatcher	Dienst zur Skript-Untersuchung

Gruppen von Kaspersky Anti-Virus

Tabelle 9. Gruppen von Kaspersky Anti-Virus

GRUPPE	ZIEL
KAVWSEE Administrators	Die Benutzer aus dieser Gruppe besitzen auf dem geschützten Server Vollzugriff auf den Verwaltungsdienst für Kaspersky Anti-Virus sowie Zugriff auf alle Funktionen von Kaspersky Anti-Virus.

Schlüssel der Systemregistrierung

Tabelle 10. Schlüssel der Systemregistrierung

SCHLÜSSEL	ZIEL
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Parameter für Kaspersky Anti-Virus Service
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Anti-Virus]	Einstellungen für den Ereignisbericht von Kaspersky Anti-Virus (Kaspersky Event Log)
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsscs]	Parameter für Script Interceptor Dispatcher
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Einstellungen für den Verwaltungsdienst von Kaspersky Anti-Virus
In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus\Performance] In der 64-Bit-Version von Microsoft Windows: [[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Anti-Virus x64\Performance].	Parameter für die Produktivitäts-Counter
In der 32-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\SnmpAgent] In der 64-Bit-Version von Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\KAVFSEE\SnmpAgent]	Parameter für die Komponente Unterstützung des SNMP-Protokolls
In der 32-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\Software\KasperskyLab\KAVFSEE\8.0\Trace\ In der 64-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\8.0\Trace\	Parameter des Protokoll der Ablaufverfolgung
In der 32-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\KAVFSEE\8.0\CrashDump\ In der 64-Bit-Version von Microsoft Windows: HKEY_LOCAL_MACHINE\Software\Wow6432Node\KasperskyLab\KAVFSEE\8.0\CrashDump\	Parameter für Dumps

PROZESSE VON KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus startet die in der folgende Tabelle beschriebenen Prozesse.

Tabelle 11. Prozesse von Kaspersky Anti-Virus

DATEINAME	ZIEL
kavfs.exe	Prozess von Kaspersky Anti-Virus Service
kavfswp.exe	Arbeitsprozess von Kaspersky Anti-Virus
kavfsscs.exe	Prozess von Script Interceptor Dispatcher
kavtray.exe	Prozess für die Komponente "Kaspersky Anti-Virus-Symbol"
Kavfsgt.exe	Prozess für den Verwaltungsdienst von Kaspersky Anti-Virus
kavshell.exe	Prozess der Befehlszeilen-Utility
kavfsrcn.exe	Prozess für die Fernverwaltung von Kaspersky Anti-Virus

INSTALLATION PLANEN

Dieser Abschnitt beschreibt die Administrations-Tools für Kaspersky Anti-Virus sowie die Besonderheiten, die bei der Installation von Kaspersky Anti-Virus mit folgenden Methoden gelten: mithilfe des Setup-Assistenten, aus der Befehlszeile, über Kaspersky Security Center und über Active Directory-Gruppenrichtlinien.

Bevor Sie mit der Installation von Kaspersky Anti-Virus beginnen, sollten Sie die wichtigsten Installationsetappen planen.

Gehen Sie folgendermaßen vor, um die Installation zu planen:

1. Wählen Sie die Administrations-Tools aus, die Sie zur Verwaltung und Konfiguration von Kaspersky Anti-Virus einsetzen möchten.
2. Entscheiden Sie, welche Programmkomponenten installiert werden müssen (s. S. 14).
3. Wählen Sie eine Installationsmethode aus.

IN DIESEM ABSCHNITT

ADMINISTRATIONSWERKZEUGE WÄHLEN

Entscheiden Sie, welche Administrationswerkzeuge Sie für die Verwaltung von Kaspersky Anti-Virus und dessen Einrichtung einsetzen möchten. Als Administrationswerkzeuge von Kaspersky Anti-Virus können die Konsole von Kaspersky Anti-Virus, das Befehlszeilen-Utility sowie die Anwendung Kaspersky Security Center dienen.

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.

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.

Die Konsole von Kaspersky Anti-Virus gehört zu dem Komponentensatz "Administrationswerkzeuge".

Befehlszeilen-Utility

Sie können Kaspersky Anti-Virus über die Befehlszeile des geschützten Servers verwalten.

Die Befehlszeilen-Utility gehört zu dem zum Satz der Programmkomponenten von Kaspersky Anti-Virus.

Kaspersky Security Center

Wenn Sie zur zentralisierten Verwaltung des Antiviren-Schutzes für die Computer in Ihrem Unternehmen das Programm Kaspersky Security Center verwenden, können Sie Kaspersky Anti-Virus über die Administrationskonsole von Kaspersky Security Center verwalten.

Die folgende Programmkomponenten müssen installiert werden.

Modul für die Integration in den Administrationsagenten von Kaspersky Security Center. Diese Komponente gehört zu dem zum Satz der Programmkomponenten von Kaspersky Anti-Virus. Sie gewährleistet die Verbindung zwischen Kaspersky Anti-Virus und dem Administrationsagenten. Installieren Sie das Modul zur Integration mit dem Administrationsagenten von Kaspersky Security Center auf dem geschützten Server.

Sie können Details über die Kaspersky Anti-Virus-Komponenten und dessen Codes nachlesen (s. S. 14).

Administrationsagent für Kaspersky Security Center. Installieren Sie ihn auf jedem geschützten Server. Diese Komponente koordiniert die Interaktion zwischen dem Programm Kaspersky Anti-Virus, das auf dem Server installiert ist, und dem Administrationsserver von Kaspersky Security Center. Die Installationsdatei des Administrationsagenten gehört zum Lieferumfang von Kaspersky Security Center.

Verwaltungs-Plug-in für Kaspersky Anti-Virus. Installieren Sie auf den Computer, auf dem die Administrationskonsole von Kaspersky Security Center installiert ist, zusätzlich das Verwaltungs-Plug-in für Kaspersky Anti-Virus über die Administrationskonsole. Das Plug-In bietet die Oberfläche zur Anti-Virus-Verwaltung über Kaspersky Security Center. Die Installationsdatei für das Plug-In \plugin\klcfginst .exe gehört zum Lieferumfang von Kaspersky Anti-Virus.

INSTALLATIONSMETHODE AUSWÄHLEN

Sie haben die benötigten Programmkomponenten für die Installation festgelegt (s. Pkt. "Programmkomponenten von Kaspersky Anti-Virus und seine Codes für den Dienst Windows Installer" auf S. 14).

Jetzt entscheiden Sie sich für die Installationsmethode je nach der Netzwerkarchitektur und den folgenden Bedingungen:

- ob Sie spezielle Installationsparameter für Kaspersky Anti-Virus angeben müssen oder die standardmäßigen Installationsparameter heranziehen (s. S. 16);
- ob die Installationsparameter für alle Server einheitlich oder für jeden Server individuell sind.

Sie können Kaspersky Anti-Virus mit dem Installationsassistenten sowie ohne Benutzereingriff installieren, indem Sie die Installationsparameter in die Befehlszeile eingeben. Für eine zentralisierte Remote-Installation von Kaspersky Anti-Virus bestehen folgende Varianten: über Active Directory oder mithilfe der Aufgabe zur Remote-Installation von Kaspersky Security Center.

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

Installationsassistent starten

Mit dem Installationsassistenten können Sie installieren:

- Programmkomponenten von Kaspersky Anti-Virus auf dem geschützten Server (s. S. 26) aus der Datei \server\setup.exe im Lieferumfang;
- Konsole von Kaspersky Anti-Virus aus der Datei \client\setup.exe im Lieferumfang auf dem geschützten Server oder auf einem anderen Rechner des lokalen Netzwerks.

Aus der Befehlszeile Datei des Installationspaketes mit Installationsparametern starten

Indem Sie die Datei des Installationspaketes ohne Schlüssel aufrufen, installieren Sie Kaspersky Anti-Virus mit den standardmäßigen Installationsparametern. Mit speziellen Schlüsseln von Kaspersky Anti-Virus können Sie die Installationsparameter ändern.

Sie können die Konsole von Kaspersky Anti-Virus auf dem geschützten Server und/oder auf dem Administrator-Desktop installieren.

Beispiele für Befehle zur Installation von Kaspersky Anti-Virus und der Konsole von Kaspersky Anti-Virus stehen in Pkt. "Installation und Deinstallation von Kaspersky Anti-Virus aus der Befehlszeile" (s. S. 36).

Zentrale Installation über Kaspersky Security Center

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

Die Server, auf denen Sie Kaspersky Anti-Virus über Kaspersky Security Center installieren möchten (s. S. 40), können sich in der gleichen Domäne wie der Administrationsserver oder in einer anderen Domäne befinden, oder keiner Domäne angehören.

Zentrale Installation über Gruppenrichtlinien des Active Directory

Mit den Gruppenrichtlinien von Active Directory können Sie Kaspersky Anti-Virus auf dem geschützten Server installieren. Sie können auch die Anti-Virus-Konsole auf dem geschützten Server oder auf dem Administrator-Desktop installieren.

Sie können Kaspersky Anti-Virus nur mit den standardmäßigen Installationsparametern installieren.

Server, auf denen Sie Kaspersky Anti-Virus über Gruppenrichtlinien des Active Directory installieren, müssen sich in einer Domäne und in einer Organisationseinheit befinden. Die Installation erfolgt beim Serverstart vor der Anmeldung bei Microsoft Windows.

INSTALLATION UND DEINSTALLATION VON KASPERSKY ANTI-VIRUS MIT DEM ASSISTENTEN

Hier wird beschrieben, wie Kaspersky Anti-Virus und die Konsole für Kaspersky Anti-Virus mithilfe des Setup-Assistenten auf einem geschützten Server installiert und vom Server entfernt werden. Außerdem finden Sie hier Informationen über erweiterte Einstellungen für Kaspersky Anti-Virus und über die Aktionen, die nach der Installation von Kaspersky Anti-Virus erforderlich sind.

IN DIESEM ABSCHNITT

INSTALLATION MIT DEM INSTALLATIONSASSISTENTEN

Die folgenden Abschnitte bieten Informationen darüber, wie Kaspersky Anti-Virus und die Konsole von Kaspersky Anti-Virus installiert werden

Gehen Sie folgendermaßen vor, um den Kaspersky Anti-Virus zu installieren und das Programm zu verwenden:

1. Installieren Sie Kaspersky Anti-Virus auf dem geschützten Server.
2. Installieren Sie die Konsole für Kaspersky Anti-Virus auf den Computern, von denen Sie Kaspersky Anti-Virus verwalten möchten.
3. Wenn Sie die Konsole für Kaspersky Anti-Virus nicht auf dem geschützten Server installiert haben, sondern auf einem anderen Computer, so sind zusätzliche Einstellungen erforderlich, damit Kaspersky Anti-Virus von den Benutzern über die Konsole fernverwaltet werden kann.
4. Führen Sie die empfohlenen Aktionen nach der Installation von Kaspersky Anti-Virus aus.

IN DIESEM ABSCHNITT

INSTALLATION VON KASPERSKY ANTI-VIRUS AUF DEM GESCHÜTZTEM SERVER

Führen Sie vor der Installation von Kaspersky Anti-Virus folgende Aktionen aus:

- Vergewissern Sie sich, dass auf dem Server keine anderen Antiviren-Anwendungen installiert sind. Sie können Kaspersky Anti-Virus installieren, ohne Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition oder Kaspersky Anti-Virus 6.0 / 8.0 für Windows Servers zu deinstallieren.
- Vergewissern Sie sich, dass das Benutzerkonto, mit dessen Berechtigungen Sie den Installationsassistenten starten, in der Administratorengruppe auf dem geschützten Server angemeldet ist.

Nach diesen Vorbereitungen können Sie zur Installation übergehen. Folgen Sie den Anweisungen des Installationsassistenten und geben Sie die Installationsparameter für Kaspersky Anti-Virus an. Sie können die Installation von Kaspersky Anti-Virus bei jedem Schritt des Installationsassistenten abbrechen. Klicken Sie dazu im Fenster des Installationsassistenten auf die Schaltfläche **Abbrechen**.

Sie können Details über die Parameter der Installation /Deinstallation nachlesen (s. S. 16).

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus zu installieren:

1. Starten Sie auf dem Server die Datei des Begrüßungsprogramms setup.exe.
2. Das Fenster des Willkommen-Programms wird geöffnet.

   Klicken Sie auf das Link **Kaspersky Anti-Virus**.
3. Das Willkommensfenster des Installationsassistenten von Kaspersky Anti-Virus wird geöffnet. Klicken Sie auf **Weiter**.
4. Das Fenster **Lizenzvertrag** wird geöffnet.

   Lesen Sie die Bedingungen des Lizenzvertrags und aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**, um die Installation fortzusetzen. Klicken Sie auf **Weiter**.
5. Wenn auf dem Server eine Vorgängerversion von Kaspersky Anti-Virus für Windows Servers Enterprise Edition oder Kaspersky Anti-Virus für Windows Servers installiert ist, wird das Fenster **Vorgängerversion des Programms wurde gefunden** geöffnet.

   Wenn die oben genannte Programme nicht installiert sind, gehen Sie zu Schritt **6**.

   Um die Vorgänger-Version zu aktualisieren, klicken Sie auf die Schaltfläche **Installieren**. Der Setup-Assistent aktualisiert Kaspersky Anti-Virus. Dabei werden kompatible Einstellungen in die neue Version übernommen (s. Abschnitt "Upgrade einer Vorgängerversion des Programms" auf S. 47). Nach Abschluss öffnet sich das Fenster **Installation wurde abgeschlossen** (gehen Sie zum Schritt **15** dieser Anleitung).
6. Das Fenster **Untersuchung des Computers auf Viren vor dem Start der Installation** wird geöffnet.

   Aktivieren Sie das Kontrollkästchen **Computer auf Viren untersuchen**, um die Bootsektoren von lokalen Datenträgern des Servers und Systemspeicher auf Bedrohungen untersucht werden. Nach der Untersuchung öffnet sich das Fenster mit den Ergebnissen der Antiviren-Untersuchung.

   Sie können folgende Informationen über die Objekte einsehen, die auf dem Server untersucht wurden: Anzahl der untersuchten Objekte, Anzahl der gefundenen Bedrohungstypen, Anzahl der gefundenen infizierten und möglicherweise infizierten Objekte, Anzahl der infizierten oder möglicherweise infizierten Prozesse, die Kaspersky Anti-Virus aus dem Arbeitsspeicher entfernt hat, und Anzahl der infizierten oder möglicherweise infizierten Prozesse, die Kaspersky Anti-Virus nicht entfernen konnte.

   Um anzuzeigen, welche Objekte genau untersucht worden sind, klicken Sie auf die Schaltfläche **Liste der verarbeiteten Objekte**.

   Klicken Sie im Fenster **Untersuchung des Computers auf Viren vor dem Start der Installation** auf **Weiter**.
7. Das Fenster **Installationstyp** wird geöffnet.

   Wählen Sie eine der folgenden Varianten:

   - **Empfohlene Installation**, um alle Programmkomponenten von Kaspersky Anti-Virus zu installieren, mit der Ausnahme von **Skript-Untersuchung**.
   - **Benutzerdefinierte Installation**, um die Komponenten aus der Liste der Programmkomponenten von Kaspersky Anti-Virus auszuwählen.

   Informieren Sie sich ausführlicher über die Programmkomponenten von Kaspersky Anti-Virus (s. S. 14).

   Wenn Sie sich für den Installationstyp **Empfohlene Installation** entschieden haben, gehen Sie weiter zu Schritt 11.
8. Wenn Sie sich für den Installationstyp **Benutzerdefinierte Installation** entschieden haben, öffnet sich das Fenster **Benutzerdefinierte Installation**.

   Standardmäßig umfasst die Liste der zu installierenden Objekte alle Komponenten von Kaspersky Anti-Virus, mit der Ausnahme von **Skript-Untersuchung**.

   Die Komponente **Unterstützung des SNMP-Protokolls** von Kaspersky Anti-Virus wird auf dem geschützten Server nur installiert, wenn auf dem Server der Service SNMP Microsoft Windows installiert ist.

   Wählen Sie die Komponente, die Sie installieren wollen. Um alle Änderungen im Fenster **Benutzerdefinierte Installation** zu verwerfen, klicken Sie auf die Schaltfläche **Zurücksetzen**. Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie den Komponentenbestand gewählt haben.

9. Das Fenster **Zielordner auswählen** wird geöffnet.

   Geben Sie bei Bedarf einen anderen Ordner an, in dem die Dateien von Kaspersky Anti-Virus gespeichert werden sollen. Klicken Sie auf **Weiter**.

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

    Passen Sie die folgende Parameter der Installation an:

    - **Echtzeitschutz nach der Installation des Programms aktivieren.**
    - **Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen.**
    - **Dateien, die von Kaspersky Lab empfohlen werden, zu Ausnahmen hinzufügen.**
    - **Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen**.

    Sie können Details über die Parameter der Installation /Deinstallation nachlesen (s. S. 16).

11. Das Fenster **Einstellungen aus einer Konfigurationsdatei importieren** wird geöffnet.

    Um die Einstellungen für Kaspersky Anti-Virus aus einer vorhandenen Konfigurationsdatei zu importieren, die in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition erstellt wurde, geben Sie diese Konfigurationsdatei an. Klicken Sie auf **Weiter**.

12. Das Fenster **Programmaktivierung** wird geöffnet.

    Geben Sie die Schlüsseldatei von Kaspersky Anti-Virus an, um den Schlüssel hinzuzufügen:

    - Wenn Sie zuvor eine Schlüsseldatei im Ordner \server (der zum Lieferumfang gehört) gespeichert haben, wird der Name dieser Datei im Feld **Schlüssel** angezeigt.
    - Wenn Sie einen Schlüssel aus der Datei, die in einem anderen Ordner gespeichert ist, hinzufügen möchten, geben Sie die Schlüsseldatei an.

      Sehen Sie Details über Lizenz ein. Kaspersky Anti-Virus zeigt das berechnete Ablaufdatum der Lizenz an. Die Gültigkeitsdauer der Lizenz wird ab dem Hinzufügen des Schlüssels gezählt, läuft jedoch spätestens nach dem Ablauf der Gültigkeitsfrist der Schlüsseldatei ab.

      Wenn der hinzugefügte Schlüssel in Übereinstimmung mit den Lizenzbedingungen die Schutzfunktion für Netzwerkspeicher unterstützt, steht Ihnen die Funktion zum Schutz von Netzwerkspeichern zur Verfügung.

      Klicken Sie auf **Weiter**, um einen Schlüssel hinzuzufügen.

13. Es öffnet sich das Fenster **Bereit zur Installation**. Klicken Sie auf **Installieren**. Der Assistent installiert nun die Komponenten von Kaspersky Anti-Virus.

14. Sobald die Installation abgeschlossen wurde, öffnet sich das Fenster **Installation wurde abgeschlossen**. Setzen Sie das Häkchen im Kontrollkästchen **Versionshinweise lesen**, um die Ausgabedaten nach Fertigstellung des Installationsassistenten anzusehen.

    Klicken Sie auf **OK** um das Fenster des Assistenten zu schließen.

    Sobald die Installation abgeschlossen wurde, ist Kaspersky Anti-Virus einsatzbereit, unter der Voraussetzung, dass Sie einen Schlüssel hinzugefügt haben.

INSTALLATION DER KONSOLE VON KASPERSKY ANTI-VIRUS

Folgen Sie den Anweisungen des Installationsassistenten und geben Sie die Installationsparameter für die Konsole von Kaspersky Anti-Virus an. Sie können die Installation bei jedem Schritt des Assistenten abbrechen. Klicken Sie dazu im Fenster des Assistenten auf die Schaltfläche **Abbrechen**.

➧ *Gehen Sie folgendermaßen vor, um die Konsole von Kaspersky Anti-Virus zu installieren:*

1. Vergewissern Sie sich, dass das Benutzerkonto, mit dessen Berechtigungen Sie den Installationsassistenten starten, zur Administratorengruppe auf dem Computer gehört.
2. Starten Sie auf dem Computer die Datei des Begrüßungsprogramms.
3. Das Fenster des Willkommen-Programms wird geöffnet.

   Klicken Sie auf das Link **Administrations-Tools**.

4. Es öffnet sich das Begrüßungsfenster des Installationsassistenten. Klicken Sie auf **Weiter**.

5. Das Fenster **Lizenzvertrag** wird geöffnet.

   Lesen Sie die Bedingungen des Lizenzvertrags und aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen des Lizenzvertrags**, um die Installation fortzusetzen. Klicken Sie auf **Weiter**.

6. Das Fenster **Installationstyp** wird geöffnet.

   Wählen Sie eine der folgenden Varianten:

   - **Vollständige Installation**, damit auf dem Computer der komplette Satz aus den Programmkomponenten der Administrationswerkzeuge installiert wird. Er umfasst die Konsole von Kaspersky Anti-Virus, die Hilfe und Dateien mit den Handbüchern.
   - **Benutzerdefinierte Installation**, um die Komponenten manuell aus der Liste auszuwählen.

   Informieren Sie sich ausführlicher über die Programmkomponenten von Kaspersky Anti-Virus (s. S. 14).

   Klicken Sie auf **Weiter**.

   Wenn Sie sich für den Installationstyp **Vollständige Installation** entschieden haben, wechseln Sie zu Schritt **8**.

7. Wenn Sie sich für den Installationstyp **Benutzerdefinierte Installation** entschieden haben, öffnet sich das Fenster **Benutzerdefinierte Installation**.

   In der Grundeinstellung enthält die Liste der zu installierenden Komponenten alle Komponenten des Satzes "Administrationswerkzeuge". Wählen Sie die Komponente, die Sie installieren wollen. Klicken Sie auf **Weiter**.

8. Das Fenster **Zielordner auswählen** wird geöffnet.

   Geben Sie bei Bedarf einen anderen Ordner an, in dem die Dateien des Anti-Virus gespeichert werden sollen. Klicken Sie auf **Weiter**.

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

   Wenn Sie planen, Kaspersky Anti-Virus auf einem Remote-Computer mithilfe der Konsole von Kaspersky Anti-Virus zu verwalten, so aktivieren Sie das Kontrollkästchen **Remote-Zugriff erlauben**. Klicken Sie auf **Weiter**.

10. Es öffnet sich das Fenster **Bereit zur Installation**. Klicken Sie auf **Installieren**. Der Assistent installiert nun die ausgewählten Komponenten.

11. Sobald die Installation abgeschlossen wurde, öffnet sich das Fenster **Installation wurde abgeschlossen**. Klicken Sie auf die Schaltfläche **OK**, um den Assistenten zu schließen.

Wenn Sie den Satz "Administrationswerkzeuge" nicht auf dem geschützten Server, sondern auf einem anderen Computer installiert haben, nehmen Sie Zusatzeinstellungen vor (s. Abschnitt "Zusätzliche Einstellungen nach der Installation der Konsole von Kaspersky Anti-Virus auf einem anderen Computer" auf S. 29).

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

Wenn Sie die Konsole für Kaspersky Anti-Virus nicht auf dem geschützten Server installiert haben, sondern auf einem anderen Computer, so gehen Sie wie folgt vor, damit Kaspersky Anti-Virus von den Benutzern fernverwaltet werden kann:

- Fügen Sie auf dem geschützten Server die Benutzer von Kaspersky Anti-Virus zur Gruppe KAVWSEE Administrators hinzu.
- Wenn der geschützte Server unter Microsoft Windows Server 2003 / 2008 / 2012 / 2012 R2 läuft, erlauben Sie auf dem Server Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus kavfsgt.exe.
- Wenn Sie bei der Installation der Kaspersky Anti-Virus-Konsole auf einem Computer mit Microsoft Windows die Einstellung **Netzwerkverbindungen für die Konsole von Kaspersky Anti-Virus zulassen** nicht aktiviert haben, erlauben Sie die Netzwerkverbindungen für die Kaspersky Anti-Virus-Konsole über die Firewall auf diesem Computer manuell.

IN DIESEM ABSCHNITT

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

Um Kaspersky Anti-Virus über die Konsole von Kaspersky Anti-Virus zu verwalten, die auf einem anderen Computer installiert ist, müssen die Benutzer auf dem geschützten Server Vollzugriff auf den Verwaltungsdienst von Kaspersky Anti-Virus (Kaspersky Anti-Virus Management) besitzen. Standardmäßig besitzen die Benutzer, die der Gruppe der Administratoren angehören, Zugriff auf den Dienst.

Sie können eine Liste der Kaspersky Anti-Virus-Dienste einsehen (s. Abschnitt "Veränderungen, die sich nach der Installation von Kaspersky Anti-Virus im System ergeben" auf S. 21).

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 ein Benutzerkonto mit gleichen Namen und gleichen Kennwort eingerichtet ist.

NETZWERKVERBINDUNGEN AUF DEM SERVER FÜR DEN VERWALTUNGSDIENST VON KASPERSKY ANTI-VIRUS ERLAUBEN

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

Um eine Verbindung zwischen der Konsole von Kaspersky Anti-Virus und dem Verwaltungsdienst von Kaspersky Anti-Virus herzustellen, müssen Sie in der Firewall des geschützten Servers Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus erlauben.

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

Um Netzwerkverbindungen für den Verwaltungsdienst von Kaspersky Anti-Virus zu erlauben, gehen Sie wie folgt vor:

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

NETZWERKVERBINDUNGEN FÜR DIE KONSOLE VON KASPERSKY ANTI-VIRUS IN MICROSOFT WINDOWS ERLAUBEN

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

Die Konsole von Kaspersky Anti-Virus verwendet das DCOM-Protokoll, um vom Verwaltungsdienst für Kaspersky Anti-Virus auf dem Remote-Server Informationen über die Anti-Virus-Ereignisse zu erhalten (beispielsweise über untersuchte Objekte und über das Beenden von Aufgaben).

Wenn die Konsole von Kaspersky Anti-Virus auf einem Computer mit Microsoft Windows XP mit Service Pack 2 oder höher / Vista / 7 / 8 / 8.1 installiert ist, müssen Sie in der Firewall dieses Computers Netzwerkverbindungen erlauben, um eine Verbindung zwischen der Konsole von Kaspersky Anti-Virus und dem Verwaltungsdienst von Kaspersky Anti-Virus herzustellen.

Um eine Verbindung zwischen der Konsole und dem Verwaltungsdienst von Kaspersky Anti-Virus herzustellen, gehen Sie wie folgt vor:

1. 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).
2. Schalten Sie in der Windows-Firewall den TCP-Port 135 frei und erlauben Sie Netzwerkverbindungen für die ausführbare Datei kavfsrcn.exe (Prozess zur Fernverwaltung von Kaspersky Anti-Virus). Über den Port TCP 135 tauscht der Computer, auf dem die Konsole von Kaspersky Anti-Virus in der MMC installiert ist, Daten mit dem geschützten Server aus, auf dem Kaspersky Anti-Virus installiert ist.

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 die Schaltfläche **OK**.
2. Öffnen Sie in der Konsole **Komponentendienste** des Computers den Knoten **Computer**, öffnen Sie das Kontextmenü des Knotens **Arbeitsplatz** und wählen Sie den Befehl **Eigenschaften**.
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. Gehen Sie je nach Betriebssystem wie folgt vor:
   - In Microsoft Windows XP mit Service Pack 2 oder höher:
     a. Klicken Sie auf **Start** → **Systemsteuerung** → **Windows-Firewall**.
     b. Klicken Sie im Fenster **Windows-Firewall** auf der Registerkarte **Ausnahmen** auf **Programm hinzufügen**.
   - In Microsoft Windows Vista:
     a. Klicken Sie auf **Start** → **Systemsteuerung** → **Windows-Firewall** und wählen Sie im Fenster **Windows-Firewall** den Punkt **Einstellungen ändern**.
     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. Der vollständige Pfad lautet standardmäßig:

- in der 32-Bit-Version von Microsoft Windows – %ProgramFiles%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe;
- in der 64-Bit-Version von Microsoft Windows – %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Admins Tools\kavfsrcn.exe.

4. Klicken Sie auf **OK**.

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

AKTIONEN NACH DER INSTALLATION VON KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus beginnt sofort nach der Installation damit, seine Funktionen auszuführen, wenn Sie einen Schlüssel hinzugefügt haben. Wenn Sie bei der Installation von Kaspersky Anti-Virus den Punkt **Echtzeitschutz nach der Installation des Programms aktivieren** ausgewählt haben, untersucht Kaspersky Anti-Virus die Objekte des Serverdateisystems, wenn auf sie zugegriffen wird. Außerdem wird der Programmcode von zu startenden Skripten überprüft, falls Sie die Komponente zur Skript-Untersuchung installiert haben. Jeden Freitag um 20.00 Uhr führt Kaspersky Anti-Virus die Aufgabe **Untersuchung kritischer Bereiche** aus.

Es wird empfohlen, nach der Installation von Kaspersky Anti-Virus folgende Aktionen auszuführen:

- **Datenbanken von Kaspersky Anti-Virus aktualisieren**. Nach seiner Installation untersucht Kaspersky Anti-Virus Objekte anhand von Datenbanken, die im Lieferumfang enthalten sind. Um die Datenbanken zu aktualisieren, müssen Sie die Aufgabe **Update der Programm-Datenbanken** einrichten und starten.
- **Untersuchung von kritischen Bereichen des Servers auszuführen**.

Sie können Benachrichtigungen für den Administrator bei Ereignissen von Kaspersky Anti-Virus einrichten (s. *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition*).

IN DIESEM ABSCHNITT

AUFGABE ZUM UPDATE DER DATENBANKEN VON KASPERSKY ANTI-VIRUS ANPASSEN UND STARTEN

Richten Sie in der Aufgabe: 1) **Update der Datenbanken** eine Verbindung zur Updatequelle ein – *HTTP- oder FTP-Updateservern von Kaspersky Lab* und 2) starten Sie die Aufgabe **Update der Datenbanken**.

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

1. Öffnen Sie auf dem Computer die Konsole von Kaspersky Anti-Virus, wählen Sie **Start → Programme → Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Administrationswerkzeuge → Konsole für Kaspersky Anti-Virus**.
2. Wenn Sie die Konsole von Kaspersky Anti-Virus nicht auf dem geschützten Server gestartet haben, sondern auf einem anderen Computer, stellen Sie eine Verbindung mit dem geschützten Server her: Öffnen Sie das Kontextmenü auf dem Namen des Anti-Virus-Snap-ins, wählen Sie den Befehl **Verbindung mit anderem Computer herstellen**, wählen Sie dann im Dialogfenster **Computer wählen** die Variante **Anderer Computer** und geben Sie im Eingabefeld den Netzwerknamen des geschützten Server an.

Wenn das Benutzerkonto, das Sie zur Anmeldung bei Microsoft Windows verwendet haben, auf dem Server nicht über die erforderlichen Rechte für den Verwaltungsdienst von Kaspersky Anti-Virus verfügt, so geben Sie ein Benutzerkonto mit entsprechenden Rechten an. Informieren Sie sich darüber, welchen Benutzerkonten der Zugriff auf den Anti-Virus-Verwaltungsdienst gewährt werden kann (s. Abschnitt "Benutzer von Kaspersky Anti-Virus auf dem geschützten Server zur Gruppe KAVWSEE Administrators hinzufügen" auf S. 30).

Das Konsolenfenster von Kaspersky Anti-Virus wird geöffnet.

3. Wählen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Update**.
4. Öffnen Sie das Kontextmenü durch Rechtsklick auf die Aufgabe **Update der Programm-Datenbanken** und wählen Sie den Befehl **Eigenschaften**.
5. Im Dialogfenster **Eigenschaften: Update der Programm-Datenbanken** die Registerkarte **Verbindungseinstellungen anpassen.**
6. Führen Sie folgende Aktionen aus:
   a. Wenn in Ihrem Netzwerk das Web Proxy Auto-Discovery Protocol (WPAD) zur automatischen Erkennung von Proxyservern in einem lokalen Netzwerk eingerichtet ist, tragen Sie die Parameter des Proxyservers ein: In der Parametergruppe **Proxyserver-Parameter** gehen Sie auf **Folgende Proxyserver-Parameter verwenden**, im Feld **Adresse** tragen Sie die Adresse und im Feld **Port** – tragen Sie die Portnummer des Proxyservers ein.
   b. Wenn in Ihrem Netzwerk beim Zugriff auf den Proxyserver eine Authentifizierung erfolgt, wählen Sie die gewünschte Methode der Authentifizierung in der Optionsgruppe :**Einstellungen für Authentifizierung auf dem Proxyserver** aus:
      - **NTLM-Authentifizierung verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung (NTLM-authentication) unterstützt. Kaspersky Anti-Virus benutzt für den Zugriff auf den Proxyserver das Benutzerkonto, das in der Aufgabe angegeben ist (standardmäßig läuft die Aufgabe unter dem Benutzerkonto **Lokales System** (**SYSTEM**)).
      - **NTLM-Authentifizierung mit Name und Kennwort verwenden**, wenn der Proxyserver die in Microsoft Windows integrierte Authentifizierung unterstützt. Kaspersky Anti-Virus verwendet das von Ihnen vorgegebene Benutzerkonto für die Authentifizierung am Proxyserver.

        Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.
      - **Benutzername und Kennwort verwenden**, um die übliche Authentifizierung auszuwählen (Basic authentication). Geben Sie den Benutzernamen und das Kennwort ein oder markieren Sie den Benutzer in der Liste.
7. Im Dialogfenster **Update der Programm-Datenbanken Eigenschaften** klicken Sie auf **OK**.

Sie haben die Verbindung mit der Update-Quelle in der Aufgabe **Update der Programm-Datenbanken** eingerichtet. Starten Sie jetzt diese Aufgabe.

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

1. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Update**.
2. Öffnen Sie das Kontextmenü durch Rechtsklick auf die Aufgabe **Update der Programm-Datenbanken** und wählen Sie den Befehl **Starten**.

Nachdem die Aufgabe erfolgreich abgeschlossen wurde, können Sie das Erstellungsdatum der zuletzt installierten Datenbank-Updates im Knoten **Kaspersky Anti-Virus** anzeigen lassen.

UNTERSUCHUNG KRITISCHER BEREICHE

Nachdem Sie die Datenbanken von Kaspersky Anti-Virus aktualisiert haben, untersuchen Sie den Server mit der Aufgabe **Untersuchung kritischer Bereiche** auf Schadprogramme.

➧ *Um die Aufgabe **Untersuchung kritischer Bereiche** anzupassen, gehen Sie wie folgt vor:*

1. Öffnen Sie die Konsole von Kaspersky Anti-Virus (s. S. 32).
2. Wählen Sie In der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Untersuchung auf Befehl** aus.
3. Öffnen Sie das Kontextmenü durch Rechtsklick auf die Aufgabe **Untersuchung kritischer Bereiche** und wählen Sie den Befehl **Starten**.

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

Um den Bericht über die Aufgabenausführung zu öffnen, wählen Sie die Aufgabe **Untersuchung kritischer Bereiche** und klicken Sie im Ergebnisfenster auf den Link **Ausführungsbericht öffnen**.

KOMPONENTEN HINZUFÜGEN UND ENTFERNEN, KASPERSKY ANTI-VIRUS REPARIEREN

Sie können Komponenten von Kaspersky Anti-Virus hinzufügen und entfernen. Sie müssen vorsichtshalber erst den Echtzeitschutz ausschalten, falls Sie die Komponente **Echtzeitschutz** deinstallieren wollen. In den übrigen Fällen ist es nicht erforderlich, den Echtzeitschutz oder den Dienst von Kaspersky Anti-Virus anzuhalten.

Wenn bei der Ausführung von Kaspersky Anti-Virus Probleme aufgetreten sind (Kaspersky Anti-Virus stürzt ab, Aufgaben stürzen ab oder werden nicht gestartet), können Sie versuchen, Anti-Virus zu reparieren. Wenn die Reparatur ausgeführt wird, können entweder die aktuellen Werte der Parameter, Funktionen und Aufgaben von Kaspersky Anti-Virus beibehalten werden oder alle Parameter von Kaspersky Anti-Virus können auf die Standardwerte zurückgesetzt werden.

Um für die Einstellungen von Kaspersky Anti-Virus die Standardwerte wiederherzustellen, aktivieren Sie im Assistentenfenster **Installierte Komponenten reparieren** das Kontrollkästchen **Empfohlene Programmeinstellungen wiederherstellen**.

DEINSTALLATION MIT INSTALLATIONS-/DEINSTALLATIONSASSISTENT

IN DIESEM ABSCHNITT

KASPERSKY ANTI-VIRUS VON EINEM GESCHÜTZTEN SERVER DEINSTALLIEREN

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

Sie können Kaspersky Anti-Virus mit dem Installations-/Deinstallationsassistenten vom geschützten Server deinstallieren.

Nach der Deinstallation von Kaspersky Anti-Virus vom geschützten Server muss möglicherweise der Server neu gestartet werden. Sie können den Neustart verschieben.

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus zu entfernen:

1. Wählen Sie im **Startmenü** den Punkt **Alle Programme → Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Ändern oder Löschen**.
2. Im Assistenten wird das Fenster **Installation ändern, reparieren oder löschen** geöffnet.

   Wählen Sie die Variante **Löschen von Programmkomponenten** und klicken Sie auf **Weiter**.
3. Das Fenster **Erweiterte Einstellungen für die Deinstallation des Programms** wird geöffnet.

   Falls erforderlich, aktivieren Sie die folgenden Kontrollkästchen:

   - **Quarantäne-Objekte exportieren**, damit Kaspersky Anti-Virus die Quarantäne-Objekte exportiert. Klicken Sie auf **Auswählen** und geben Sie an, welche Komponenten exportiert werden sollen.
   - **Backup-Objekte exportieren**, damit Kaspersky Anti-Virus die Objekte aus dem Backup-Speicher exportiert.

   Klicken Sie auf **Weiter**.
4. Klicken Sie im Fenster **Bereit zur Deinstallation** auf **Löschen**.
5. Nach Abschluss der Deinstallation öffnet sich das Fenster **Die Deinstallation wurde abgeschlossen**.
6. Klicken Sie im Fenster **Die Deinstallation wurde abgeschlossen** auf **OK**.

KONSOLE VON KASPERSKY ANTI-VIRUS DEINSTALLIEREN

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

Sie können die Konsole von Kaspersky Anti-Virus mit Hilfe des Installations-/Deinstallationsassistenten vom Computer deinstallieren.

Nach der Deinstallation der Konsole von Kaspersky Anti-Virus ist kein Neustart des Computers erforderlich.

Gehen Sie folgendermaßen vor, um die Konsole von Kaspersky Anti-Virus zu deinstallieren:

1. Wählen Sie im **Startmenü** den Punkt **Alle Programme→ Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition → Administrations-Tools → Ändern oder Löschen**.
2. Im Assistenten wird das Fenster **Installation ändern, reparieren oder löschen** geöffnet.

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

   Das Fenster **Die Deinstallation wurde abgeschlossen** wird geöffnet.
4. Klicken Sie auf die Schaltfläche **OK**, um den Assistenten zu schließen.

INSTALLATION UND DEINSTALLATION VON KASPERSKY ANTI-VIRUS AUS DER BEFEHLSZEILE

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

In diesem Abschnitt

KASPERSKY ANTI-VIRUS AUS DER BEFEHLSZEILE INSTALLIEREN UND DEINSTALLIEREN

Sie können Kaspersky Anti-Virus installieren oder deinstallieren sowie seine Komponenten hinzufügen oder entfernen, indem Sie die Datei des Installationspakets \server\kavws.msi aufrufen und Installationsparameter mit den Standardschlüsseln angeben.

Sie können den Satz "Administrationswerkzeuge" auf dem geschützten Server oder auf einem beliebigen Computer im Netzwerk installieren, damit Sie mit der Konsole von Kaspersky Anti-Virus lokal oder im Remote-Betrieb arbeiten können. Sie können dazu die Installationspaket \client\kavwstools.msi verwenden.

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

Wenn Sie auf dem geschützten Server die Datei \server\kavws.msi ohne zusätzliche Schlüssel starten, wird Kaspersky Anti-Virus mit den Standardparametern installiert (s. S. 16).

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

INSTALLATION VON KASPERSKY ANTI-VIRUS

In diesem Abschnitt

BEISPIELE FÜR BEFEHLE ZUR INSTALLATION VON KASPERSKY ANTI-VIRUS

Dieser Abschnitt bietet Beispiele für Befehle zur Installation von Kaspersky Anti-Virus.

Starten Sie die Datei auf einem Computer mit einer 32-Bit-Version von Microsoft Windows aus dem im Lieferumfang enthaltenen Ordner \x86, auf einem Computer mit einer 64-Bit-Version von Microsoft Windows aus dem mitgelieferten Ordner \x64.

Erläuterungen zur Verwendung der Standardbefehle und -schlüssel des Dienstes Windows Installer finden Sie in der entsprechenden Dokumentation der Firma Microsoft.

Beispiele für Befehle zur Installation von Kaspersky Anti-Virus: Start der Datei setup.exe

- *Führen Sie folgenden Befehl aus, um Kaspersky Anti-Virus mit den standardmäßigen Installationseinstellungen ohne Interaktion mit dem Benutzer zu installieren:*

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

- *Um Kaspersky Anti-Virus mit den folgenden Installationsparametern zu installieren:*

  - nur Komponente **Echtzeitschutz für Dateien** und **Untersuchung auf Befehl** installieren;
  - den Echtzeitschutz beim Start von Kaspersky Anti-Virus nicht zu starten;
  - und Dateien nicht von der Untersuchung auszuschließen, deren Ausschluss von Microsoft empfohlen wird;

  führen Sie folgenden Befehl aus:

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

- *Um Anti-Virus zu installieren und die Datei des Installationsprotokolls mit dem Namen kavws.log im Ordner \x86 zu speichern, führen Sie den folgenden Befehl aus:*

  ```
  \x86\server\setup.exe /l kavws.log
  ```

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

- *Führen Sie folgenden Befehl aus, um Kaspersky Anti-Virus mit den standardmäßigen Installationseinstellungen zu installieren, ohne dass Interaktion mit dem Benutzer erfolgt:*

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

- *Führen Sie folgenden Befehl aus, um Kaspersky Anti-Virus mit den standardmäßigen Installationseinstellungen zu installieren und die Installationsoberfläche anzuzeigen:*

  ```
  msiexec /i kavws.msi /qf EULA=1
  ```

- *Um Kaspersky Anti-Virus mit der Aktivierung aus der Schlüsseldatei C:\0000000A.key zu installieren:*

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

- *Um Kaspersky Anti-Virus zu installieren, wobei vorher die aktiven Prozesse und die Bootsektoren der lokalen Computerlaufwerke untersucht werden, geben Sie folgenden Befehl ein:*

  ```
  msiexec /i kavws.msi PRESCAN=1 /qn EULA=1
  ```

- *Um Kaspersky Anti-Virus zu installieren und seine Dateien im Zielordner C:\WSEE zu speichern, geben Sie den folgenden Befehl ein:*

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

- *Um Kaspersky Anti-Virus zu installieren und die Datei des Installationsprotokolls mit dem Namen kavws.log im Ordner, in dem die msi-Datei des Anti-Virus-Installationspakets gespeichert ist, zu speichern, geben Sie den folgenden Befehl ein:*

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

- *Führen Sie folgenden Befehl aus, um die Konsole von Kaspersky Anti-Virus zu installieren:*

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

- *Um Kaspersky Anti-Virus mit der Aktivierung aus der Schlüsseldatei C:\0000000A.key zu installieren; Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen; Kaspersky Anti-Virus gemäß den in der Konfigurationsdatei C:\settings.xml beschriebenen Parametern anzupassen, geben Sie den folgenden Befehl ein:*

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

SIEHE:

AKTIONEN NACH DER INSTALLATION VON KASPERSKY ANTI-VIRUS

Wenn Sie bei der Installation von Kaspersky Anti-Virus einen Schlüssel hinzugefügt ind **Echtzeitschutz aktivieren** ausgewählt haben, untersucht Kaspersky Anti-Virus direkt nach der Installation die Objekte des Serverdateisystems, auf die zugegriffen wird. Außerdem wird der Programmcode von gestarteten Skripts überprüft, falls Sie die Komponente zur Skript-Untersuchung installiert haben. Jeden Freitag um 20.00 Uhr startet Kaspersky Anti-Virus die Untersuchung von kritischen Bereichen des Servers.

Es wird empfohlen, nach der Installation von Kaspersky Anti-Virus folgende Aktionen auszuführen:

- Update-Aufgabe für die Datenbanken von Kaspersky Anti-Virus starten. Nach seiner Installation untersucht Kaspersky Anti-Virus Objekte anhand von Datenbanken, die im Lieferumfang enthalten sind. Es wird empfohlen, diese Datenbanken für Kaspersky Anti-Virus umgehend zu aktualisieren. Dazu müssen Sie die Aufgabe **Update der Programm-Datenbanken** starten. Danach wird das Update dem standardmäßigen Zeitplan stündlich ausgeführt.

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

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

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

  Details zur Verwaltung von Kaspersky Anti-Virus aus der Befehlszeile finden Sie im *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition.*

- Untersuchung von kritischen Bereichen des Servers ausführen, wenn vor der Installation von Kaspersky Anti-Virus auf dem geschützten Server keine Antiviren-Anwendung installiert und die Funktion zum Echtzeitschutz für Dateien nicht aktiviert war.

- *Um die Aufgabe **Untersuchung kritischer Bereiche** anzupassen, führen Sie den folgenden Befehl aus:*

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

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

- Einrichten von Benachrichtigungen für den Administrator bei Ereignissen von Kaspersky Anti-Virus (s. *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition*).

KOMPONENTEN HINZUFÜGEN UND ENTFERNEN. BEISPIELE FÜR BEFEHLE

Wenn Kaspersky Anti-Virus bereits installiert ist und Sie Komponenten hinzufügen (s. S. 14), geben Sie in der Liste für Werte des Schlüssels ADDLOCAL nicht nur die Codes der Komponenten an, die Sie installieren möchten, sondern auch die Codes der bereits installierten Komponenten. Andernfalls werden die bereits installierten Komponenten entfernt.

Die Komponente "Untersuchung auf Befehl" wird automatisch installiert. Es ist nicht erforderlich, diese Komponente in der Liste für die Werte des Schlüssels ADDLOCAL anzugeben, um Komponenten von Kaspersky Anti-Virus hinzuzufügen oder zu entfernen.

- *Um die Komponente "Skript-Untersuchung" zu den bereits installierten Komponenten "Untersuchung auf Befehl" und "Echtzeitschutz" hinzuzufügen, führen Sie folgenden Befehl aus:*

  ```
  msiexec /i kavws.msi ADDLOCAL=Oas,ScriptChecker /qn EULA=1
  ```

  oder

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

KASPERSKY ANTI-VIRUS DEINSTALLIEREN BEISPIELE FÜR BEFEHLE

- *Um Kaspersky Anti-Virus vom geschützten Server zu deinstallieren, führen Sie folgenden Befehl aus:*

  ```
  msiexec /x kavws.msi /qn EULA=1
  ```

- *Um die Konsole von Kaspersky Anti-Virus zu deinstallieren, führen Sie folgenden Befehl aus:*

  ```
  msiexec /x kavwstools.msi /qn EULA=1
  ```

RÜCKGABECODES

In diesem Abschnitt werden die Feedback-Codes der Befehlszeile beschrieben.

Tabelle 12. Rückgabecodes

CODE	BESCHREIBUNG
25001	Berechtigungen für Programminstallation reichen nicht.
25002	Die Deinstallation der Vorgängerversion des Programms wurde nicht abgeschlossen.
25003	Die zu installierende Applikation passt nicht zur Bit-Version des Betriebssystems.
25004	Es wurde ein inkompatibles Programm gefunden.

INSTALLATION UND DEINSTALLATION VON KASPERSKY ANTI-VIRUS ÜBER KASPERSKY SECURITY CENTER

Dieser Abschnitt bietet allgemeine Informationen zur Installation von Kaspersky Anti-Virus über Kaspersky Security Center, eine Beschreibung des Vorgehens für die Installation und Deinstallation von Kaspersky Anti-Virus über Kaspersky Security Center, sowie eine Beschreibung der Aktionen, die nach der Installation von Kaspersky Anti-Virus erforderlich sind.

IN DIESEM ABSCHNITT

ALLGEMEINES ZUR INSTALLATION ÜBER KASPERSKY SECURITY CENTER

Sie können Kaspersky Anti-Virus mithilfe einer Remote-Installationsaufgabe über Kaspersky Security Center installieren.

Mithilfe einer Remote-Installationsaufgabe wird Kaspersky Anti-Virus auf mehreren Computern mit einheitlichen Einstellungen installiert.

Sie können Server in eine Administrationsgruppe zusammenführen und eine Gruppenaufgabe zur Installation von Kaspersky Anti-Virus auf den Servern dieser Gruppe erstellen.

Sie können eine Remote-Installationsaufgabe für Kaspersky Anti-Virus erstellen, die sich auf eine Auswahl von Computern bezieht, die nicht zur gleichen Administrationsgruppe gehören. Legen Sie dazu eine Liste mit Computern an, auf die Kaspersky Anti-Virus installiert werden soll.

Genaue Angaben über die Remote-Installationsaufgabe finden Sie im *Administratorhandbuch für Kaspersky Security Center*.

RECHTE FÜR DIE INSTALLATION ODER DEINSTALLATION VON KASPERSKY ANTI-VIRUS

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

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

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

- Alle Computer, auf denen Sie Kaspersky Anti-Virus installieren möchten, gehören zur gleichen Domäne wie der Administrationsserver und der Administrationsserver ist unter dem Benutzerkonto **Domain-Administrator** (**Domain Admin**) angemeldet (wenn es über die Rechte eines Administrators auf den Computern der Domäne verfügt).

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

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

- über das Recht Anwendungen remote zu starten;
- über die Rechte auf **Admin$** Ressource;
- über das Recht **Als Dienst starten**.

INSTALLATION VON KASPERSKY ANTI-VIRUS ÜBER KASPERSKY SECURITY CENTER

IN DIESEM ABSCHNITT

PROZEDUR FÜR INSTALLATION VON KASPERSKY ANTI-VIRUS ÜBER KASPERSKY SECURITY CENTER

Dieser Abschnitt bietet eine kurze Anleitung für die Installation von Kaspersky Anti-Virus mit Hilfe einer Aufgabe zur Remote-Installation über Kaspersky Security Center.

Details darüber, wie ein Installationspaket und die Aufgabe zur Remote-Installation erstellt werden, finden Sie im Dokument "*Kaspersky Security Center. Implementierungshandbuch*".

Wenn Sie planen, Kaspersky Anti-Virus künftig über Kaspersky Security Center zu verwalten, gehen Sie wie folgt vor:

- Installieren Sie auf dem Computer, auf dem die Administrationskonsole von Kaspersky Security Center installiert ist, das Verwaltungs-Plug-in für Kaspersky Anti-Virus (Datei \plugin\klcfginst.exe aus dem Lieferumfang von Anti-Virus).
- Wenn der Administrationsagent von Kaspersky Security Center nicht auf den geschützten Servern installiert ist, können Sie ihn im Rahmen der Remote-Installationsaufgabe zusammen mit Kaspersky Anti-Virus installieren.

Außerdem können Sie bestimmte Server vorab in einer Administrationsgruppe zusammenfassen, um die Schutzparameter später mit Hilfe von Gruppenrichtlinien von Kaspersky Security Center zu verwalten.

➧ *Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus mit Hilfe einer Aufgabe zur Ferninstallation zu installieren:*

1. Klappen Sie in der Administrationskonsole den Knoten **Remote-Installation** auf und erstellen Sie im untergeordneten Knoten **Installationspakete** ein neues Installationspaket. Geben Sie dabei als Datei für das Installationspaket die Datei kavws.kpd aus dem Lieferumfang an.
2. Ändern Sie bei Bedarf in den Eigenschaften des erstellten Installationspakets den Bestand der zu installierenden Komponenten von Kaspersky Anti-Virus, die Installationsparameter.

   Sie können Details über die Programmkomponenten von Kaspersky Anti-Virus (s. S. 14) und die standardmäßigen Installationsparameter nachlesen (s. S. 16).

   Klappen Sie in der Administrationskonsole den Knoten **Remote-Installation** auf und öffnen Sie im untergeordneten Knoten **Installationspakete** im Ergebnisfenster das Kontextmenü für das neue Installationspaket von Kaspersky Anti-Virus. Wählen Sie dort den Befehl **Eigenschaften**. Im Fenster **Eigenschaften: <Name des Installationspakets>** im Abschnitt **Einstellungen** wie folgt vor:

   a. Aktivieren Sie in der Optionsgruppe **Zu installierende Komponenten** die Kontrollkästchen der Komponenten von Kaspersky Anti-Virus, die Sie installieren möchten.

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

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

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

   - Antiviren-Untersuchung des Computers vor Beginn der Installation ausführen.
   - Echtzeitschutz nach der Installation des Programms aktivieren.
   - Dateien, die von Microsoft empfohlen werden, zu Ausnahmen hinzufügen.
   - Ausnahmen, die von Kaspersky Lab empfohlen werden, berücksichtigen.
   - Objekte nach der Maske not-a-virus:RemoteAdmin* zu Ausnahmen hinzufügen.

d. Um die Einstellungen für Kaspersky Anti-Virus aus einer vorhandenen Konfigurationsdatei zu importieren, die in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition erstellt wurde, geben Sie diese Konfigurationsdatei an.

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

3. Erstellen Sie im Knoten **Installationspakete** eine Aufgabe zur Remote-Installation, mit der Kaspersky Anti-Virus auf die ausgewählten Computer (Gruppe) installiert wird. Passen Sie die Aufgabeneinstellungen an.

   Genaue Angaben darüber, wie eine Remote-Installationsaufgabe erstellt und angepasst wird, finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

4. Starten Sie die neue Aufgabe zur Remote-Installation von Kaspersky Anti-Virus.

   Kaspersky Anti-Virus wird auf den in der Aufgabe angegebenen Computern installiert.

SIEHE:

Aktionen nach der Installation von Kaspersky Anti-Virus 42

Einstellungen von Kaspersky Anti-Virus prüfen. Verwendung des EICAR-Testvirus 60

AKTIONEN NACH DER INSTALLATION VON KASPERSKY ANTI-VIRUS

Nach der Installation von Kaspersky Anti-Virus wird empfohlen, die Antiviren-Datenbanken auf den Servern zu aktualisieren. Sollte vor der Installation von Kaspersky Anti-Virus auf den Servern keine Antiviren-Anwendungen mit integrierter Funktion zum Echtzeitschutz von Dateien installiert gewesen sein, wird außerdem empfohlen, die Untersuchung von kritischen Bereichen der Server vorzunehmen.

Wenn Server, auf denen Sie Kaspersky Anti-Virus installiert haben, von Kaspersky Security Center zu einer Administrationsgruppe zusammengefasst sind, können Sie diese Aufgaben auf folgende Weise ausführen:

1. Erstellen Sie eine Aufgabe Update der Programm-Datenbanken für Server, auf denen Sie Kaspersky Anti-Virus installiert haben. Geben Sie als Update-Quelle den Administrationsserver an. Starten Sie die Aufgabe.
2. Erstellen Sie eine Gruppenaufgabe zur Untersuchung auf Befehl mit dem Status "Aufgabe zur Untersuchung von kritischen Bereichen". Die Anwendung Kaspersky Security Center wird den Sicherheitszustand jedes Servers der Gruppe aufgrund der Ausführungsergebnisse dieser Gruppe bewerten, nicht nach den Ergebnissen der Systemaufgabe **Untersuchung kritischer Bereiche**. Starten Sie die Aufgabe.
3. Erstellen Sie eine neue Richtlinie für die Servergruppe. Deaktivieren Sie in den Eigenschaften der erstellten Richtlinie auf der Registerkarte **Systemaufgaben** den nach Zeitplan gesteuerten Start von Systemaufgaben zur Untersuchung auf Befehl und Update der Datenbanken auf den Servern der Gruppe.

Sie können auch die Benachrichtigung des Administrators bei Ereignissen von Kaspersky Anti-Virus einrichten (s. *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition*).

IN DIESEM ABSCHNITT

Gruppenaufgabe für das Update der Programm-Datenbanken erstellen und starten 43

Gruppenaufgabe für die Untersuchung von Servern erstellen und starten, und dieser Aufgabe den Status "Aufgabe zur Untersuchung kritischer Bereiche" zuweisen 43

GRUPPENAUFGABE FÜR DAS UPDATE DER PROGRAMM-DATENBANKEN ERSTELLEN UND STARTEN

Nachdem Sie mit der Richtlinie die Update-Quelle festgelegt haben, erstellen Sie eine Gruppenaufgabe zum Update der Datenbanken von Kaspersky Anti-Virus und starten Sie die Aufgabe. Als Startintervall der Aufgabe können Sie **Nach Update-Download durch den Administrationsserver** wählen.

Um eine Gruppenaufgabe für das Update der Programm-Datenbanken zu erstellen, gehen Sie wie folgt vor:

1. Starten Sie den Assistenten für neue Gruppenaufgaben: Klappen Sie in der Struktur der Administrationskonsole den Knoten **Verwaltete Computer** auf, wählen Sie die Gruppe aus, für deren Server Sie eine Aufgabe erstellen möchten, öffnen Sie das Kontextmenü für den Ordner **Aufgaben** und klicken Sie auf **Erstellen → Aufgabe**.
2. Geben Sie im Assistenten für neue Aufgaben im Fenster **Aufgabenname festlegen** einen Namen für die Aufgabe an, z. B. **Datenbank-Update auf den Servern der Gruppe**.
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: **Update der Programm-Datenbanken.**
4. Wählen Sie im Fenster **Einstellungen** den Punkt **Erstellen**.
5. Wählen Sie im Fenster **Update-Quelle** den Punkt **Administrationsserver für Kaspersky Security Center**.
6. Aktivieren Sie im Fenster **Zeitplan** das Kontrollkästchen **Aufgabe nach Zeitplan starten** und aus der Liste **Startintervall** wählen Sie den Punkt **Nach Update-Download durch den Administrationsserver** aus.
7. Klicken Sie im Fenster **Erstellung der Aufgabe abschließen** des Assistenten für neue Aufgaben auf **Fertig stellen**.
8. Starten Sie die Aufgabe.

GRUPPENAUFGABE FÜR DIE UNTERSUCHUNG VON SERVERN ERSTELLEN UND STARTEN, UND DIESER AUFGABE DEN STATUS "AUFGABE ZUR UNTERSUCHUNG KRITISCHER BEREICHE" ZUWEISEN

Um in der Administrationskonsole eine Gruppenaufgabe zur Untersuchung von kritischen Bereichen für die Server zu erstellen und der Aufgabe den Status einer Aufgabe zur Untersuchung kritischer Bereiche zuzuweisen, gehen Sie wie folgt vor:

1. Starten Sie den Assistenten für neue Gruppenaufgaben: Klappen Sie in der Struktur der Administrationskonsole den Knoten **Verwaltete Computer** auf, wählen Sie die Gruppe aus, für deren Server Sie eine Aufgabe erstellen möchten, öffnen Sie das Kontextmenü für den Ordner **Aufgaben** und klicken Sie auf **Erstellen → Aufgabe.**
2. Geben Sie im Assistenten für neue Aufgaben im Fenster **Aufgabenname festlegen** einen Namen für die Aufgabe an, z. B. **Untersuchung kritischer Bereiche auf den Servern der Gruppe**.
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: **Untersuchung auf Befehl.**
4. Wählen Sie im Fenster **Einstellungen** den Punkt **Erstellen**.
5. Ändern Sie bei Bedarf den Untersuchungsbereich im Fenster **Untersuchungsbereich**. Wichtige Bereiche des Servers gehören standardmäßig zum Untersuchungsbereich.
6. Aktivieren Sie im Fenster **Einstellungen** das Kontrollkästchen **Aufgabenausführung als Untersuchung kritischer Computerbereiche betrachten**.
7. Nehmen Sie im Fenster **Zeitplan** folgende Zeitplaneinstellungen für die Aufgabe vor:
   a. Aktivieren Sie das Kontrollkästchen **Aufgabe nach Zeitplan starten**.
   b. Wählen Sie das Startintervall der Aufgabe, beispielsweise ein Mal in der Woche.
   c. Legen Sie im Feld **Start** die Uhrzeit des Aufgabenstarts fest.
   d. Tragen Sie im Feld **Beginnen am** das aktuelle Datum als Termin für das Inkrafttreten des Zeitplans ein.
   e. Klicken Sie auf **OK**.
8. Klicken Sie im Fenster **Erstellung der Aufgabe abschließen** des Assistenten für neue Aufgaben auf **Fertig stellen**.
9. Starten Sie die Aufgabe.

INSTALLATION DER KONSOLE VON KASPERSKY ANTI-VIRUS ÜBER KASPERSKY SECURITY CENTER

Dieser Abschnitt bietet eine kurze Anleitung für die Installation der Konsole von Kaspersky Anti-Virus mit Hilfe einer Aufgabe zur Remote-Installation über Kaspersky Security Center.

Details darüber, wie ein Installationspaket und die Aufgabe zur Remote-Installation erstellt werden, finden Sie im Dokument "*Kaspersky Security Center. Implementierungshandbuch*".

Gehen Sie folgendermaßen vor, um die Konsole von Kaspersky Anti-Virus mit Hilfe einer Aufgabe zur Ferninstallation zu installieren:

1. Klappen Sie in der Administrationskonsole den Knoten **Remote-Installation** auf und erstellen Sie im untergeordneten Knoten **Installationspakete** auf Basis der Datei client\setup.exe ein neues Installationspaket. Um das neue Installationspaket zu erstellen:

   - Wählen Sie im Fenster **Typ des Installationspakets auswählen** den Punkt **Installationspaket für die benutzerdefinierte Anwendung erstellen** und wählen Sie die Datei client\setup.exe aus. Diese Datei wird mitgeliefert und befindet sich im Ordner für die jeweilige Bit-Version des installierten Microsoft Windows-Betriebssystems (Ordner \x86 – für 32-Bit Microsoft Windows; Ordner \x64 – für 64-Bit Microsoft Windows).
   - Falls erforderlich, ändern Sie im Feld **Starteinstellungen für ausführbare Datei (optional)** mithilfe des Parameters ADDLOCAL die Auswahl der zu installierenden Komponenten und ändern Sie den Zielordner.

     Um beispielsweise im Ordner C:\KasperskyConsole nur die Anti-Virus-Konsole zu installieren, nicht aber die Hilfedatei und Dokumentation, geben Sie folgenden Befehl ein:

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

   Informieren Sie sich ausführlicher über die Programmkomponenten von Kaspersky Anti-Virus (s. S. 14).

2. Erstellen Sie im Knoten **Installationspakete** eine Aufgabe zur Remote-Installation der Konsole von Kaspersky Anti-Virus auf ausgewählten Computern (in eine Gruppe). Passen Sie die Aufgabeneinstellungen an.

   Genaue Angaben darüber, wie eine Remote-Installationsaufgabe erstellt und angepasst wird, finden Sie im *Administratorhandbuch zu Kaspersky Security Center*.

3. Starten Sie die angelegte Aufgabe zur Remote-Installation. Die Konsole von Kaspersky Anti-Virus wird auf den in der Aufgabe angegebenen Computern installiert.

DEINSTALLATION VON KASPERSKY ANTI-VIRUS ÜBER KASPERSKY SECURITY CENTER

Um Kaspersky Anti-Virus zu deinstallieren, führen Sie in der Administrationskonsole von Kaspersky Security Center folgende Aktionen aus.

1. Erstellen Sie eine Aufgabe zur Programmdeinstallation und starten Sie die Aufgabe.
2. Wählen Sie in der Aufgabe die Deinstallationsmethode (auf die gleiche Weise, wie die Installationsmethode gewählt wurde; s. vorhergehender Punkt) und geben Sie das Benutzerkonto an, unter dem der Administrationsserver auf die Computer zugreifen soll. Sie können Kaspersky Anti-Virus nur mit den standardmäßigen Deinstallationsparametern deinstallieren (s. Pkt. Parameter für Installation und Deinstallation sowie deren Schlüssel für den Dienst Windows Installer auf der Seite 16).

INSTALLATION UND DEINSTALLATION VON KASPERSKY ANTI-VIRUS ÜBER GRUPPENRICHTLINIEN VON ACTIVE DIRECTORY

Dieser Abschnitt bietet eine Beschreibung der Installation und Deinstallation von Kaspersky Anti-Virus über Active Directory-Gruppenrichtlinien, sowie Informationen über die Aktionen, die nach der Installation von Kaspersky Anti-Virus über Active Directory-Gruppenrichtlinien erforderlich sind.

IN DIESEM ABSCHNITT

INSTALLATION VON KASPERSKY ANTI-VIRUS ÜBER GRUPPENRICHTLINIEN DES ACTIVE DIRECTORY

Sie können Kaspersky Anti-Virus auf einigen Servern über eine Gruppenrichtlinie des Active Directory installieren. Auf die gleiche Weise kann auch die Konsole von Kaspersky Anti-Virus installiert werden.

Die Computer, auf denen Sie Kaspersky Anti-Virus (die Konsole von Kaspersky Anti-Virus) installieren möchten, müssen zu einer Domäne und einer Organisationseinheit gehören.

Die Betriebssysteme auf den Computern, auf denen Sie Kaspersky Anti-Virus mit der Richtlinie installieren wollen, müssen die gleiche Bit-Version (32-Bit oder 64-Bit) besitzen.

Sie müssen über Administratorrechte auf dem Domain verfügen.

Um Kaspersky Anti-Virus zu installieren, verwenden Sie das Installationspakets kavws.msi. Um die Konsole von Kaspersky Anti-Virus zu installieren, verwenden Sie kavwstools.msi.

Details darüber, wie die folgenden Schritte auszuführen sind, finden Sie in der entsprechenden Dokumentation der Firma Microsoft.

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus (die Konsole von Kaspersky Anti-Virus) zu installieren:

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

Kaspersky Anti-Virus wird auf den Computern der Gruppe nach deren Neustart und vor der Anmeldung bei Microsoft Windows installiert.

AKTIONEN NACH DER INSTALLATION VON KASPERSKY ANTI-VIRUS

Nach der Installation von Kaspersky Anti-Virus auf den geschützten Servern wird empfohlen, sofort die Datenbanken von Kaspersky Anti-Virus zu aktualisieren und eine Untersuchung von kritischen Bereichen des Servers auszuführen. Diese Aktionen können aus der Konsole von Kaspersky Anti-Virus ausgeführt werden (s. S. 32).

Sie können auch die Benachrichtigung des Administrators bei Ereignissen von Kaspersky Anti-Virus einrichten (s. *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition*).

KASPERSKY ANTI-VIRUS ENTFERNEN ÜBER GRUPPENRICHTLINIEN DES ACTIVE DIRECTORY

Wenn Sie Kaspersky Anti-Virus (die Konsole von Kaspersky Anti-Virus) auf Rechnern einer Gruppe mit einer Gruppenrichtlinie des Active Directory installiert haben, können Sie diese Richtlinie verwenden, um Kaspersky Anti-Virus (die Konsole von Kaspersky Anti-Virus) zu deinstallieren.

Sie können die Deinstallation nur mit den standardmäßigen Deinstallationsparametern ausführen.

Details darüber, wie die folgenden Schritte auszuführen sind, finden Sie in der entsprechenden Dokumentation der Firma Microsoft.

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus (die Konsole von Kaspersky Anti-Virus) zu deinstallieren:

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

Kaspersky Anti-Virus wird von den Computern nach deren Neustart und vor der Anmeldung bei Microsoft Windows deinstalliert.

UPGRADE EINER VORGÄNGERVERSION DES PROGRAMMS

Sie können Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 installieren, ohne die Vorgängerversion des Programms zu löschen. Dies gilt, wenn auf Ihrem Computer eine der folgenden Versionen von Kaspersky Anti-Virus installiert ist:

- Kaspersky Anti-Virus 6.0 für Windows Servers MP4
- Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition

Dieser Abschnitt informiert darüber, welche Einstellungen für installierte Programme in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 gespeichert werden, wie diese Einstellungen heißen und welche Werte diese Einstellungen nach der Migration annehmen.

Bei einem Upgrade des Programms auf Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 kann ein Neustart des Computers erforderlich werden.

IN DIESEM ABSCHNITT

MIGRATION VON EINSTELLUNGEN AUS KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4

In diesem Abschnitt stehen Informationen darüber, welche Parameter von Kaspersky Anti-Virus 6.0 für Windows Servers MP4 in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition gespeichert werden, wie sie heißen und welche Werte nach dem Import übernommen werden.

IN DIESEM ABSCHNITT

ALLGEMEINE EINSTELLUNGEN UND DIENSTEINSTELLUNGEN

In den folgenden Tabellen stehen Angaben darüber, welchen Parametern in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 die allgemeinen Parameter und Service-Parameter entsprechen und welche Werte sie nach der Migration auf die neue Version annehmen.

Tabelle 13. Allgemeine Parameter

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Schutz aktivieren (an/aus)	–	Fehlt. In Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 können Sie den Serverschutz verwalten, indem Sie die Aufgaben **Echtzeitschutz für Dateien** und **Skript-Untersuchung** starten und beenden.
Programm bei Einschalten des Computers starten	–	Fehlt.
Erweitert (Ressourcen für andere Programme freigeben)	Aufgabe im Hintergrund ausführen	Wird in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 für alle Untersuchungsaufgaben verwendet.
Technologie zur aktiven Desinfektion verwenden	–	Fehlt.
Malware-Kategorien	–	Fehlt.
Programmeinstellungen verwalten	–	Fehlt.
Leistung	–	Fehlt. In Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 können Sie das Maximum der Prozesse vorgeben, die Kaspersky Anti-Virus gleichzeitig starten kann, sowie andere Leistungsparameter (allgemeine Parameter von Kaspersky Anti-Virus).
Datendateien	–	Fehlt.
Ansicht	–	Fehlt.

Tabelle 14. Service-Parameter

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Interaktion mit dem Benutzer	Benachrichtigung von Benutzern	Entspricht dem Standardwert in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2.
Selbstschutz	–	Fehlt
Konfigurationsverwaltung	–	Fehlt
Kompatibilität	–	Fehlt

EINSTELLUNGEN FÜR DATEI-ANTI-VIRUS

In den folgenden Tabellen stehen Angaben darüber, welchen Parametern in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 die allgemeinen Parameter von Datei-Anti-Virus entsprechen und welche Werte sie nach der Migration annehmen.

Tabelle 15. Aufgaben des Echtzeitschutzes

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Mail-Anti-Virus	Aufgabe **Echtzeitschutz für Dateien**	Wird gespeichert.
Status des Echtzeitschutzes (**Datei-Anti-Virus aktivieren**)	Zeitplan der Aufgabe **Echtzeitschutz für Dateien**	Speicherung mit den folgenden Werten: • Datei-Anti-Virus ist aktiviert – Startintervall für den Zeitplan: **Bei Programmstart**. • Datei-Anti-Virus ist deaktiviert - Zeitplan für die Aufgabe **Echtzeitschutz für Dateien** ist ausgeschaltet.

*Tabelle 16. Schutzbereich der Aufgabe **Echtzeitschutz für Dateien***

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Vordefinierte Schutzbereiche		
Festplatten	Lokale Festplatten	Wird gespeichert.
Wechseldatenträger	Wechseldatenträger	Wird gespeichert.
Netzwerklaufwerke	Netzwerkumgebung	Wird beibehalten; Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 untersucht in der Grundeinstellung alle Dateien im Netzwerk, auf die Serveranwendungen zugreifen.
Dateien und Ordner, die der Benutzer vorgibt	Dateien und Ordner, die der Benutzer vorgibt	Es werden alle Objekte gespeichert, außer "Datei"-Objekten, für die das Kontrollkästchen **Untergeordnete Ordner** aktiviert ist. In Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 wird in den Schutzbereich nur die Datei mit dem von Ihnen angegebenen Pfad eingefügt. Dateien mit dem von Ihnen angegebenen Namen, die sich in untergeordneten Ordner befinden, werden nicht in den Schutzbereich eingefügt. In Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 können Sie so keine Objekte in den Schutzbereich aufnehmen.

Bei der Migration können Fehler auftreten, die mit nicht unterstützten Bereichen oder einem nicht definierten Untersuchungsbereich zusammenhängen. In diesem Fall ist es nicht möglich, wenigstens einen Untersuchungsbereich zu migrieren. Dann muss als Untersuchungsbereich das Objekt **MyComputer** hinzugefügt werden, für das die gleichen Untersuchungseinstellungen wie in der zu übertragenden Aufgabe angepasst werden müssen.

Tabelle 17. Parameter für Echtzeitschutz

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Vordefinierte Sicherheitsstufe		
Hoch	Maximale Sicherheit	Wird mit den Parameterwerten gespeichert, die der Sicherheitsstufe in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 entsprechen.
Empfohlen	Empfohlen	Wird mit den Parameterwerten gespeichert, die der Sicherheitsstufe in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 entsprechen.
Niedrig	Maximale Leistung	Wird mit den Parameterwerten gespeichert, die der Sicherheitsstufe in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 entsprechen.
Benutzerdefiniert	Benutzerdefiniert	Alle Einstellungen, die zu der Sicherheitsstufe **Benutzerdefiniert** gehören, werden nach folgenden Regeln übertragen: Die Einstellungen für Aktionen in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 werden auf alle Objekte des Schutzbereichs angewendet. (In Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 sind diese Einstellungen für jedes einzelne Schutzobjekt individuell). Die Einstellungen für Aktionen in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 werden für infizierte und möglicherweise infizierte Objekte jeweils separat angepasst.
Kategorien schädlicher Programme	–	Fehlt. Standardmäßig erkennt Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 alle Kategorien von Malware. Sie können von der Verarbeitung einzelne Malware-Kategorien mit Ausnahmen von der vertrauenswürdigen Zone ausschließen.
Parameter für Sicherheit		
Dateitypen	Schutz von Objekten	Wird gespeichert.
Optimierung	Nur neue und veränderte Dateien untersuchen.	Wird gespeichert.
Compound-Dateien	Schutz von zusammengesetzten Objekten	Wird gespeichert.
Entpacken verschieben, wenn Datei größer	–	Fehlt.
Nicht entpacken, wenn Datei größer	Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	Wird gespeichert.
Untersuchungsmodus	Schutzmodus für Objekte	Wird gespeichert.

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Beenden einer Aufgabe nach Zeitplan	Zeitplan der Aufgabe **Echtzeitschutz für Dateien**	Speichern. Zeitplan-Parameter **Anhalten von … bis**, in dem die Frist dem in Kaspersky Anti-Virus 6.0 für Windows Servers MP4 eingegebenen Wert entspricht, wird eingeschaltet.
Anhalten des Schutzes beim Programmstart	–	Fehlt.
Aktionen (wenn ein infiziertes Objekt gefunden wurde)		
Die Kontrollkästchen **Desinfizieren** und **Löschen** sind nicht aktiviert.	Zugriff sperren	Wird gespeichert.
Desinfizieren	Zugriff verweigern und desinfizieren	Wird gespeichert.
Löschen	Zugriff verweigern und löschen	Wird gespeichert.
Desinfizieren, wenn Desinfektion nicht möglich ist	Zugriff verweigern und desinfizieren. Irreparable Objekte löschen	Wird gespeichert.
Aktionen (wenn ein möglicherweise infiziertes Objekt gefunden wurde)		
Die Kontrollkästchen **Desinfizieren** und **Löschen** sind nicht aktiviert.	Zugriff sperren	Wird gespeichert.
Desinfizieren	Zugriff verweigern und in die Quarantäne verschieben	Wird gespeichert.
Löschen	Zugriff verweigern und löschen	Wird gespeichert.
Desinfizieren, wenn Desinfektion nicht möglich ist	Zugriff verweigern und in die Quarantäne verschieben	Wird gespeichert.
Aktionen beim Erkennen von infizierten oder möglicherweise infizierten Objekten		
Benutzer für <Stunden> sperren	–	Fehlt.
Benutzer benachrichtigen (Net Send)	–	Wird gespeichert.

EINSTELLUNGEN FÜR DIE UNTERSUCHUNG AUF BEFEHL

In den folgenden Tabellen stehen Angaben darüber, welchen Parametern in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 die Parameter der Untersuchung auf Befehl entsprechen und welche Werte sie nach der Migration auf die neue Version annehmen.

Tabelle 18. Parameter von Aufgaben zur Untersuchung auf Befehl

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Aufgabe		
Kritische Bereiche	Fehlt	–
Arbeitsplatz	Vollständige Untersuchung des Computers	Fehlt.
Autostart-Objekte	Untersuchung bei Systemstart	Fehlt.
Vollständige Untersuchung	Vollständige Untersuchung des Computers	Benutzerdefinierte Aufgabenkategorien.
Schnelle Untersuchung	Untersuchung beim Start des Betriebssystems	Wird gespeichert.
Ressourcen für andere Programme freigeben	Aufgabe im Hintergrund ausführen	Speichern, gilt für alle Aufgaben zur Untersuchung auf Befehl.
Starten der Aufgabe im Namen von	Start mit Rechten	Werden beibehalten, außer den Kennwörtern. Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 importiert keine Kennwörter. Sie müssen das Kennwort nach dem Import der Parameter in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 noch einmal eingeben.

Tabelle 19. Untersuchungsbereich in den Aufgaben zur Untersuchung auf Befehl

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Vordefinierte Untersuchungsbereiche		Wenn der Untersuchungsbereich bei der Migration auf die neue Version nicht beibehalten wurde (wenn beispielsweise keiner der ausgewählten vordefinierten Untersuchungsbereiche einen entsprechenden Bereich in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 hat), dann wird in der Aufgabe der vordefinierte Untersuchungsbereich **Arbeitsplatz** aktiviert.
Systemspeicher	Systemspeicher	Wird gespeichert.
Autostart-Objekte	Autostart-Objekte	Wird gespeichert.
System-Backup	Fehlt	–
Posteingänge	Fehlt	–
Boot-Sektoren der Datenträger	Parameter **Bootsektoren und MBR** für die vordefinierten Bereiche **Lokale Festplatten** und **Wechseldatenträger**	Wird gespeichert.
Festplatten	Lokale Festplatten	Standardumfang des Untersuchungsbereiches in benutzerdefinierten Aufgaben zur Untersuchung auf Befehl.

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Wechseldatenträger	Wechseldatenträger	Standardumfang des Untersuchungsbereiches in benutzerdefinierten Aufgaben zur Untersuchung auf Befehl.
Netzwerklaufwerke	Netzwerkumgebung	Wird beibehalten; Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 untersucht in der Grundeinstellung alle Dateien im Netzwerk, auf die Serveranwendungen zugreifen.
Dateien und Ordner, die der Benutzer vorgibt	Dateien und Ordner, die der Benutzer vorgibt	Es werden alle Objekte gespeichert, außer "Datei"-Objekten, für die das Kontrollkästchen **Untergeordnete Ordner** aktiviert ist. In Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 wird in den Untersuchungsbereich nur die Datei mit dem von Ihnen angegebenen Pfad eingefügt. Dateien mit den von Ihnen angegebenen Namen, die sich in untergeordneten Ordnern befinden, werden nicht in den Untersuchungsbereich eingefügt. In Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 können Sie so keine Objekte in den Untersuchungsbereich aufnehmen.

Tabelle 20. Sicherheitseinstellungen für Aufgaben zur Untersuchung auf Befehl

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Vordefinierte Sicherheitsstufe		
Hoch	Maximale Sicherheit	Wird mit den Parameterwerten gespeichert, die der Sicherheitsstufe in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 entsprechen.
Empfohlen	Empfohlen	Wird mit den Parameterwerten gespeichert, die der Sicherheitsstufe in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 entsprechen.
Niedrig	Maximale Leistung	Wird mit den Parameterwerten gespeichert, die der Sicherheitsstufe in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 entsprechen.
Benutzerdefiniert	Benutzerdefiniert	Alle Einstellungen, die zu der Sicherheitsstufe **Benutzerdefiniert** gehören, werden nach folgenden Regeln übertragen: Die Einstellungen für Aktionen in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 werden auf alle Objekte des Schutzbereichs angewendet. (In Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 sind diese Einstellungen für jedes einzelne Schutzobjekt individuell). Die Einstellungen für Aktionen in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 werden für infizierte und möglicherweise infizierte Objekte jeweils separat angepasst.
Untersuchungsmethoden		

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Heuristische Analyse aktivieren / deaktivieren	Heuristische Analyse verwenden	Wird gespeichert.
Emulationsniveau	Emulationsniveau	Fehlt.
Rootkit-Suche	–	Fehlt.
Parameter für Sicherheit		
Dateitypen	Untersuchungsobjekte	Wird gespeichert.
Optimierung	Nur neue und veränderte Dateien untersuchen.	Wird gespeichert.
Compound-Dateien	Zusammengesetzte Objekte untersuchen	Wird gespeichert.
Start mit Rechten	Start mit Rechten	Das Kennwort wird nicht gespeichert. Nachdem die Einstellungen in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 importiert worden sind, müssen die Kennwörter neu eingegeben werden.
iChecker-Technologie verwenden	iChecker-Technologie verwenden	Wird gespeichert.
iSwift-Technologie verwenden	iSwift-Technologie verwenden	Wird gespeichert.
Entpacken verschieben, wenn Datei größer	–	Fehlt.
Nicht entpacken, wenn Datei größer	Zusammengesetzte Objekte nicht scannen, wenn größer als (MB)	Wird gespeichert.
Untersuchungsmodus	Schutzmodus für Objekte	Wird gespeichert.
Beenden einer Aufgabe nach Zeitplan	Zeitplan der Aufgabe **Echtzeitschutz für Dateien**	Speichern. Zeitplan-Parameter **Anhalten von … bis**, in dem die Frist dem in Kaspersky Anti-Virus 6.0 für Windows Servers MP4 eingegebenen Wert entspricht, wird eingeschaltet.
Anhalten des Schutzes beim Programmstart	–	Fehlt.
Malware-Kategorien	–	Fehlt. Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 erkennt alle Kategorien von Malware.
Aktionen (wenn ein möglicherweise infiziertes Objekt gefunden wurde)		
Die Kontrollkästchen **Desinfizieren** und **Löschen** sind nicht aktiviert.	Überspringen	Wird gespeichert.
Desinfizieren	Desinfizieren	Wird gespeichert.
Löschen	Löschen	Wird gespeichert.

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Desinfizieren, wenn Desinfektion nicht möglich ist	Desinfizieren. Irreparable Objekte löschen	Wird gespeichert.
Aktionen (wenn ein infiziertes Objekt gefunden wurde)		
Nach Untersuchung abfragen	–	Fehlt. Es gilt der Wert **Desinfizieren. Irreparable Objekte löschen**, der in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 als Standard voreingestellt ist.
Bei Untersuchung abfragen	–	Fehlt. Es gilt der Wert **Desinfizieren. Irreparable Objekte löschen**, der in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 als Standard voreingestellt ist.
Die Kontrollkästchen **Desinfizieren** und **Löschen** sind nicht aktiviert.	Überspringen	Wird gespeichert.
Desinfizieren	In Quarantäne verschieben	Wird gespeichert.
Löschen	Löschen	Wird gespeichert.
Desinfizieren, wenn Desinfektion nicht möglich ist	In Quarantäne verschieben	Wird gespeichert.

EINSTELLUNGEN FÜR DIE VERTRAUENSWÜRDIGE ZONE

In der folgenden Tabelle stehen Angaben darüber, welchen Parametern in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 die Parameter für die vertrauenswürdige Zone entsprechen und welche Werte sie nach der Migration annehmen.

Tabelle 21. Ausnahmeregeln für die vertrauenswürdige Zone

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Ordner ohne Unterordner	Wird dadurch gekennzeichnet, dass am Ende ein Schrägstrich steht und das Kontrollkästchen, das die Verschachtelung anzeigt, einen Nullwert besitzt.	Wird in eine Ausnahme des Typs "Datei" übertragen
Ordner mit Unterordnern	Wird dadurch gekennzeichnet, dass am Ende ein Schrägstrich steht und das Kontrollkästchen, das die Verschachtelung anzeigt, den Wert Eins besitzt.	Wird in eine Ausnahme des Typs "Ordner" übertragen

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Datei ohne Unterordner	Wird dadurch gekennzeichnet, dass am Ende kein Schrägstrich steht und das Kontrollkästchen, das die Verschachtelung anzeigt, einen Nullwert besitzt.	Wird in eine Ausnahme des Typs "Datei" übertragen
Datei mit Unterordnern	Wird dadurch gekennzeichnet, dass am Ende kein Schrägstrich steht und das Kontrollkästchen, das die Verschachtelung anzeigt, einen Nicht-Nullwert besitzt.	Wird in eine Ausnahme des Typs "Datei" übertragen
Laufwerk mit Unterordnern	Laufwerk mit Unterordnern	Wird in eine Ausnahme des Typs "Laufwerk" übertragen
Laufwerk ohne Unterordner	Laufwerk ohne Unterordner	Wird in eine Ausnahme des Typs "Datei" übertragen

UPDATE-EINSTELLUNGEN

In der folgenden Tabelle stehen Angaben darüber, welchen Parametern in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition die allgemeinen Update-Einstellungen entsprechen und welche Werte sie nach der Migration annehmen.

Tabelle 22. Update-Einstellungen

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Programm-Module aktualisieren	Aufgabe **Update der Programm-Module**	Speichern: • Der Modus **Programm-Module aktualisieren** ist aktiviert. Die Aufgabe **Update der Programm-Module** wird mit der Option **Wichtige Updates für Programm-Module verteilen und installieren** ausgeführt. • Modus **Programm-Module updaten** ist deaktiviert – Aufgabe **Update der Programm-Module** wird mit dem Parameter **Nur auf wichtige Updates für Programm-Module überprüfen** ausgeführt. Startmodus entspricht dem Zeitplan der **Update der Programm-Module** Update der Programm-Module Die übrigen Update-Einstellungen entsprechen denen in Kaspersky Anti-Virus 6.0 for Windows Servers MP4.
In Ordner kopieren	Aufgabe **Update-Verteilung**	Speichern mit den Update-Einstellungen und dem Ordnernamen, der in Kaspersky Anti-Virus 6.0 for Windows Servers MP4 angegeben wurde. Startmodus entspricht dem Zeitplan der **Update-Verteilung**.
Startmodus	Zeitplan	Es werden alle Einstellungen gespeichert, außer dem automatischen Startmodus (**Automatisch**). Dieser Modus wird für alle Update-Aufgaben durch den geplanten Start mit dem Intervall **Stündlich** ersetzt.

PARAMETER IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDER PARAMETER IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2	WERT: WIRD BEIBEHALTEN / FEHLT / ENTSPRICHT DEM STANDARDWERT IN KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVERS ENTERPRISE EDITION SERVICE PACK 2
Aktionen nach Update	–	Fehlt.
Starten der Aufgabe im Namen von	Start mit Rechten	Werden beibehalten, außer den Kennwörtern. Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 importiert keine Kennwörter. Sie müssen nach dem Import der Einstellungen in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 noch einmal das Kennwort eingeben.
Update-Quelle		Wenn in Kaspersky Anti-Virus 6.0 for Windows Servers MP4 mehr als ein Typ von Update-Quellen angegeben ist, wird in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 nur der Typ Update-Quelle verwendet, der in der Liste an erster Stelle steht (Kaspersky-Lab-Update-Server, Administrationsserver für Kaspersky Administration Kit oder benutzerdefinierte Quellen).
Es wurde keine Update-Quelle angegeben.	–	Fehlt. Es gilt der Wert **Kaspersky-Lab-Update-Server**, der in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 standardmäßig verwendet wird.
Administrationsserver von Kaspersky Security Center	Administrationsserver von Kaspersky Security Center	Speichern
Kaspersky-Lab-Update-Server	Kaspersky-Lab-Update-Server	Speichern
Benutzerdefinierte Update-Quellen	Andere HTTP-, FTP-Server oder Netzwerkressourcen	Gespeichert werden alle benutzerdefinierten Update-Quellen
LAN-Einstellungen		
Passiven FTP-Modus benutzen, wenn möglich, Zeitüberschreitung für Verbindung	Passiven FTP-Modus verwenden, wenn möglich	Speichern
Proxyserver verwenden	Proxyserver-Einstellungen für die Verbindung zu anderen Servern verwenden	Speichern
Parameter des Proxyservers (IP-Adresse oder DNS-Namen des Servers und dessen Port, Daten für Echtheitsprüfung)	Parameter des Proxyservers	Speichern, außer den Kennwörtern. Geben Sie die Kennwörter in Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 erneut ein.

EINSTELLUNGEN FÜR RICHTLINIEN

Die Parameter für die Registrierung von Ereignissen in Kaspersky Anti-Virus 6.0 for Windows Servers MP4 werden wie in den folgenden Tabellen beschrieben gespeichert. Bei der Migration werden die Parameter für die Registrierung von Ereignissen (Art der Benachrichtigung zum Ereignis, Speicherdauer des Ereignisses auf dem Server u. ä.). Wenn Sie allerdings den Text der Nachricht geändert haben, wird der von Ihnen eingegebene Text nicht gespeichert. Es gilt der Text, der in Kaspersky Anti-Virus 8.0 für Windows Server Enterprise Edition Service Pack 2 standardmäßig verwendet wird.

In den folgenden Tabellen stehen die Ereignisse von Kaspersky Anti-Virus 6.0 for Windows Servers MP4, deren Benachrichtigungen Sie mit den Richtlinien von Kaspersky Security Center konfigurieren können, und die entsprechenden Ereignisse von Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2.

Tabelle 23. Kritische Ereignisse

EREIGNIS IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDES EREIGNIS VON KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2
Erkennen von Viren, Würmern, Trojanern und Hackerprogrammen	Objekt gefunden
Erkennen eines möglicherweise infizierten Objektes	Möglicherweise infiziertes Objekt gefunden
Desinfizieren nicht möglich	Infiziertes Objekt wurde nicht desinfiziert
Lizenz ist abgelaufen	Gültigkeitsdauer der Lizenz ist abgelaufen
Bedrohungssignaturen sind stark veraltet	Datenbanken sind stark veraltet

Tabelle 24. Ereignisse "Funktionsausfall"

EREIGNIS IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDES EREIGNIS VON KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2
Lizenz fehlt, ist annulliert oder beschädigt	Bedingungen des Lizenzvertrags wurden verletzt
Fehler bei Programm-Update	Allgemeiner Update-Fehler
Aufgabe kann nicht ausgeführt werden	Interner Fehler
Bedrohungssignaturen fehlen oder sind beschädigt	Die Datenbanken sind beschädigt

Tabelle 25. Informative Ereignisse:

EREIGNIS IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDES EREIGNIS VON KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2
Erkennung von Spyware, Adware und anderen Programmarten	Fehlt
Lizenz endet bald	Die Gültigkeitsdauer der Lizenz läuft bald ab.
Weitere wichtige Ereignisse	Fehlt
Nachricht für Selbstschutz	Fehlt
Nachrichten über Computersperren	Fehlt

Tabelle 26. Ereignisse "Warnung"

EREIGNIS IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDES EREIGNIS VON KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2
Desinfektion der infizierten Objekte	Objekt wurde desinfiziert
Löschen der infizierten Objekte	Objekt wurde gelöscht
Objekt wurde in Quarantäne verschoben	Fehlt
Erkennen eines kennwortgeschützten Archives	Objekt erkannt, das kennwortgeschützt ist
Abschließen des Updates	Fehlt

EREIGNIS IN KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS MP4	ENTSPRECHENDES EREIGNIS VON KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 2
Aktivieren und Deaktivieren des Computerschutzes	Fehlt
Bedrohungssignaturen sind veraltet	Datenbanken sind veraltet

EINSTELLUNGEN FÜR GRUPPENAUFGABEN

Es muss sichergestellt werden, dass die Einstellungen für folgende Aufgabentypen von Kaspersky Anti-Virus 6.0 für Windows Servers MP4 in die Aufgaben für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 kopiert werden:

- Aufgabe zur Untersuchung auf Befehl
- Update-Aufgabe

Aufgabe zur Untersuchung auf Befehl

Alle Einstellungen der Untersuchungsaufgabe werden gemäß dem Übertragungsalgorithmus für lokale Untersuchungsaufgaben kopiert.

Die Einstellungen für den Untersuchungsbereich werden gemäß dem Übertragungsalgorithmus für den Untersuchungsbereich von Datei-Anti-Virus übertragen.

Update-Aufgabe

Die Einstellungen für die Update-Aufgabe werden gemäß den Einstellungen für lokale Update-Aufgaben kopiert und können verwendet werden, um folgende Gruppenaufgaben für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 zu erstellen:

- Update der Programm-Datenbanken
- Update der Programm-Module
- Update-Verteilung.

MIGRATION DER EINSTELLUNGEN AUS KASPERSKY ANTI-VIRUS 8.0 FÜR WINDOWS SERVER ENTERPRISE EDITION SERVICE PACK 1

Beim Upgrade von Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 1 auf Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition Service Pack 2 bleiben alle Programmeinstellungen unverändert erhalten. Richtlinien und Gruppenaufgaben für Kaspersky Security Center müssen nicht konvertiert werden und werden ohne Neuinstallation des Verwaltungs-Plug-ins für Kaspersky Anti-Virus unterstützt.

EINSTELLUNGEN VON KASPERSKY ANTI-VIRUS PRÜFEN. VERWENDUNG DES EICAR-TESTVIRUS

Dieser Abschnitt beschreibt den EICAR-Testvirus und das Vorgehen, mit dem die Kaspersky Anti-Virus-Funktionen "Echtzeitschutz" und "Untersuchung auf Befehl" mithilfe des EICAR-Testvirus überprüft werden.

IN DIESEM ABSCHNITT

EICAR-TESTVIRUS

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

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

Die Datei, die den Testvirus enthält, heißt eicar.com. Sie können sie von der Internetseite http://www.eicar.org/anti_virus_test_file.htm des **EICAR** laden.

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

Die Datei eicar.com enthält eine Textzeile. Beim Untersuchen der Datei erkennt Kaspersky Anti-Virus in dieser Textzeile eine Testbedrohung", weist der Datei den Status **Infiziert** zu und löscht sie. Die Daten über die erkannte Bedrohung in der Datei erscheinen in der Konsole von Kaspersky Anti-Virus im Detaillog über die Aufgabenausführung.

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

Damit Kaspersky Anti-Virus die Datei eicar.com mit Präfix verarbeitet, aktivieren Sie in Kaspersky Anti-Virus die Sicherheitseinstellung **Schutz von Objekten** in der Aufgabe **Echtzeitschutz für Dateien** / Aufgabe zur Untersuchung auf Befehl und legen Sie dafür den Wert **Alle Objekte** fest. S. Beschreibung im *Administratorhandbuch für Kaspersky Anti-Virus 8.0 für Windows Servers Enterprise Edition*.

Tabelle 27. Präfixe in EICAR-Dateien

PRÄFIX	STATUS DER DATEI NACH UNTERSUCHUNG UND AKTION VON KASPERSKY ANTI-VIRUS
Ohne Präfix	Kaspersky Anti-Virus weist dem Objekt den Status Infiziert zu und löscht es.
SUSP–	Kaspersky Anti-Virus weist dem Objekt den Status Möglicherweise infiziert (mit heuristischer Analysemethode erkannt) zu und löscht es (möglicherweise infizierte Objekte werden nicht desinfiziert).
WARN–	Kaspersky Anti-Virus weist dem Objekt den Status Möglicherweise infiziert (Code des Objektes stimmt partiell mit einem bekannten schädlichen Code überein) zu und löscht es (möglicherweise infizierte Objekte werden nicht desinfiziert).
CURE–	Kaspersky Anti-Virus weist dem Objekt den Status Infiziert zu und desinfiziert es. Wenn die Desinfektion gelingt, wird der gesamte Text in der Datei durch das Wort "CURE" ersetzt.

PRÜFUNG DER FUNKTIONEN VON KASPERSKY ANTI-VIRUS ECHTZEITSCHUTZ UND UNTERSUCHUNG AUF BEFEHL

Nach der Installation von Kaspersky Anti-Virus können Sie prüfen, dass Kaspersky Anti-Virus Objekte erkennt, die Malware enthalten. Für die Prüfung können Sie auf den Testvirus **EICAR** zurückgreifen (s. Seite 60).

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

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

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

2. Wenn Sie außerdem noch die Benachrichtigungen für die Benutzer des Netzwerks prüfen möchten, vergewissern Sie sich, dass auf dem geschützten Server und auf dem Computer, auf dem Sie die Datei eicar.com gespeichert haben, der Messenger von Microsoft Windows aktiviert ist.
3. Öffnen Sie die Konsole von Kaspersky Anti-Virus.
4. Kopieren Sie auf folgende Weise die gespeicherte Datei eicar.com auf den lokalen Datenträger des geschützten Servers:
   - Um die Funktion Benachrichtigung über Terminaldienste zu überprüfen, kopieren Sie die Datei eicar.com auf einen Server, der mit Hilfe des Programms "Remote Desktop Connection" an den Server angeschlossen ist.
   - Um die Funktion Benachrichtigung über den Messenger von Microsoft Windows zu überprüfen, kopieren Sie die Datei eicar.com von dem Computer, auf dem Sie sie gespeichert haben, über die Netzwerkumgebung dieses Computers.

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

- Die Datei eicar.com vom Datenträger des geschützten Servers gelöscht wurde.
- In der Konsole von Kaspersky Anti-Virus hat der Bericht über Aufgabenausführung den Status **Kritisch** angenommen. Im Bericht erschien eine Zeile mit einer Bedrohung in der Datei eicar.com. (Um einen Bericht über die Aufgabenausführung anzuzeigen, öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Echtzeitschutz**, wählen Sie die Aufgabe **Echtzeitschutz für Dateien** aus und klicken Sie im Ergebnisfenster auf den Link **Ausführungsbericht öffnen**).
- Es ist eine Meldung des Messengers von Microsoft Windows auf dem Bildschirm erschienen, von dem aus Sie die Datei kopiert haben (Terminaldienste in der Terminalsitzung auf dem Server), in der Folgendes steht: "Kaspersky Anti-Virus hat den Zugriff auf <Pfad der Datei eicar.com auf dem Server>\eicar .com für den Computer <Netzwerkname des Servers> um <Uhrzeit für Ereigniseintritt> gesperrt. Grund: Bedrohung erkannt. Virus: EICAR-Test-File. Name des Objektbenutzers: <Benutzername>. Computername des Objektbenutzers: <Netzwerkname des Computers, von dem die Datei kopiert wurde>".

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

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

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

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

2. Öffnen Sie die Konsole von Kaspersky Anti-Virus.

3. Führen Sie folgende Aktionen aus:
   a. Öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Untersuchung auf Befehl**.
   b. Markieren Sie die Aufgabe **Untersuchung kritischer Bereiche**.
   c. Auf der Registerkarte **Untersuchungsbereich anpassen** öffnen Sie das Kontextmenü für den Knoten **Netzwerkumgebung** und wählen Sie **Netzwerkordner hinzufügen**.
   d. Tragen Sie den Netzwerkpfad zur Datei eicar.com auf dem Remote-Computer im UNC-Format (Universal Naming Convention) ein.
   e. Aktivieren Sie das Kontrollkästchen, um den hinzugefügten Netzwerkpfad in den Untersuchungsbereich aufzunehmen.
   f. Starten Sie die Aufgabe **Untersuchung kritischer Bereiche**.

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

- Die Datei eicar.com vom Datenträger des Computers gelöscht wurde.
- In der Konsole von Kaspersky Anti-Virus besitzt der Bericht über Aufgabenausführung den Status **Kritisch**  . Im Bericht über Aufgabenausführung **Untersuchung kritischer Bereiche** ist eine Zeile mit Informationen über eine Bedrohung in der Datei eicar.com erschienen. (Um einen Bericht über die Aufgabenausführung anzuzeigen, öffnen Sie in der Konsolenstruktur von Kaspersky Anti-Virus den Knoten **Untersuchung auf Befehl**, wählen Sie die Aufgabe **Untersuchung kritischer Bereiche** aus und klicken Sie im Ergebnisfenster auf den Link **Ausführungsbericht öffnen**).

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
- Deutsch
- Russisch
- Spanisch
- Polnisch
- Französisch
- Italienisch
- Portugiesisch
- 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.

PROTOKOLLIERUNGSDATEI 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.

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

Technologie zur Erkennung von Bedrohungen, die noch nicht in den Datenbanken von Kaspersky Lab verzeichnet sind. Die heuristische Analyse erkennt Objekte, deren Verhalten eine Sicherheitsbedrohung für das Betriebssystem darstellen kann. Objekte, die mithilfe der heuristischen Analyse gefunden werden, werden als möglicherweise infiziert eingestuft. Als möglicherweise infiziert kann beispielsweise ein Objekt gelten, das eine Befehlsfolge enthält, die für schädliche Objekte als charakteristisch gilt (Datei öffnen, in Datei schreiben).

I

INFIZIERBARE DATEI

Datei, die 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

SCHLÜSSELDATEI

Datei der Form xxxxxxxx.key, mit deren Hilfe das Kaspersky-Lab-Programm durch Hinzufügen eines Schlüssels aktiviert werden kann. Dabei gelten die Lizenzbedingungen.

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

Eingetragene Marken und Dienstleistungszeichen sind Eigentum der jeweiligen Rechteinhaber.

Citrix, Citrix Presentation Server, XenApp und XenDesktop sind Marken von Citrix Systems, Inc. und/oder Tochterunternehmen, die in den USA und in anderen Ländern durch Patent geschützt sind.

Core und Intel sind in den Vereinigten Staaten von Amerika und in anderen Ländern eingetragene Marken der Intel Corporation.

Active Directory, Hyper-V, Excel, Microsoft, Windows, Windows Server, Windows Vista und JScript sind Handelsmarken von Microsoft Corporation, die in den USA und anderen Ländern eingetragen sind.

Radmin und Remote Administrator sind eingetragene Marken von Famatech.

SACHREGISTER

A

P